Documentazione Firew4ll

Release latest

InSecureNet SRL

30 giu 2020

Indice

La seguente documentazione offre istruzioni su come installare, configurare e gestire al meglio il software Firew4LL per proteggere la vostra rete, sia che siate alle prime armi, sia che siate più esperti.

Suggerimento: La documentazione è in continua evoluzione e aggiornamento.

CAPITOLO 1

Prefazione

Firew4LL-OS è un sistema operativo basato su **FreeBSD** e derivante dal fork di *pfSense*, completamente tradotto in italiano, tranne che nei termini prettamente tecnici, corredato da documentazione anch'essa in italiano.

Con Firew4ll-OS si può implementare un firewall in poche ore.

– Francesco Pellegrino (InSecureNet SRL) -

Suggerimento: Grazie al lavoro di InSecureNet è disponibile all'indirizzo: https://www.insecurelab.it/hackzionario un progetto per la semplificazione dei termini informatici.

«n» «n» «InSecureNet è Vincitore Progetto PIN - Iniziativa promossa dalle Politiche Giovanili della Regione Puglia e ARTI e finanziata con risorse del FSE-PO Puglia 2014/2020 Azione 8.4 e del Fondo per lo Sviluppo e la Coesione».

1.1 Avviso sul Copyright

1.2 Commenti

L'editore e gli autori incoraggiano i commenti per ampliare la documentazione di Firew4LL-OS.

Per un feedback generale relativo al progetto Firew4LL, si prega di contattarci agli indirizzi presenti sul sito di Firew4LL-OS.

Grazie per l'aiuto

CAPITOLO 2

Introduzione

2.1 Cosa significa Firew4LL?

Da un'idea di Francesco Pellegrino di InSecureNet e grazie all'iniziativa del Progetto PIN promosso dalla Regione Puglia, nasce il progetto Firew4LL, parola formata dalle 3 parole: «Firewall», «4», «All», letteralmente **Firewall per tutti**, che consiste nello sviluppo di un appliance con a bordo un sistema operativo, derivante dal fork di *pfSense*, completamente tradotto in italiano corredato da relativa documentazione.

2.2 Perché FreeBSD?

Numerosi fattori sono stati presi in considerazione nella scelta del sistema operativo di base per il progetto. Questa sezione illustra i motivi principali per la scelta di FreeBSD.

2.2.1 Supporto Wireless

Il supporto wireless è una funzionalità fondamentale per molti utenti. Nel 2004, il supporto wireless in OpenBSD era molto limitato rispetto a FreeBSD. OpenBSD non supportava driver o protocolli di sicurezza e non offriva piani per la loro implementazione. Ad oggi, FreeBSD supera le capacità wireless di OpenBSD.

2.2.2 Prestazioni della rete

Le prestazioni di rete in FreeBSD sono significativamente migliori di quelle di OpenBSD e altri os. Per distribuzioni di piccole e medie dimensioni, questo in genere non ha importanza, su scale superiori è il problema principale.

Il supporto del multiprocessore per pf in FreeBSD consente una maggiore scalabilità ed è utilizzato da Firew4LL, come si attesta in questa analisi delle prestazioni della rete: https://github.com/gvnn3/netperf/blob/master/Documentation/netperf.pdf.

2.2.3 Familiarità e facilità fork

Il codice di *m0n0wall* era basato su FreeBSD, e Firew4LL è un fork di *pfSense* che è un fork di *m0n0wall*. La modifica del sistema operativo di base richiederebbe modifiche proibitive e potrebbe aver introdotto limitazioni da altri sistemi operativi, richiedendo la rimozione o l'alterazione di funzionalità.

2.3 Funzionalità comuni

Firew4LL è in grado di soddisfare le esigenze di quasi ogni tipo e dimensione di ambiente di rete, da un SOHO (pmi o casa) a un data center. Questa sezione illustra gli scenari più comuni.

2.3.1 Firewall perimetrale

La funzione più comune di Firew4LL è quella di firewall perimetrale. Firew4LL supporta reti che richiedono più connessioni Internet, più reti LAN e più reti DMZ. Sono inoltre configurabili BGP (Border Gateway Protocol), ridondanza della connessione e capacità di bilanciamento del carico

Vedi anche:

Queste funzionalità avanzate sono descritte in *Routing* e *Multi WAN*.

2.3.2 Router LAN o WAN

Firew4LL, comunemente viene configurato come router LAN, WAN e firewall perimetrale in reti di piccole dimensioni, in reti più grandi routing LAN e WAN svolgono ruoli separati.

Router LAN

Firew4LL è una soluzione adatta per il collegamento di più segmenti di rete interni. Questo di solito è implementato su VLAN configurate con trunking 802.1Q.

Nota: Viene descritto meglio nella sezione *VLAN*.

In alcuni ambienti vengono utilizzate anche interfacce Ethernet multiple. Gli ambienti con un alto traffico LAN con meno requisiti di filtraggio possono invece necessitare di switch di livello 3 o di router basati su ASIC.

Router WAN

Firew4LL è un'ottima soluzione per i provider di servizi Internet. Offre tutte le funzionalità richieste dalla maggior parte delle reti a un prezzo molto più basso rispetto ad altre offerte commerciali.

2.3.3 Apparecchi per usi speciali

Firew4LL può essere utilizzato per scenari di distribuzione meno comuni come singolo servizio. Gli esempi includono: VPN, Sniffer e server DHCP.

Dispositivo VPN

Firew4LL installato come un VPN server aggiunge funzionalità VPN senza modificare l'infrastruttura firewall esistente, includendo più protocolli VPN.

Dispositivo Sniffer

Firew4LL offre un'interfaccia web per l'analisi di pacchetti tcpdump. I file .cap acquisiti vengono scaricati e analizzati in Wireshark.

Vedi anche:

Acquisizione dei pacchetti.

Server DHCP

Firew4LL può essere distribuito rigorosamente come un server DHCP. Tuttavia esistono limitazioni nella GUI di Firew4LL per la configurazione avanzata del demone ISC DHCP.

Terminologia delle interfacce

A ogni interfaccia Firew4LL può essere assegnato un qualsiasi nome, ma inizialmente hanno tutti nomi predefiniti: WAN, LAN e OPT.

2.3.4 WAN

Abbreviazione di *Wide Area Network*, **WAN** è la rete pubblica non controllata esterna firewall. In altre parole, l'interfaccia WAN è la connessione del firewall a Internet o ad altre reti upstream. In una distribuzione WAN multiple, WAN è la prima o principale connessione Internet.

Nota: Il firewall deve avere almeno un'interfaccia WAN.

2.3.5 LAN

Abbreviazione di *Local Area Network*, **LAN** è comunemente la rete privata. In genere utilizza uno schema di *indirizzamento IP privato* per i client locali. Nelle reti di piccole dimensioni, è in genere l'unica interfaccia interna.

2.3.6 OPT

Le interfacce *OPT o opzionali* si riferiscono a qualsiasi interfaccia aggiuntiva diversa da WAN e LAN primarie. Le interfacce OPT possono essere segmenti LAN aggiuntivi, connessioni WAN, segmenti DMZ, interconnessioni ad altre reti private e così via.

2.3.7 DMZ

Abbreviazione del termine militare zona demilitarizzata (*demilitarized zone*), **DMZ** si riferisce alla zona cuscinetto tra un'area protetta e una zona di guerra. Nella rete, è un'area in cui i server pubblici sono raggiungibili da Internet tramite WAN, ma isolati dalla LAN. Impedisce ai sistemi di altri segmenti di essere messi in pericolo se la rete è compromessa, proteggendo allo stesso tempo gli host nella DMZ da altri segmenti locali e da Internet in generale.

2.3.8 Denominazione dell'interfaccia di FreeBSD

Il nome di un'interfaccia di FreeBSD inizia con il nome del suo driver di rete. È quindi seguito da un numero che inizia da 0 e aumenta in modo incrementale di uno per ogni interfaccia aggiuntiva che condivide quel driver. Ad esempio, un driver comune utilizzato dalle schede di interfaccia di rete Intel gigabit è igb. La prima di queste carte in un sistema sarà igb0, la seconda è *igb1* e così via. Altri nomi di driver comuni includono cxl (Chelsio 10G), em (anche Intel 1G), ix (Intel 10G), bge (vari chipset Broadcom), tra gli altri. Se un sistema combina una scheda Intel e una scheda Chelsio, le interfacce saranno rispettivamente igb0 e cxl0.

Vedi anche:

Le assegnazioni e la denominazione dell'interfaccia sono trattate ulteriormente in *Installazione e aggiornamento*.

Tutte le richieste di informazioni e supporto possono essere trovate o trasmesse su:

- Firew4LL
- InSecureNet

CAPITOLO 3

Rete

3.1 Conoscere gli indirizzi IP pubblici e privati

3.1.1 Indirizzi IP privati

Lo standard di rete RFC 1918 definisce le sottoreti IPv4 riservate per il solo uso nelle reti private (Tabella *RFC 1918 Spazio indirizzi IP privati*). RFC 4193 definisce gli indirizzi locali univoci (ULA) per IPv6 (Tabella *RFC 4193 Spazio degli indirizzi locali univoci*). Nella maggior parte degli ambienti, viene scelta e utilizzata una sottorete IP privata di RFC 1918 su tutti i dispositivi di rete interni. I dispositivi vengono quindi collegati a Internet tramite un firewall o un router che implementa il software Network Address Translation (NAT), come Firew4LL. IPv6 viene completamente instradato dalla rete interna senza NAT dal Global Unicast Addresses (GUA). NAT sarà spiegato ulteriormente nella *traduzione degli indirizzi di rete*.

Tabella 1: Spazio degli indirizzi IP privati RFC 1918

Intervallo CIDR	Intervallo indirizzi IP
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Tabella 2: Spazio indirizzi locali univoci RFC 4193

Prefisso	Intervallo indirizzi IP
fc00::/7	fc00:: - fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Un elenco completo di reti IPv4 per uso speciale è disponibile in *RFC 3330*. Esistono indirizzi IPv4 privati, come 1.0.0.0/8 e 2.0.0.0/8, che da allora sono stati allocati nel pool IPv4 in diminuzione. L'uso di questi indirizzi è problematico e sconsigliato. Inoltre, evitare di utilizzare 169.254.0.0/16, che secondo RFC 3927 è riservato per la configurazione automatica «Link-Locale». Non deve essere assegnato da DHCP o impostato manualmente e i router non consentiranno ai pacchetti di quella sottorete di attraversare un dominio di trasmissione specifico. Lo spazio di indirizzi riservato da *RFC 1918* è sufficiente, quindi non è necessario deviare dall'elenco mostrato nella tabella *Spazio degli indirizzi IP privati RFC*. L'indirizzamento errato comporterà un errore di rete e dovrebbe essere corretto.

3.1.2 Indirizzi IP pubblici

Ad eccezione delle reti più grandi, gli indirizzi IP pubblici sono assegnati dai provider di servizi Internet. Le reti che richiedono centinaia o migliaia di indirizzi IP pubblici hanno comunemente uno spazio di indirizzi assegnato direttamente dal loro registro Internet regionale (RIR). Un RIR è un'organizzazione che supervisiona l'allocazione e la registrazione di indirizzi IP pubblici in determinate regioni del mondo.

Alla maggior parte delle connessioni Internet residenziali viene assegnato un unico indirizzo IPv4 pubblico. Alla maggior parte delle connessioni di classe business sono assegnati più indirizzi IP pubblici. Un singolo indirizzo IP pubblico è adeguato in molte circostanze e può essere utilizzato in collaborazione con NAT per connettere a Internet centinaia di sistemi indirizzati privatamente. Questa guida aiuterà a determinare il numero di indirizzi IP pubblici richiesti.

La maggior parte delle distribuzioni IPv6 fornirà all'utente finale almeno una rete con prefisso /64 da utilizzare come rete interna instradata. Per ogni sito, si tratta di circa 2^{64} indirizzi IPv6 o 18 *quintilioni* di indirizzi, completamente instradati in Internet senza necessità di NAT

3.1.3 Indirizzi riservati e documentazione

Oltre ai blocchi definiti in *RFC 1918*, *RFC 5735* descrive blocchi riservati per altri scopi speciali come documentazione, test e benchmarking. *RFC 6598* aggiorna *RFC 5735* e definisce lo spazio degli indirizzi anche per NAT di livello Carrier. Queste reti speciali includono:

Tabella 3: Spazio per gli indirizzi riservati RFC 5735

Intervallo CIDR	Scopo
192.0.2.0/24	Documentazione e codice di esempio
198.51.100.0/24	Documentazione e codice di esempio
203.0.113.0/24	Documentazione e codice di esempio
198.18.0.0/25	Analisi comparativa degli indirizzi di rete
100.64.0.0/10	Spazio per il Nat livello Carrier

Nella guida, useremo esempi con indirizzi degli intervalli di documentazione (v. sopra) e reti *RFC 1918* poiché sono più familiari agli utenti.

Alcuni trovano questi indirizzi allettanti da utilizzare per VPN o anche reti locali. Non possiamo raccomandare di usarli per scopi diversi da quelli previsti, ma è molto meno probabile che vengano visti «allo stato brado» rispetto alle reti *RFC 1918*.

3.2 Concetti delle sottoreti (subnet) IP

Quando si configurano le impostazioni TCP/IP su un dispositivo, è necessario specificare una subnet mask (o la lunghezza del prefisso per IPv6). Questa maschera consente al dispositivo di determinare quali indirizzi IP si trovano sulla rete locale e quali devono essere raggiunti da un gateway nella tabella di routing del dispositivo. L'indirizzo IP LAN predefinito 192.168.1.1 con una maschera (subnet mask) di 255.255.255.0 o /24 nella notazione CIDR ha un indirizzo network di 192.168.1.0/24. Il CIDR viene discusso in *Informazioni sulla notazione della subnet mask CIDR*.

3.3 Configurazione dell'indirizzo IP, della sottorete e del gateway

La configurazione TCP/IP di un host è composta da indirizzo, subnet mask (o lunghezza prefisso per IPv6) e gateway. L'indirizzo IP combinato con la subnet mask è il **modo** in cui l'host identifica quali indirizzi IP si trovano sulla sua

rete locale. Gli indirizzi esterni alla rete locale vengono inviati al gateway predefinito configurato dell'host, che si presume trasferirà il traffico alla destinazione desiderata. Un'eccezione a questa regola è una route statica che indica a un dispositivo di contattare specifiche sottoreti non locali raggiungibili tramite router connessi localmente. Questo elenco di gateway e route statiche viene conservato nella tabella di routing di ciascun host. Per visualizzare la tabella di routing utilizzata da Firew4LL, vedere *Visualizzare Route*. Ulteriori informazioni sul routing sono disponibili in *Routing*.

In una tipica distribuzione Firew4LL, agli host vengono assegnati un indirizzo IP, una subnet mask e un gateway all'interno dell'intervallo LAN del dispositivo. L'indirizzo IP LAN su Firew4LL diventa il gateway predefinito. Per gli host che si connettono tramite un'interfaccia diversa dalla LAN, utilizzare la configurazione appropriata per l'interfaccia a cui è collegato il dispositivo.

Gli host all'interno di una singola rete comunicano direttamente tra loro senza il coinvolgimento del gateway predefinito. Ciò significa che nessun firewall, incluso Firew4LL, può controllare le comunicazioni da host a host all'interno di un segmento di rete.

Se è richiesta questa funzionalità, gli host devono essere segmentati tramite l'uso di più switch, VLAN o utilizzare funzionalità di switch equivalenti come PVLAN. Le VLAN sono coperte dalla LAN Virtuale (VLAN).

3.4 Conoscere e capire la notazione della subnet mask CIDR

Firew4LL utilizza la notazione CIDR (Routing dell'intra-dominio senza classe, Classless Inter-Domain Routing) anziché la subnet mask comune 255.x.x.x durante la configurazione di indirizzi e reti. Fare riferimento alla seguente tabella della sottorete CIDR per trovare l'equivalente CIDR di una subnet mask decimale.

Table 4: Tabella delle sottoreti CIDR

Maschera sottorete	Prefisso CIDR	Indirizzi IP totali	Indirizzi IP utili	Numero di reti /24
255.255.255.255	/32	1	1	1/256
255.255.255.254	/31	2	2	1/128
255.255.255.252	/30	4	2	1/64
255.255.255.248	/29	8	6	1/32
255.255.255.240	/28	16	14	1/16
255.255.255.224	/27	32	30	1/8
255.255.255.192	/26	64	62	1/4
255.255.255.128	/25	128	126	1/2
255.255.255.0	/24	256	254	1
255.255.254.0	/23	512	510	2
255.255.252.0	/22	1024	1022	4
255.255.248.0	/21	2048	2046	8
255.255.240.0	/20	4096	4094	16
255.255.224.0	/19	8192	8190	32
255.255.192.0	/18	16,384	16,382	64
255.255.128.0	/17	32,768	32,766	128
255.255.0.0	/16	65,536	65,534	256
255.254.0.0	/15	131,072	131,070	512
255.252.0.0	/14	262,144	262,142	1024
255.248.0.0	/13	524,288	524,286	2048
255.240.0.0	/12	1,048,576	1,048,574	4096
255.224.0 0	/11	2,097,152	2,097,150	8192
255.192.0.0	/10	4,194,304	4,194,302	16,384
255.128.0.0	/9	8,388,608	8,388,606	32,768

Continua alla pagina successiva

Tabella 1 – continua dalla pagina precedente

Maschera sottorete	Prefisso CIDR	Indirizzi IP totali	Indirizzi IP utili	Numero di reti /24
255.0.0.0	/8	16,777,216	16,777,214	65,536
254.0.0.0	/7	33,554,432	33,554,430	131,072
252.0.0.0	/6	67,108,864	67,108,862	262,144
248.0.0.0	/5	134,217,728	134,217,726	1,048,576
240.0.0.0	/4	268,435,456	268,435,454	2,097,152
224.0.0.0	/3	536,870,912	536,870,910	4,194,304
192.0.0.0	/2	1,073,741,824	1,073,741,822	8,388,608
128.0.0.0	/1	2,147,483,648	2,147,483,646	16,777,216
0.0.0.0	/0	4,294,967,296	4,294,967,294	33,554,432

Nota: L'uso di reti /31 è un caso speciale definito da RFC in cui i due indirizzi IP nella sottorete sono utilizzabili per collegamenti punto-punto per conservare lo spazio degli indirizzi IPv4. Non tutti i sistemi operativi supportano RFC 3021, quindi va usato con cautela. Sui sistemi che non supportano RFC 3021, la sottorete è inutilizzabile perché gli unici due indirizzi definiti dalla subnet mask sono la route e la trasmissione nulla e nessun indirizzo host utilizzabile.

Firew4LL 0.1-RELEASE-p3 supporta l'uso di reti /31 per interfacce e indirizzi IP virtuali

3.4.1 Quindi da dove provengono i numeri CIDR?

Il numero CIDR è ottenuto da quelli della subnet mask convertiti in binario.

La subnet mask comune 255.255.255.0 è 11111111.11111111.11111111.00000000 in binario. Questo aggiunge fino a 24, o /24 (pronunciato «barra ventiquattro»).

Una subnet mask di 255.255.255.192 è 11111111.11111111.11111111.11000000 in binario o 26 unità, quindi /26.

3.5 Riepilogo CIDR

Oltre a specificare le maschere di sottorete, il CIDR può essere utilizzato anche per scopi di riepilogo IP o di rete. La colonna «Indirizzi IP totali» nella *tabella delle sottoreti CIDR* indica quanti indirizzi sono riepilogati da una determinata maschera CIDR. Ai fini del riepilogo delle reti, è utile la colonna «Numero di reti /24». Il CIDR verrà utilizzato in diverse parti dell'interfaccia Web di Firew4LL, tra cui regole firewall, NAT, IP virtuali, IPsec e route statiche.

Gli indirizzi IP o le reti, che possono essere contenuti all'interno di una singola maschera CIDR, sono noti come «riepilogo CIDR».

Quando si progetta una rete, assicurarsi che tutte le sottoreti IP private in uso in una determinata posizione siano riassumibili in CIDR. Ad esempio, se sono richieste tre sottoreti /24 in una posizione, è necessario utilizzare una rete /22 come sottorete in quattro reti /24. La tabella seguente mostra le quattro sottoreti /24 utilizzate con la sottorete 10.70.64.0/22.

Tabella 5: Riepilolo delle route CIDR

10.70.64.0/22 divisi in reti /24
10.70.64.0/24
10.70.65.0/24
10.70.66.0/24
10.70.67.0/24

Ciò mantiene il routing più gestibile per le reti multi-sito connesse a un'altra posizione fisica tramite l'uso di un circuito WAN privato o VPN. Con le sottoreti riepilogabili CIDR, una destinazione del percorso copre tutte le reti in ciascuna posizione. Senza di essa, ci sono diverse reti di destinazione diverse per posizione.

La tabella precedente è stata sviluppata utilizzando un calcolatore di rete disponibile sul sito Web https://www.subnetmask.info.

La calcolatrice converte da decimale puntato a maschera CIDR e viceversa, come mostrato nella figura *Convertitore subnet mask*. Se la *tabella delle sottoreti CIDR* fornita in questo capitolo non è disponibile, questo strumento può essere utilizzato per convertire un prefisso CIDR in notazione decimale puntata. Immettere un prefisso CIDR o una maschera decimale punteggiata e fare clic sul pulsante Calcola per trovare la conversione.

Fig. 1: Convertitore subnet mask

Immettere la maschera decimale con i punti nella sezione Calcolatore di rete/ nodo insieme a una delle reti /24. Cliccare su **Calcolare** per riempire le caselle inferiori con l'intervallo coperto da quel particolare /24, come mostrato in Figura *Calcolatore di rete/ nodo*. In questo esempio, l'indirizzo di rete è 10.70.64.0/22 e le reti utilizzabili /24 sono da 67. Il termine «Indirizzo di trasmissione» in questa tabella indica l'indirizzo più alto.

Fig. 2: Calcolatore di rete/nodo

3.5.1 Trovare una rete CIDR corrispondente

Gli intervalli IPv4 nel formato x.x.x.x-y.y.y.y sono supportati negli alias. Per gli alias di tipo rete, un intervallo IPv4 viene automaticamente convertito nel set equivalente di blocchi CIDR. Per gli alias di tipo Host, un intervallo viene convertito in un elenco di indirizzi IPv4. Vedere *Alias* per maggiori informazioni.

Se non è necessaria una corrispondenza esatta, è possibile inserire numeri nel calcolatore di rete/nodo per approssimare il riepilogo desiderato.

3.6 Domini broadcast

Un dominio broadcast è la parte di una rete che condivide lo stesso segmento di livello una rete con un singolo switch senza VLAN, il dominio di trasmissione è l'intero switch. In una rete con più switch interconnessi senza l'uso di VLAN, il dominio di trasmissione include tutti questi switch.

Un singolo dominio di trasmissione *può* contenere più di una sottorete IPv4 o IPv6, che generalmente non è considerata un buon progetto di rete. Le sottoreti IP devono essere separate in domini di trasmissione separati tramite switch o VLAN separati. L'eccezione è l'esecuzione di reti IPv4 e IPv6 all'interno di un singolo dominio di trasmissione.

Questo processo si chiama dual stack ed è una tecnica comune e utile che utilizza la connettività IPv4 e IPv6 per gli host.

I domini di trasmissione possono essere combinati collegando insieme due interfacce di rete, ma è necessario prestare attenzione per evitare loop di commutazione. Esistono anche alcuni proxy per determinati protocolli che non combinano domini di trasmissione ma producono lo stesso effetto di rete, come un relè DHCP che inoltra le richieste DHCP in un dominio di trasmissione su un'altra interfaccia. Ulteriori informazioni sui domini di trasmissione e su come combinarli sono disponibili in *Bridging*.

3.7 IPv6

3.7.1 Basi

IPv6 consente uno spazio di indirizzi IP esponenzialmente maggiore rispetto a IPv4. IPv4 utilizza un indirizzo a 32 bit, che consente 2^{32} o oltre 4 miliardi di indirizzi, meno se vengono rimossi i blocchi riservati considerevoli e gli IP masterizzati dalla sottorete. IPv6 utilizza un indirizzo a 128 bit, ovvero 2^{128} o 3.403 x 10^{38} indirizzi IP. La sottorete IPv6 di dimensioni standard definita da IETF è a /64, che contiene 2^{64} IP o 18,4 *quintilioni* di indirizzi. L'intero spazio IPv4 può adattarsi più volte all'interno di una tipica sottorete IPv6 con spazio libero.

Uno dei miglioramenti più sottili con IPv6 è che nessun indirizzo IP viene perso nella sottorete. Con IPv4, vengono persi due indirizzi IP per sottorete per tenere conto di una route nulla e per trasmettere l'indirizzo IP. In IPv6, la trasmissione viene gestita tramite gli stessi meccanismi utilizzati per il multicast che coinvolge indirizzi speciali inviati all'intero segmento di rete. Ulteriori miglioramenti includono la crittografia integrata dei pacchetti, dimensioni di pacchetti potenziali maggiori e altri elementi di progettazione che semplificano la gestione di IPv6 da parte dei router a livello di pacchetto.

A differenza di IPv4, tutti i pacchetti vengono instradati in IPv6 senza NAT. Ogni indirizzo IP è direttamente accessibile da un altro a meno che non sia bloccato da un firewall. Questo può essere un concetto molto difficile da comprendere per le persone che sono abituate a far esistere la propria LAN con una specifica sottorete privata e quindi eseguire NAT a qualunque indirizzo esterno.

Esistono differenze fondamentali nel funzionamento di IPv6 rispetto a IPv4, ma principalmente sono solo queste. Alcune cose sono più semplici di IPv4, altre sono leggermente più complicate, ma per la maggior parte sono semplicemente diverse. Le principali differenze si verificano al livello 2 (ARP contro NDP ad esempio) e al livello 3 (indirizzamento IPv4 vs. IPv6). I protocolli utilizzati ai livelli superiori sono identici; è cambiato solo il meccanismo di trasporto per tali protocolli. HTTP è ancora HTTP, SMTP è ancora SMTP, ecc.

3.7.2 Considerazioni per Firewall e VPN

IPv6 ripristina la vera connettività peer-to-peer originariamente in atto con IPv4, rendendo ancora più importanti i controlli appropriati del firewall. In IPv4, il NAT è stato utilizzato in modo improprio come controllo firewall aggiuntivo. In IPv6, il NAT viene rimosso. Le porte forward non sono più richieste in IPv6, pertanto l'accesso remoto verrà gestito dalle regole del firewall. È necessario assicurarsi che il traffico VPN da LAN a LAN crittografato non venga instradato direttamente al sito remoto. Consulta le *Regole firewall e VPN con IPv6* per una discussione più approfondita sulle preoccupazioni relative al firewall IPv6 per quanto riguarda il traffico VPN.

3.7.3 Requisiti

IPv6 richiede una rete abilitata per IPv6. La connettività IPv6 fornita direttamente da un ISP è l'ideale. Alcuni ISP implementano una configurazione dual stack in cui IPv4 e IPv6 vengono consegnati contemporaneamente sullo stesso trasporto. Altri ISP utilizzano tipi di tunneling o distribuzione per fornire indirettamente IPv6. È anche possibile utilizzare un fornitore di terze parti come il servizio di tunnelbroker di Hurricane Electric.

Oltre al servizio, il software deve supportare anche IPv6. Firew4LL supporta IPv6 dalla versione 2.1. Anche i sistemi operativi e le applicazioni client devono supportare IPv6. Molti sistemi operativi e applicazioni comuni lo supportano senza problemi. Microsoft Windows supporta IPv6 in stato pronto per la produzione dal 2002 sebbene le versioni più recenti lo gestiscano molto meglio. OS X supporta IPv6 dal 2001 con la versione 10.1 «PUMA». Sia FreeBSD che Linux lo supportano nel sistema operativo. La maggior parte dei browser Web e dei client di posta elettronica supporta IPv6, così come le versioni recenti di altre applicazioni comuni. Per garantire l'affidabilità, è sempre utile utilizzare gli ultimi aggiornamenti.

Alcuni sistemi operativi mobili hanno diversi livelli di supporto per IPv6. Android e iOS supportano entrambi IPv6, ma Android supporta solo la configurazione automatica senza stato per ottenere un indirizzo IP e non DHCPv6. IPv6 fa parte delle specifiche LTE, quindi qualsiasi dispositivo mobile che supporta reti LTE supporta anche IPv6.

3.7.4 Tipi di WAN IPv6

I dettagli sono disponibili nei *tipi di WAN IPv6*, ma alcuni dei modi più comuni per distribuire IPv6 sono:

- **Indirizzamento statico** Nativo e utilizzo di IPv6 da solo o in una configurazione a doppio stack insieme a IPv4.
- **DHCPv6** Indirizzo ottenuto automaticamente da DHCPv6 a un server upstream. La delega del prefisso può anche essere utilizzata con DHCPv6 per recapitare una sottorete indirizzata a un client DHCPv6.
- **(SLAC)Configurazione automatica dell'indirizzo senza stato** Determina automaticamente l'indirizzo IPv6 consultando i messaggi d'annuncio del router e generando un indirizzo IP all'interno di un prefisso. Questo non è molto utile per un router, in quanto non è possibile instradare una rete per «l'interno» del firewall. Può essere utile per le modalità dell'appliance.
- **Tunnel 6RD** Metodo di tunneling del traffico IPv6 all'interno di IPv4. Viene utilizzato dagli ISP per una rapida implementazione di IPv6.
- **Tunnel 6to4** Simile al 6RD ma con diversi meccanismi e limitazioni.
- **Tunnel GIF** Tecnicamente non è un tipo di WAN diretto, ma è comunemente usato. Il cliente costruisce un tunnel GIF IPv4 a un

provider per il tunneling del traffico IPv6.

Sebbene non sia tecnicamente un tipo di WAN, la connettività IPv6 può anche essere organizzata su OpenVPN o IPsec con IKEv2. OpenVPN e IPsec in modalità IKEv2 possono trasportare contemporaneamente il traffico IPv4 e IPv6, quindi possono fornire IPv6 su IPv4, anche se con un overhead maggiore rispetto a un tipico broker tunnel che utilizza GIF. Queste sono buone opzioni per un'azienda che ha IPv6 in un datacenter o in un ufficio principale ma non in una posizione remota.

3.7.5 Formato degli indirizzi

Un indirizzo IPv6 è composto da 32 cifre esadecimali, in 8 sezioni di 4 cifre ciascuna, separate da due punti. Sembra qualcosa del genere: *1234:5678:90ab:cdef:1234:5678:90ab:cdef*

Gli indirizzi IPv6 hanno diverse scorciatoie che consentono loro di essere compressi in stringhe più piccole seguendo determinate regole. Se in una sezione sono presenti zero iniziali, è possibile che vengano tralasciati. *0001:0001:0001:0001:0001:0001:0001:0001* potrebbe essere scritto come *1:1:1:1:1:1:1:1*.

È possibile comprimere un numero qualsiasi di parti di indirizzo costituite solo da zero utilizzando *::* ma ciò può essere eseguito una sola volta in un indirizzo IPv6 per evitare ambiguità. Un buon esempio di ciò è l'host locale, comprimendo *0000:0000:0000:0000:0000:0000:0000:0001* a *::1*. Ogni volta *::* che appare in un indirizzo IPv6, i valori tra tutti sono zero. Un indirizzo IP come *fe80:1111:2222:0000:0000:0000:7777:8888*, può essere rappresentato come *fe80:1111:2222::7777:8888*. Tuttavia, *fe80:1111:0000:0000:4444:0000:0000:8888* non può essere abbreviato utilizzando *::* più di una volta. Sarebbe o *fe80:1111::4444:0:0:8888* o *fe80:1111:0:0:4444::8888* ma *non può* essere *fe80:1111::4444::8888* perché non c'è modo di dire quanti zero sono stati sostituiti da uno dei due operatori *::* .

Determinazione di uno schema di indirizzamento IPv6

A causa della maggiore lunghezza degli indirizzi, dell'ampio spazio disponibile anche in una sottorete di base /64 e della possibilità di utilizzare cifre esadecimali, c'è più libertà nel progettare gli indirizzi di rete dei dispositivi.

Sui server che utilizzano più alias di indirizzi IP per host virtuali, jail, ecc., Uno schema di indirizzamento utile consiste nell'utilizzare la settima sezione dell'indirizzo IPv6 per indicare il server. Quindi utilizzare l'ottava sezione per i singoli alias IPv6. Questo raggruppa tutti gli IP in un singolo host riconoscibile. Ad esempio, il server stesso sarebbe *2001:db8:1:1::a:1* e quindi il primo alias IP sarebbe *2001:db8:1:1::a:2*, quindi * *2001:db8:1:1::a:3*, ecc. Il prossimo server sarebbe *2001:db8:1:1::b:1* e ripete lo stesso schema. Ad alcuni amministratori piace divertirsi con i loro indirizzi IPv6 usando lettere esadecimali e numeri/lettere equivalenti per ricavare parole dai loro indirizzi IP. Gli *elenchi di parole esadecimali sul Web* possono essere utilizzati per creare indirizzi IP più memorabili come *2001:db8:1:1::dead:beef*.

Confusione decimale vs esadecimale

La creazione di indirizzi IPv6 consecutivi con una base esadecimale può causare confusione. I valori esadecimali sono a base differenza dei valori decimali che sono a base 10. Ad esempio, l'indirizzo IPv6 *2001:db8:1:1::9* è seguito da *2001:db8:1:1::a*, *non 2001:db8:1:1::10*. Andando a destra fino al *2001:db8:1:1::10*, i valori a-f sono stati saltati, lasciando un vuoto. Non sono richiesti schemi di numerazione consecutivi e il loro utilizzo è a discrezione del progettista della rete. Per alcuni è psicologicamente più semplice evitare di usare le cifre esadecimali.

Dato che tutti gli indirizzi IPv4 possono essere espressi in formato IPv6, questo problema si presenta quando si progetta una rete dual stack che mantiene una sezione dell'indirizzo IPv6 uguale alla sua controparte IPv4.

3.7.6 Sottorete IPv6

La sottorete IPv6 è più semplice della IPv4. Ma è anche diversa. Vuoi dividere o combinare una sottorete? Tutto ciò che serve è aggiungere o tagliare le cifre e regolare la lunghezza del prefisso di un multiplo di quattro. Non è più necessario calcolare gli indirizzi di inizio/fine della sottorete, gli indirizzi utilizzabili, il percorso nullo o l'indirizzo di trasmissione.

IPv4 aveva una subnet mask (notazione quadrata tratteggiata) che è stata successivamente sostituita dal mascheramento CIDR. IPv6 non ha una subnet mask ma la chiama lunghezza del prefisso, spesso abbreviata in «Prefisso». La lunghezza del prefisso e il mascheramento CIDR funzionano in modo simile; La lunghezza del prefisso indica quanti bit dell'indirizzo definiscono la rete in cui esiste. Più comunemente, i prefissi utilizzati con IPv6 sono multipli di quattro, come si vede nella tabella *Tabella delle sottoreti IPv6*, ma possono essere qualsiasi numero compreso tra 0 e 128.

L'uso di lunghezze di prefisso in multipli di quattro consente a di distinguere più facilmente le sottoreti IPv6. Tutto ciò che serve per progettare una sottorete più grande o più piccola è regolare il prefisso di multipli di quattro. Per riferimento, vedere la tabella *Tabella delle sottoreti IPv6* che elenca i possibili indirizzi IPv6, nonché il numero di indirizzi IP contenuti all'interno di ciascuna sottorete.

Tabella 6: Tabella delle sottoreti IPv6

Prefisso	Esempio della sottorete	Indirrizzi IP totali	# di reti /64
4	x:	2 124	2 60
8	xx:	2 120	2 56
12	xxx:	2 116	2 52
16	xxxx:	2 112	2 48
20	xxxx:x:	2 108	2 44
24	xxxx:xx:	2 104	2 40

Continua alla pagina successiva

Tabella 2 – continua dalla pagina precedente

Prefisso	Esempio della sottorete	Indirizzi IP totali	# di reti /64
28	xxxx:xxx:	2 100	2 36
32	xxxx:xxxx:	2 96	4,294,967,296
36	xxxx:xxxx:x:	2 92	268,435,456
40	xxxx:xxxx:xx:	2 88	16,777,216
44	xxxx:xxxx:xxx:	2 84	1,048,576
48	xxxx:xxxx:xxxx:	2 80	65,536
52	xxxx:xxxx:xxxx:x:	2 76	4,096
56	xxxx:xxxx:xxxx:xx:	2 72	256
60	xxxx:xxxx:xxxx:xxx:	2 68	16
64	xxxx:xxxx:xxxx:xxxx:	2 64 (18,446,744,073,709,551,616)	1
68	xxxx:xxxx:xxxx:xxxx:x:	2 60 (1,152,921,504,606,846,976)	0
72	xxxx:xxxx:xxxx:xxxx:xx:	2 56 (72,057,594,037,927,936)	0
76	xxxx:xxxx:xxxx:xxxx:xxx:	2 52 (4,503,599,627,370,496)	0
80	xxxx:xxxx:xxxx:xxxx:xxxx:	2 48 (281,474,976,710,656)	0
84	xxxx:xxxx:xxxx:xxxx:xxxx:x:	2 44 (17,592,186,044,416)	0
88	xxxx:xxxx:xxxx:xxxx:xxxx:xx:	2 40 (1,099,511,627,776)	0
92	xxxx:xxxx:xxxx:xxxx:xxxx:xxx:	2 36 (68,719,476,736)	0
96	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:	2 32 (4,294,967,296)	0
100	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:x:	2 28 (268,435,456)	0
104	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xx:	2 24 (16,777,216)	0
108	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx:	2 20 (1,048,576)	0
112	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:	2 16 (65,536)	0
116	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:x:	2 12 (4,096)	0
120	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xx:	2 8 (256)	0
124	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxx:	2 4 (16)	0
128	xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx	2 0 (1)	0

Una /64 è una sottorete IPv6 di dimensioni standard definita dall'IETF. È la sottorete più piccola che può essere utilizzata localmente se si desidera la configurazione automatica.

In genere, un ISP assegna una sottorete /64 o inferiore per stabilire il servizio sulla WAN. Una rete aggiuntiva viene instradata per l'uso della LAN. La dimensione dell'allocazione dipende dall'ISP, ma non è raro vedere gli utenti finali ricevere almeno un /64 e persino fino a /48.

Un fornitore di servizi di tunnel come tunnelbroker.net gestito da Hurricane Electric assegnerà un /48 oltre a un percorso di sottorete /64 e interconnessione a /64.

Le assegnazioni superiori a /64 di solito adottano il primo /64 per LAN e suddividono il resto per requisiti come tunnel VPN, DMZ o una rete ospite.

3.7.7 Sottoreti IPv6 speciali

Le reti per uso speciale sono riservate a IPv6. Un elenco completo di questi può essere trovato nell'articolo Wikipedia IPv6. Sei esempi di reti speciali IPv6 e i loro indirizzi sono mostrati di seguito in *Reti e indirizzi speciali con IPv6*.

Tabella 7: Reti e indirizzi speciali con IPv6

Rete	Scopo
2001:db8::/32	Prefisso di documentazione, usato per esempi, come quelli che si trovano in questo libro.
::1	Host locale
fc00::/7	Indirizzi locali univoci (ULA), noti anche come indirizzi IPv6 «privati».
fe80::/10	Link Indirizzi locali, validi solo all'interno di un singolo dominio di trasmissione.
2001::/16	Indirizzi unici globali (Global Unique Addresses, GUA): indirizzi IPv6 instradabili.
ff00::0/8	Indirizzi multicast

3.7.8 NDP (Neighbor Discovery Protocol)

Gli host IPv4 si trovano su un segmento locale che usa i messaggi di trasmissione ARP, ma gli host IPv6 si trovano inviando messaggi NDP (Neighbor Discovery Protocol). Come ARP, NDP funziona all'interno di un determinato dominio di trasmissione per trovare altri host all'interno di una sottorete specifica.

Inviando pacchetti ICMPv6 speciali a indirizzi multicast riservati, NDP gestisce le attività di rilevamento dei vicini, sollecitazioni del router e reindirizzamenti del percorso simili ai reindirizzamenti ICMP di IPv4.

Firew4LL aggiunge automaticamente le regole del firewall su interfacce abilitate per IPv6 che consentono a NDP di funzionare. Tutti gli attuali vicini noti su IPv6 possono essere visualizzati nella GUI del firewall in **Diagnostica>Tabella NDP**.

3.7.9 (RA)Router Advertisements

I router IPv6 si trovano tramite i messaggi d'annuncio del router (Router Advertisement, RA) anziché tramite il DHCP. I router abilitati per IPv6 che supportano l'assegnazione di indirizzi dinamici dovrebbero annunciarsi sulla rete a tutti i client e rispondere alle richieste del router. Quando agisce come client (interfacce WAN), Firew4LL accetta i messaggi RA dai router upstream. Quando funge da router, Firew4LL fornisce messaggi RA ai client sulle sue reti interne. Vedere *Annunci router (oppure: «Dov'è l'opzione gateway DHCPv6»)* per maggiori dettagli.

3.7.10 Allocazione dell'indirizzo

Gli indirizzi client possono essere allocati con indirizzamento statico tramite SLAAC (*Annunci router (oppure: «Dov'è l'opzione gateway DHCPv6»)*), DHCP6 (*Server DHCP IPv6 e annunci router*) o altri metodi di tunneling come OpenVPN.

Delega del prefisso DHCP6

La delegazione del prefisso DHCP6 consegna una sottorete IPv6 a un client DHCP6. Un'interfaccia di tipo WAN può essere impostata per ricevere un prefisso su DHCP6 (*DHCP6, interfaccia di traccia*). Un router funzionante ai margini di una rete di grandi dimensioni può fornire la delegazione dei prefissi ad altri router all'interno della rete (*Delegazione dei prefissi DHCPv6*).

3.7.11 IPv6 e NAT

Sebbene IPv6 elimini la maggior parte delle esigenze del NAT, esistono rare situazioni che richiedono l'uso di NAT con IPv6 come Multi-WAN per IPv6 su reti residenziali o di piccole imprese.

Gone è il tipo tradizionale di NAT (PAT) tradotto con brutte porte in cui gli indirizzi interni vengono tradotti usando le porte su un singolo indirizzo IP esterno. È sostituito da una traduzione diretta dell'indirizzo di rete chiamata Traduzione dei prefissi di rete (Network Prefix Translation, NPT). Questo è disponibile in Firew4LL in **Firewall>NAT** nella scheda NPt. NPt traduce un prefisso in un altro. Quindi *2001:db8:1111:2222::/64* si traduce in * *2001:db8:3333:4444::/64*. Sebbene il prefisso cambi, il resto dell'indirizzo sarà identico per un determinato host su quella sottorete. Per ulteriori informazioni su NPt, vedere *Traduzione dei prefissi di rete IPv6, (NPt)*.

Esiste un meccanismo integrato in IPv6 per accedere agli host IPv4 utilizzando una notazione di indirizzo speciale, come *::ffff:192.168.1.1*. Il comportamento di questi indirizzi può variare tra sistema operativo e applicazione ed è inaffidabile.

3.7.12 IPv6 e Firew4LL

Salvo diversamente specificato, si può presumere che IPv6 sia supportato da Firew4LL in una determinata area o funzionalità.

Alcune aree degne di nota di Firew4LL che non supportano IPv6 sono: Captive Portal e la maggior parte dei provider DynDNS.

Per consentire IPv6:

- Passare a `Sistema>Avanzate` nella scheda `Rete`
- Selezionare `Consentire IPv6`
- Fare clic su `Salvare`

Pacchetti di Firew4LL

Alcuni pacchetti sono gestiti dalla community, quindi il supporto IPv6 varia. Nella maggior parte dei casi, il supporto IPv6 dipende dalle capacità del software sottostante. È sicuro supporre che un pacchetto non supporti IPv6 se non diversamente specificato. I pacchetti vengono aggiornati periodicamente, pertanto è consigliabile testare un pacchetto per determinare se supporta IPv6.

3.7.13 Connessione con un servizio Tunnel Broker

Una posizione che non ha accesso alla connettività IPv6 nativa può ottenerla utilizzando un servizio di broker di tunnel come Hurricane Electric. Un sito principale con IPv6 può fornire la connettività IPv6 a un sito remoto utilizzando un tunnel VPN o GIF.

Questa sezione fornisce la procedura per il collegamento di Firew4LL con Hurricane Electric (spesso abbreviato in HE.net o HE) per il transito IPv6. L'uso di HE.net è semplice e facile. Consente l'impostazione multi-tunnel, ciascuno con un trasporto /64 e un percorso /64. Inoltre è incluso un instradato /48 da utilizzare con uno dei tunnel. È un ottimo modo per ottenere molto spazio IPv6 indirizzato per sperimentare e imparare, il tutto gratuitamente.

Iscriviti al servizio

Prima di poter creare un tunnel, le richieste di eco ICMP devono essere concesse alla WAN. Una regola per passare richieste di eco ICMP da una fonte qualsiasi è una buona misura temporanea. Una volta scelto il punto finale del tunnel per HE.net, la regola può essere resa più specifica.

Per iniziare su HE.net, registrati su www.tunnelbroker.net. Le reti /64 vengono allocate dopo la registrazione e la selezione di un server tunnel IPv6 regionale. Un riepilogo della configurazione del tunnel può essere visualizzato sul sito Web di HE.net come mostrato nella figura *Riepilogo di configurazione del tunnel HE.net*. Contiene informazioni importanti come l'"**ID tunnel** dell'utente, l'"**indirizzo IPv4 del server** (indirizzo IP del server tunnel), l'"**indirizzo IPv4**

del client (l'indirizzo IP esterno del firewall), il **server** e gli **indirizzi IPv6 del client** (che rappresentano gli indirizzi IPv6 all'interno del tunnel), e i **prefissi IPv6 instradati**.

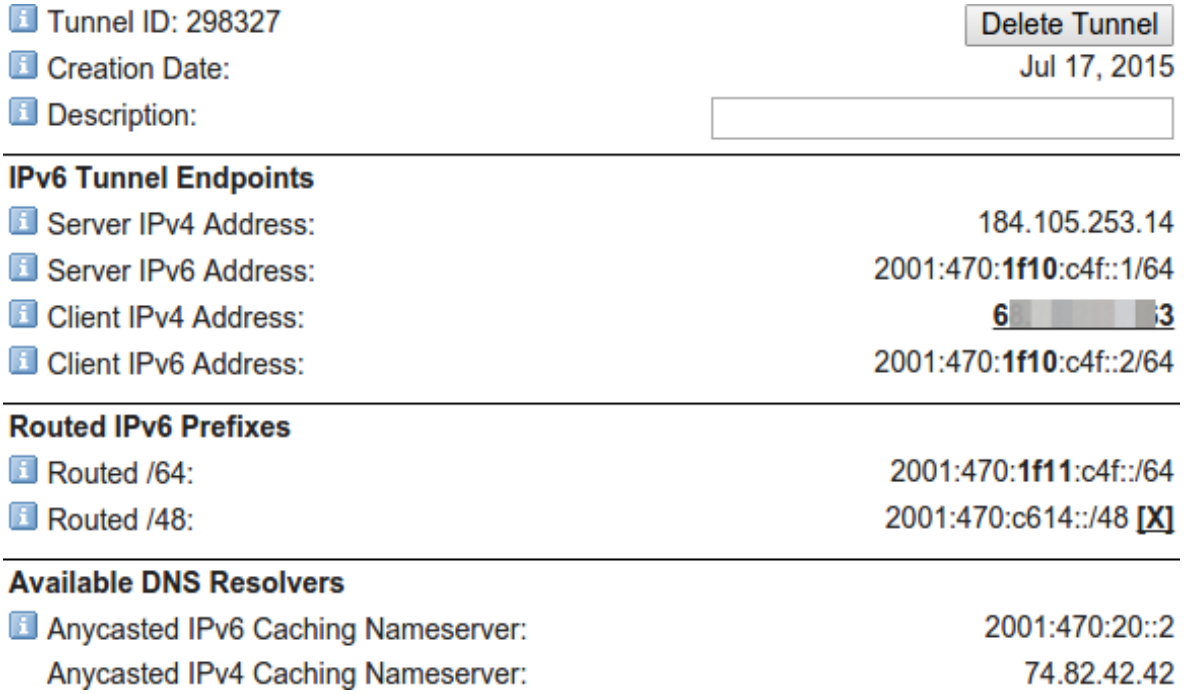


Fig. 3: Riepilogo di configurazione del tunnel HE.net

La scheda **Avanzate** sul sito del broker del tunnel ha due ulteriori opzioni degne di nota: un cursore MTU e una chiave di aggiornamento per l'aggiornamento dell'indirizzo del tunnel. Se utilizzata per terminare il tunnel GIF è PPPoE o un altro tipo di WAN con un MTU basso, spostare il cursore verso il basso in base alle esigenze. Ad esempio, un MTU comune per le linee PPPoE con un broker tunnel sarebbe 1452. Se la WAN ha un indirizzo IP dinamico, prendere nota della **chiave di aggiornamento** per un uso successivo in questa sezione.

Una volta completata la configurazione iniziale per il servizio tunnel, configurare Firew4LL per utilizzare il tunnel.

Permettere il traffico IPv6

Per abilitare il traffico IPv6, procedere come segue:

- Passare a **Sistema>Avanzate** nella scheda **Rete**
- Selezionare **Consentire IPv6** se non è già selezionato
- Fare clic su **Salvare**

Permettere ICMP

Le richieste di echo ICMP devono essere consentite sull'indirizzo WAN che sta terminando il tunnel per assicurarsi che sia online e raggiungibile. Se l'ICMP è bloccato, il broker del tunnel potrebbe rifiutare di impostare il tunnel sull'indirizzo IPv4. Modificare la regola ICMP creata in precedenza in questa sezione o creare una nuova regola per consentire le richieste di eco ICMP. Impostare l'indirizzo IP di origine **dell'indirizzo IPv4 del server** nella configurazione del tunnel, come mostrato nella figura *Esempio di regola ICMP* per garantire la connettività.

Fig. 4: Esempio di regola ICMP

Creare e assegnare l'interfaccia GIF

Prossimo passaggio, creare l'interfaccia per il tunnel GIF in Firew4LL. Completare i campi con le informazioni corrispondenti dal riepilogo della configurazione del broker tunnel.

- Passa a **Interfacce>** (assegnare) nella scheda **GIF**.
- Fare clic su  **Aggiungi** per aggiungere una nuova voce.
- Impostare **l'interfaccia primaria** sulla WAN in cui termina il tunnel. Questa sarebbe la WAN che ha l'**indirizzo IPv4 del client** sul broker del tunnel.
- Impostare **l'indirizzo remoto GIF** in Firew4LL sull'**indirizzo IPv4 del server** nel riepilogo.
- Impostare **l'indirizzo locale del tunnel** GIF in Firew4LL sull'**indirizzo IPv6 del client** nel riepilogo.
- Impostare **l'indirizzo remoto del tunnel GIF** in Firew4LL sull'**indirizzo IPv6 del server** nel riepilogo, insieme alla lunghezza del prefisso (in genere /64).
- Lasciare le opzioni rimanenti vuote o deselezionate.
- Immettere una **descrizione**.
- Fare clic su **Salvare**.

Vedere la figura *Esempio di tunnel GIF*.

Se questo tunnel viene configurato su una WAN con un IP dinamico, consultare *Aggiornamento del punto finale del tunnel* per informazioni su come mantenere aggiornato l'IP del punto finale del tunnel con HE.net.

Una volta creato, il tunnel GIF deve essere assegnato:

- Passare a **Interfacce>** (**assegnare**), scheda **Assegnazioni interfaccia**.
- Selezionare la GIF appena creata in **Porte di rete disponibili**.
- Fare clic su  **Aggiungere** per aggiungerlo come nuova interfaccia.

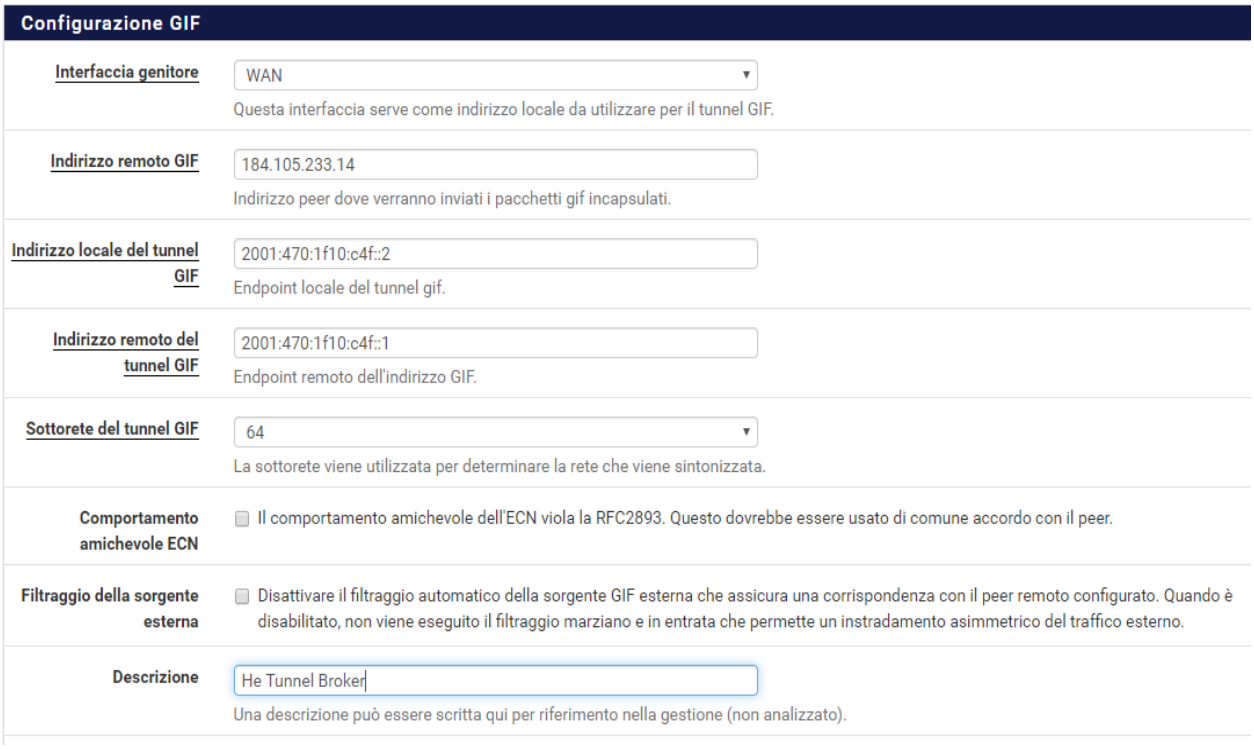


Fig. 5: Esempio di tunnel GIF

Configurare la nuova interfaccia OPT

La nuova interfaccia è ora accessibile in **Interfacce**>**OPTx**, dove x dipende dal numero assegnato all'interfaccia.

- Passare alla pagina di configurazione della nuova interfaccia. (**Interfacce> OPTx**)
- Selezionare **Abilitare interfaccia**.
- Immettere un nome per l'interfaccia nel campo **Descrizione**, ad esempio *WANv6*.
- Lasciare il **tipo di configurazione IPv6** come Nessuno.
- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**.

Configurare il gateway IPv6

Quando l'interfaccia è configurata come detto sopra, un gateway IPv6 dinamico viene aggiunto automaticamente, ma non è ancora contrassegnato come predefinito.

- Passare a **Sistema> Routing**
- Modificare il gateway IPv6 dinamico con lo stesso nome della WAN IPv6 creata sopra.
- Controllare il **gateway predefinito**.
- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**.

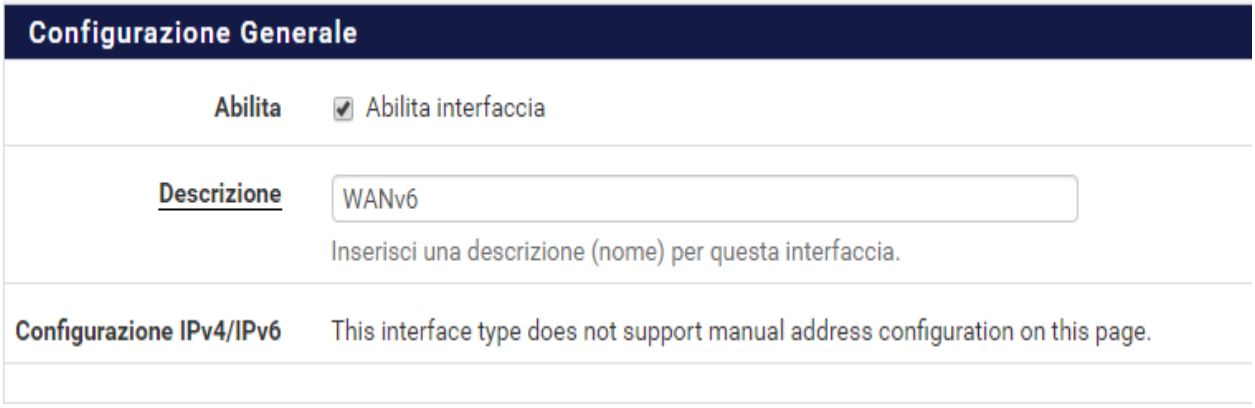


Fig. 6: Esempio dell'interfaccia del tunnel

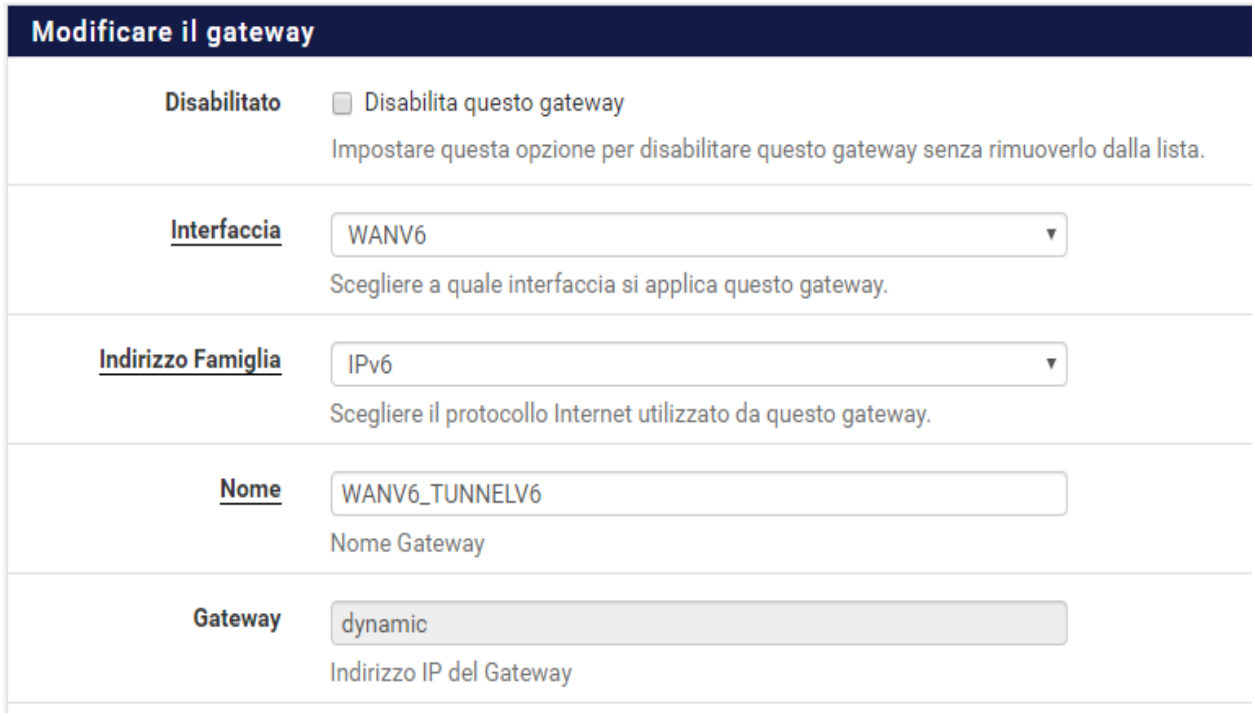


Fig. 7: Esempio del gateway del tunnel

Passare a **Stato> Gateway** per visualizzare lo stato del gateway. Il gateway verrà visualizzato come «Online» se la configurazione ha esito positivo, come mostrato nella figura *Esempio di stato del tunnel del gateway*.

Fig. 8: Esempio di stato del tunnel del gateway

Impostare DNS con IPv6

È probabile che i server DNS rispondano alle query DNS con risultati AAAA. Si consiglia di immettere i server DNS forniti dal servizio broker tunnel in **Sistema>Impostazione generale**. Inserisci almeno un server DNS con IPv6 o utilizza i server DNS con IPv6 pubblici di Google al 2001:4860:4860::8888 e 2001:4860:4860::8844. Se il Resolutore del DNS viene utilizzato in modalità senza inoltro, parlerà automaticamente con i server root IPv6 quando la connettività IPv6 sarà funzionale.

Impostare LAN con IPv6

Una volta configurato e online il tunnel, il firewall stesso ha la connettività IPv6. Per garantire che i client possano accedere a Internet su IPV6, è necessario configurare anche

Un metodo consiste nell'impostare come dual stack IPv4 e IPv6.

- Passare a **Interfacce>LAN**
- Selezionare **Tipo di configurazione IPv6** come **IPv6 statico**
- Immettere un indirizzo IPv6 da **Routed /64** nella configurazione del broker tunnel con una lunghezza prefisso di 64. Ad esempio, *2001:db8:1111:2222::1* per l'indirizzo IPv6 LAN se **Routed /64** è *2001:db8:1111:2222::/64*.
- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**

A /64 dall'interno del Routed /48 è un'altra opzione disponibile.

Impostare annunci del DHCPv6 e/o del router

Per assegnare automaticamente gli indirizzi IPv6 ai client, impostare Annunci router e/o DHCPv6. Questo argomento è trattato in dettaglio in *Annunci server e router DHCP IPv6*.

Una breve panoramica è la seguente:

- Passare a **Servizi>DHCPv6 Server/RA**
- Selezionare **Abilitare**
- Inserire un intervallo di indirizzi IP IPv6 all'interno della nuova sottorete IPv6 LAN
- Selezionare **Salvare**.
- Passare alla scheda **Annunci router**
- Impostare la **modalità** su *Gestito* (solo DHCPv6) o *Assistito* (DHCPv6 + SLAAC)
- Selezionare **Salvare**.

Le modalità sono descritte più dettagliatamente in *Annunci del router (oppure: «Dov'è l'opzione gateway DHCPv6»)*.

Per assegnare manualmente gli indirizzi IPv6 ai sistemi LAN, utilizzare l'indirizzo IPv6 LAN del firewall come gateway con una lunghezza del prefisso corrispondente adeguata e selezionare gli indirizzi all'interno della sottorete LAN

Aggiungere regole firewall

Dopo aver assegnato gli indirizzi LAN, aggiungere le regole del firewall per consentire il flusso del traffico IPv6.

- Passare a **Firewall>Regole**, scheda **LAN**.
- Controllare l'elenco per una regola IPv6 esistente. Se esiste già una regola per il passaggio del traffico IPv6, non è necessaria alcuna azione aggiuntiva.
- Fare click su  **Aggiungere** per aggiungere una nuova regola in fondo all'elenco
- Impostare la versione **TCP/IP** su *IPv6*
- Immettere la sottorete LAN IPv6 come **Origine**
- Scegli una **destinazione** per *qualsiasi*.

- Fai clic su **Salvare**
- Fai clic su **Applicare modifiche**

Per i server abilitati per IPv6 sulla LAN con servizi pubblici, aggiungere le regole del firewall nella scheda per 6 (l'interfaccia GIF assegnata) per consentire al traffico IPv6 di raggiungere i server sulle porte richieste.

Provalo!

Una volta stabilite le regole del firewall, verificare la connettività IPv6. Un buon sito con cui fare una prova è test-ipv6.com. Un esempio dei risultati di output di una corretta configurazione da un client su LAN è mostrato nella figura *Risultati del test IPv6*.

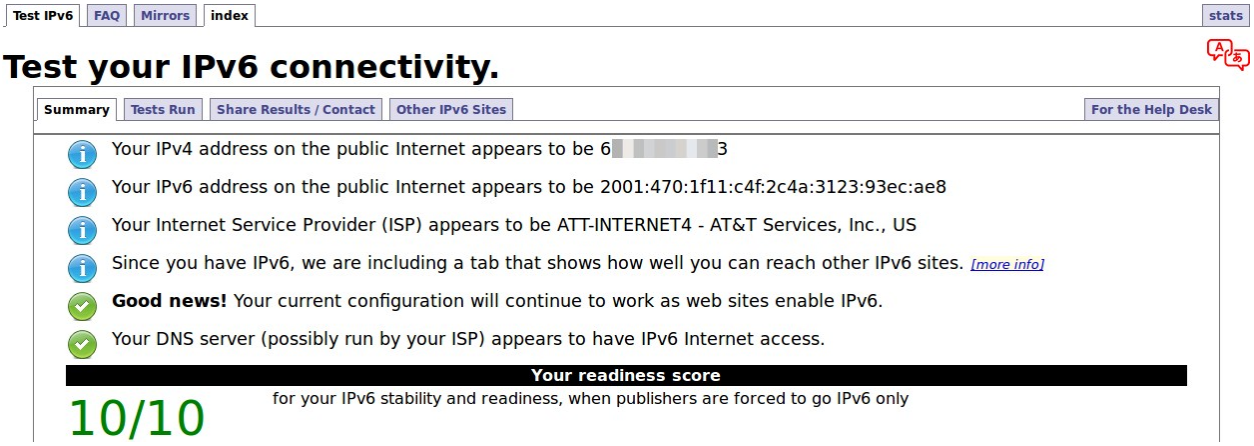


Fig. 9: Risultati test IPv6

Aggiornamento dell'endpoint del tunnel

Per una WAN dinamica, come DHCP o PPPoE, HE.net può ancora essere utilizzato come broker tunnel. Firew4LL include un tipo DynDNS che aggiornerà l'indirizzo IP dell'endpoint del tunnel ogni volta che cambia l'IP dell'interfaccia WAN.

Se si desidera DynDNS, può essere configurato come segue:

- Passare a **Servizi>DynDNS**
- Fare click su  **Aggiungere** per aggiungere una nuova voce.
- Impostare il tipo di servizio su HE.net Tunnelbroker.
- Selezionare WAN come **interfaccia da monitorare**.
- Immettere l'**ID tunnel** dalla configurazione del broker tunnel nel campo **Hostname**.
- Immettere il **nome utente** per il sito del broker di tunnel.
- Immettere la **password** o la **chiave di aggiornamento** per il sito del broker di tunnel nel campo **Password**.
- Immettere una **descrizione**.
- Fare clic su **Salvare e forzare aggiornamento**.

Se e quando l'indirizzo IP WAN cambia, Firew4LL si aggiorna automaticamente il broker del tunnel.

3.7.14 Controllo della preferenza IPv6 per il traffico dal firewall

Per impostazione predefinita, Firew4LL preferirà IPv6 quando configurato. Se il routing IPv6 non funziona ma il sistema lo ritiene, Firew4LL potrebbe non controllare gli aggiornamenti o scaricare i pacchetti correttamente.

Per modificare questo comportamento, Firew4LL fornisce un metodo nella GUI per controllare se i servizi sul firewall preferiscono IPv4 su IPv6:

- Passare a **Sistema>Avanzate** nella **scheda di Rete**
- Selezionare **Preferisci utilizzare IPv4 anche se IPv6 è disponibile**
- Fai clic su **Salvare**

Una volta salvate le impostazioni, il firewall stesso preferirà IPv4 per la comunicazione in uscita.

In tutto il mondo, la disponibilità di nuovi indirizzi IPv4 è in calo. La quantità di spazio libero varia a seconda della regione, ma alcuni hanno già esaurito le allocazioni e altri si stanno rapidamente avvicinando ai loro limiti. Al 31 gennaio 2011, IANA ha assegnato tutto il suo spazio ai registri Internet regionali (RIR). A loro volta, queste allocazioni RIR si sono esaurite in alcune località come APNIC (Asia/Pacifico), RIPE (Europa) e LACNIC (America Latina e Caraibi) per reti /8. Sebbene siano ancora disponibili alcune allocazioni più piccole, è sempre più difficile ottenere un nuovo spazio di indirizzi IPv4 in queste aree. ARIN (Nord America) si è esaurito il 24 settembre 2015. Per tenere conto di ciò, IPv6 è stato creato in sostituzione di IPv4. Disponibile in alcune forme dagli anni “90, fattori come l’inerzia, la complessità e i costi di sviluppo o acquisto di router e software compatibili hanno rallentato la sua diffusione fino agli ultimi anni. Anche allora, è stato piuttosto lento con solo l’8% degli utenti di Google con connettività IPv6 entro luglio 2015.

Nel corso degli anni, il supporto per IPv6 in software, sistemi operativi e router è migliorato, quindi la situazione è pronta per migliorare. Tuttavia spetta agli ISP iniziare a fornire agli utenti la connettività IPv6. È una situazione da 22: i fornitori di contenuti sono lenti a fornire IPv6 perché pochi utenti ce l’hanno. Nel frattempo, gli utenti non ce l’hanno perché non c’è molto contenuto IPv6 e ancora meno contenuto disponibile solo su IPv6. Gli utenti non sanno di averne bisogno, quindi non richiedono il servizio dai loro ISP.

Alcuni provider stanno sperimentando *Carrier Grade NAT* (CGN) per estendere ulteriormente le loro reti IPv4. CGN colloca i propri clienti residenziali IPv4 dietro un altro livello di NAT, rompendo ulteriormente i protocolli che già non gestiscono uno strato di NAT. I fornitori di dati mobili lo fanno da tempo, ma le applicazioni che si trovano in genere sui dispositivi mobili non sono interessate dal momento che funzionano come se fossero dietro un tipico NAT in stile router SOHO. Mentre risolve un problema, ne crea altri come osservato quando CGN viene utilizzato come WAN di un firewall, durante il tethering su un PC o in alcuni casi tentando di utilizzare una VPN IPsec tradizionale senza NAT-T o PPTP. Gli ISP che impiegano CGN dovrebbero essere usati solo se non c’è altra scelta.

Ci sono molti libri e siti Web disponibili con volumi di informazioni approfondite su IPv6. L’articolo di Wikipedia su IPv6, http://en.wikipedia.org/wiki/IPv6, è un’ottima risorsa per ulteriori informazioni e collegamenti ad altre fonti. Vale la pena utilizzarlo come punto di partenza per ulteriori informazioni su IPv6. Ci sono anche molti buoni libri su IPv6 disponibili, ma fai attenzione ad acquistare libri con recenti revisioni. Nel corso degli anni sono state apportate modifiche alle specifiche IPv6 ed è possibile che il materiale possa essere cambiato dalla stampa del libro.

Vedi anche:

Per ulteriori informazioni, puoi accedere all’archivio Hangouts per visualizzare l’Hangout di luglio 2015 su Nozioni di base su IPv6

Questa documentazione non è un’introduzione alle reti ma ci sono alcuni concetti che devono essere affrontati. Per i lettori che non hanno una conoscenza di base del networking, suggeriamo di individuare materiale introduttivo aggiuntivo poiché questo capitolo non fornirà adeguatamente tutte le informazioni necessarie.

I concetti di IPv6 sono introdotti più avanti in *IPv6*. Per chiarezza, gli indirizzi IP tradizionali vengono definiti indirizzi IPv4. Salvo dove diversamente indicato, la maggior parte delle funzioni funzionerà con indirizzi IPv4 o IPv6. Il termine generale indirizzo IP si riferisce a IPv4 o IPv6.

3.8 Breve introduzione ai livelli del modello OSI

Il modello OSI ha un framework di rete composto da sette livelli. Questi livelli sono elencati nella gerarchia dal più basso al più alto. Una breve panoramica di ogni livello è descritta di seguito. Ulteriori informazioni sono disponibili in molti testi di rete e su Wikipedia (http://en.wikipedia.org/wiki/OSI_model).

- **Livello 1 - Fisico** Si riferisce al cablaggio elettrico o ottico che trasporta i dati grezzi a tutti i livelli superiori.
- **Livello 2 - Collegamento dati** Il livello di collegamento dati si preoccupa di gestire il collegamento da un pc all'altro appartenenti alla stessa LAN, mediante il *Livello 1*. Questa guida fa spesso riferimento al livello 2 come significato degli switch Ethernet o di altri argomenti correlati come gli indirizzi ARP e MAC.
- **Livello 3 - Livello di rete** I protocolli utilizzati per spostare i dati lungo un percorso da un host all'altro, come IPv4, IPv6, routing, sottoreti ecc.
- **Livello 4 – Livello di Trasporto** Trasferimento dati tra utenti, in genere si riferisce a TCP o UDP o altri protocolli simili.
- **Livello 5 - Livello sessione** Gestisce le connessioni e le sessioni (in genere denominate «finestre di dialogo») tra gli utenti e il modo in cui si collegano e si disconnettono con grazia.
- **Livello 6 - Livello di presentazione** Gestisce qualsiasi conversione tra i formati di dati richiesti dagli utenti come set di caratteri diversi, codifiche, compressione, crittografia, ecc.
- **Livello 7 - Livello applicazione** Interagisce con l'utente o l'applicazione software, include protocolli familiari come HTTP, SMTP, SIP, ecc.

CAPITOLO 4

Manuali dei prodotti

CAPITOLO 5

Hardware

5.1 Requisiti minimi hardware

I requisiti minimi per Firew4LL 0.1-RELEASE-p3 sono:

- CPU 600 MHz o più veloce
- RAM 512 MB o più
- Unità disco da 4 GB o superiore (SSD, HDD, ecc.)
- Una o più schede di interfaccia di rete compatibili
- Unità USB di avvio o CD/DVD-ROM per l'installazione iniziale

Nota: I requisiti minimi non sono adatti a tutti gli ambienti; vedere la *Guida al dimensionamento dell'hardware* per i dettagli

5.2 Selezione dell'Hardware

L'uso di sistemi operativi open source con hardware non testato può creare conflitti hardware/software. *Ottimizzazione hardware e risoluzione dei problemi* offre suggerimenti per la risoluzione di vari problemi.

5.2.1 Previeni mal di testa per la scelta dell'hardware

Usare l'hardware ufficiale di Firew4LL

Consigliamo vivamente di utilizzare l'hardware ufficiale dal Firew4LL Store. Il nostro hardware è stato sviluppato per assicurare alla comunità che piattaforme hardware specifiche sono state testate e validate a fondo.

Convenzioni dei nomi

In tutta la guida ci riferiamo all'architettura hardware a 64 bit come «amd64», la designazione dell'architettura usata da FreeBSD. Intel ha adottato l'architettura creata da AMD per x86-64, quindi il nome amd64 si riferisce a tutte le CPU x86 a 64 bit.

5.2.2 Guida alle dimensioni dell'hardware

Durante il dimensionamento dell'hardware per Firew4LL, la velocità effettiva richiesta e le funzionalità necessarie sono i fattori primari che influenzano la selezione dell'hardware.

Considerazioni sulla velocità effettiva

I requisiti minimi sono sufficienti se sono richiesti meno di 100 Mbps di throughput non crittografato. Per requisiti di throughput più elevati, seguire queste linee guida basate su estese esperienze di test e implementazione.

L'hardware a cui fa riferimento questa sezione è disponibile nel *|firew4ll| Store*. Le specifiche generali dell'hardware sono disponibili nella tabella *Hardware |firew4ll|*.

Nelle reti reali il flusso del traffico conterrà probabilmente pacchetti di dimensioni variabili, non tutte così grandi, ma dipende dall'ambiente e dal tipo di traffico coinvolto. La tabella *500.000 PPS di throughput in varie dimensioni di frame* elenca alcune dimensioni di pacchetti comuni e il throughput ottenuto con una velocità di 500.000 pacchetti al secondo.

Tabella 1: 500.000 PPS di throughput in varie dimensioni di frame

Frame size	Throughput at 500 Kpps
64 bytes	244 Mbps
500 bytes	1.87 Gbps
1000 bytes	3.73 Gbps
1500 bytes	5.59 Gbps

Differenza di prestazioni per tipo di scheda di rete

La scelta della scheda NIC ha un impatto significativo sulle prestazioni. Le schede economiche e di fascia bassa consumano molta più CPU rispetto alle schede di migliore qualità come Intel. Il primo scoglio per il throughput del firewall è throughput migliora in modo significativo utilizzando una scheda NIC di qualità migliore con CPU più lente. Al contrario, aumentando la velocità della CPU non aumenterà proporzionalmente il throughput se abbinato a una scheda di rete di bassa qualità.

5.2.3 Considerazioni sulle funzioni

Funzionalità, servizi e pacchetti abilitati sul firewall possono ridurre il throughput potenziale totale in quanto consumano risorse hardware che potrebbero altrimenti essere utilizzate per trasferire il traffico di rete. Ciò è particolarmente vero per i pacchetti che intercettano o ispezionano il traffico di rete, come Snort o Suricata.

La maggior parte delle funzionalità del sistema di base non tiene conto in modo significativo del dimensionamento dell'hardware, ma alcune possono potenzialmente avere un impatto notevole sull'utilizzo dell'hardware.

Tabelle di stato

Le connessioni di rete attive attraverso il firewall sono tracciate nella tabella di stato del firewall. Ogni connessione attraverso il firewall consuma due stati: uno che entra nel firewall e uno che esce dal firewall. Ad esempio, se un firewall deve gestire 100.000 connessioni client simultanee del server Web, la tabella di stato deve essere in grado di contenere 200.000 stati.

I firewall in ambienti che richiedono un numero elevato di stati simultanei devono disporre di RAM sufficiente per contenere la tabella degli stati. Ogni stato richiede circa 1 KB di RAM, il che rende il calcolo dei requisiti di memoria relativamente facile. La tabella *Consumo RAM di una tabella di stato grande* fornisce una guida per la quantità di memoria richiesta per dimensioni di tabelle stato più grandi. Questa è esclusivamente la memoria utilizzata per il rilevamento dello stato. Il sistema operativo stesso insieme ad altri servizi richiederà almeno 175-256 MB di RAM aggiuntiva e possibilmente di più a seconda delle funzionalità utilizzate.

Tabella 2: Consumo RAM di una tabella di stato ampia

Stati	Connessioni	RAM Richiesta
100,000	50,000	~97 MB
500,000	250,000	~488 MB
1,000,000	500,000	~976 MB
3,000,000	1,500,000	~2900 MB
8,000,000	4,000,000	~7800 MB

È più sicuro sopravvalutare i requisiti. Sulla base delle informazioni di cui sopra, una buona stima sarebbe che 100.000 stati consumerebbero circa 100 MB di RAM o che 1.000.000 stati consumerebbero circa 1 GB di RAM.

VPN (tutti i tipi)

La domanda che i clienti pongono in genere sulle VPN è «Quante connessioni può gestire il mio hardware?» Questo è un fattore secondario nella maggior parte delle distribuzioni ed è di minore importanza. Quella metrica è un effetto di come altri fornitori hanno concesso in licenza funzionalità VPN in passato e non ha un equivalente diretto specifico in Firew4LL. La considerazione principale nel dimensionamento hardware per VPN è il potenziale throughput del traffico VPN.

La crittografia e la decrittografia del traffico di rete con tutti i tipi di VPN richiede molta CPU. Firew4LL offre diverse opzioni di cifratura da utilizzare con IPsec. Le varie cifre funzionano in modo diverso e il throughput massimo di un firewall dipende dalla cifra utilizzata e dalla possibilità o meno che tale cifra possa essere accelerata dall'hardware.

Gli acceleratori di crittografia hardware aumentano notevolmente la velocità effettiva massima della VPN ed eliminano in gran parte la differenza di prestazioni tra le cifre accelerate. La tabella *Velocità effettiva VPN per modello hardware, tutti i valori sono in Mbit/s* illustra la velocità effettiva massima per i vari componenti hardware disponibili nell'archivio Firew4LL quando si utilizza IPsec e OpenVPN.

Per IPsec, AES-GCM è accelerato da AES-NI ed è più veloce non solo per questo, ma anche perché non richiede un algoritmo di autenticazione separato. IPsec ha anche un overhead di elaborazione del sistema operativo per pacchetto inferiore rispetto a OpenVPN, quindi per ora IPsec sarà quasi sempre più veloce di OpenVPN.

Tabella 3: Velocità effettiva VPN per modello hardware, tutti i valori sono in Mbit/s

Modello	OpenVPN/AES-128+SHA1	IPsec/IKEv2+AES-GCM
	TCP 1400B	TCP 1400B
Firew4ll-ISN	103	98

Laddove un throughput VPN elevato è un requisito per un firewall, l'accelerazione crittografica dell'hardware è della massima importanza per assicurare non solo velocità di trasmissione elevate, ma anche ridurre il sovraccarico della

CPU. La riduzione del sovraccarico della CPU significa che non ridurrà le prestazioni di altri servizi sul firewall. L'attuale migliore accelerazione è disponibile utilizzando una CPU che include il supporto AES-NI combinato con AES-GCM in IPsec.

Pacchetti

Alcuni pacchetti hanno un impatto significativo sui requisiti hardware e il loro uso deve essere preso in considerazione quando si seleziona l'hardware.

Snort/Suricata

Snort e Suricata sono pacchetti Firew4LL per il rilevamento delle intrusioni nella rete. A seconda della loro configurazione, possono richiedere una quantità significativa di RAM. 1 GB deve essere considerato come minimo, ma alcune configurazioni potrebbero richiedere almeno 2 GB.

Suricata è multi-thread e può potenzialmente sfruttare NETMAP per IPS inline se l'hardware offre supporto.

Squid

Squid è un server proxy HTTP con memorizzazione nella cache disponibile come pacchetto Firew4LL. Le prestazioni di I/O del disco sono una considerazione importante per gli utenti di Squid poiché determinano le prestazioni della cache. Al contrario, la velocità del disco è in gran parte irrilevante per la maggior parte dei firewall Firew4LL poiché l'unica attività significativa del disco è il tempo di avvio e il tempo di aggiornamento; non ha rilevanza per la velocità di trasmissione della rete o altre normali operazioni.

Anche per Squid qualsiasi disco rigido sarà sufficiente in piccoli ambienti. Per oltre 200 implementazioni utente, un SSD di alta qualità di un OEM di livello 1 è un must. Un SSD di bassa qualità potrebbe non essere in grado di sopportare le numerose scritture legate al mantenimento dei dati memorizzati nella cache.

Le dimensioni della cache di squid incidono anche sulla quantità di RAM richiesta per il firewall. Squid consuma circa 14 MB di RAM per 1 GB di cache su amd64. A quel ritmo, una cache da 100 GB richiederebbe 1,4 GB di RAM per la sola gestione della cache, senza contare le altre esigenze di RAM per squid.

5.3 Ottimizzazione dell'hardware e risoluzione dei problemi

l sistema operativo che sostiene Firew4LL può essere messo a punto in molti modi. Alcuni di questi parametri sintonizzabili sono disponibili in Firew4LL in **Opzioni avanzate** (Vedere scheda *Sintonizzabili di sistema*). Altri sono indicati nell'*ottimizzazione* della pagina principale di FreeBSD (7).

L'installazione predefinita del software Firew4LL include un set completo di valori ottimizzati per una buona prestazione senza essere eccessivamente aggressivo. Ci sono casi in cui hardware o driver richiedono la modifica di valori o un carico di lavoro di rete specifico richiede modifiche per funzionare in modo ottimale. L'hardware venduto nel *negozio \firew4ll* è ulteriormente ottimizzato poiché abbiamo una conoscenza dettagliata dell'hardware, che elimina la necessità di fare affidamento su ipotesi più generali.

Modifiche comuni lungo queste linee per altro hardware sono disponibili nella pagina wiki della *documentazione per la sintonizzazione e la risoluzione dei problemi delle schede di rete.*

Nota: Le modifiche a /boot/loader.conf.local richiedono il riavviodel firewall.

5.3.1 Eusarimento del Mbuf

Un problema comune riscontrato dagli utenti dei commmodity hardware è l'esaurimento di mbuf. Per i dettagli su mbufs e il monitoraggio dell'utilizzo di mbuf, consultare *Cluster Mbuf*. Se il firewall esaurisce mbufs, può causare il panico del kernel e il riavvio con determinati carichi di rete che esauriscono tutti i buffer di memoria di rete disponibili. Ciò è più comune con le schede di rete che utilizzano più code o che sono altrimenti ottimizzate per le prestazioni rispetto all'utilizzo delle risorse. Inoltre, l'utilizzo di mbuf aumenta quando il firewall utilizza determinate funzionalità come *Limiters* Per aumentare la quantità di mbuf disponibili, aggiungere quanto segue a `/boot/loader.conf.local`:

```
kern.ipc.nmbclusters="1000000"
```

Inoltre, le schede potrebbero aver bisogno di altri valori simili aumentati come kern.ipc.nmbjumbop. Oltre ai grafici sopra menzionati, controlla l'output del comando netstat -m per verificare se ci sono aree vicine all'esaurimento.

5.3.2 NIC Queue Count Conteggio code NIC

Per motivi di prestazioni, alcuni tipi di schede di rete utilizzano più code per l'elaborazione dei pacchetti. Su sistemi multi-core, in genere un driver vorrà utilizzare una coda per core della CPU. Esistono alcuni casi in cui ciò può portare a problemi di stabilità, che possono essere risolti riducendo il numero di code utilizzate dalla scheda di rete. Per ridurre il numero di code, specificare il nuovo valore in `/boot/loader.conf.local`, come ad esempio:

```
hw.igb.num_queues=1
```

Il nome dell'OID sysctl varia in base alla scheda di rete, ma di solito si trova nell'output di sysctl -a, sotto hw.<drivername>.

5.3.3 Disabilitare MSIX

Un altro problema comune è una scheda di rete che non supporta correttamente MSIX nonostante le sue affermazioni. MSIX può essere disabilitato aggiungendo la seguente riga in */boot/loader.conf.local*:

```
hw.pci.enable_msix=0
```

La distribuzione del software Firew4LL è compatibile con la maggior parte di hardware supportati da FreeBSD.

Firew4LL è compatibile con l'hardware di architettura a 64 bit (amd64, x86-64).

5.4 Compatibilità Hardware

Il modo migliore per garantire che l'hardware sia compatibile con il software Firew4LL è acquistare hardware dallo store Firew4LL poichè sono stati testati e noti per funzionare bene con Firew4LL. L'hardware nello store viene testato con ogni versione del software Firew4LL ed è ottimizzato per le prestazioni.

Per le soluzioni casalinghe, le note hardware di FreeBSD sono la migliore risorsa per determinare la compatibilità hardware. Firew4LL versione 01-RELEASE-p3 si basa su 11.2-RELEASE-p14, quindi l'hardware compatibile si trova nelle note hardware sul sito Web di FreeBSD. Un'altra buona risorsa è la sezione Hardware delle FAQ di FreeBSD.

5.4.1 Adattatori di rete

Una vasta gamma di schede Ethernet cablate (NIC) sono supportate da FreeBSD e sono quindi compatibili con i firewall Firew4LL. Tuttavia, non tutte le schede di rete sono uguali. L'hardware può variare notevolmente in termini di qualità da un produttore all'altro.

Raccomandiamo le schede NIC Intel PRO/1000 1Gb e PRO/10GbE 10Gb perché hanno un solido supporto per i driver in FreeBSD e funzionano molto bene. La maggior parte dell'hardware venduto nel negozio Firew4LL contiene schede di rete Intel.

Delle varie altre schede PCIe/PCI supportate da FreeBSD, alcune funzionano bene. Altre potrebbero avere problemi come le VLAN che non funzionano correttamente, non essere in grado di impostare velocità o duplex o avere prestazioni scadenti. In alcuni casi, FreeBSD può supportare una particolare scheda di rete ma, con implementazioni specifiche del chipset, il supporto del driver o può essere scadente. In caso di dubbi, cerca nel forum Firew4LL le esperienze di altri utenti che utilizzano lo stesso hardware o simile.

Quando un firewall richiede l'uso di VLAN, selezionare adattatori che supportano l'elaborazione VLAN nell'hardware. Questo è discusso in *LAN virtuali (VLAN)*.

Adattatori di rete USB

Si sconsiglia di utilizzare adattatori di rete USB di qualsiasi marca / modello a causa della loro inaffidabilità e scarse prestazioni.

Adattatori wireless

Gli adattatori e i dispositivi wireless supportati sono trattati in *Wireless*.

CAPITOLO 6

Installazione e aggiornamento

L'hardware di Firew4LL Store è precaricato con il software Firew4LL. Per reinstallare il software Firew4LL o installarlo su altro hardware, scaricare un'immagine del programma di installazione come descritto in questo capitolo.

Se qualcosa va storto durante il processo di installazione, consultare *Risoluzione dei problemi di installazione*.

Questo capitolo tratta anche dell'aggiornamento delle installazioni del software Firew4LL (*Aggiornamento di un'installazione esistente*) che le mantiene aggiornate con la sicurezza, le correzioni di errori e le nuove funzionalità più recenti.

6.1 Download del supporto di installazione

I clienti che hanno acquistato i firewall da Firew4LL Store possono scaricare le immagini di installazione di fabbrica ottimizzate dal proprio account sul portale Firew4LL. Il sito della documentazione di Netgate contiene istruzioni specifiche per ciascun modello, quindi controllare quel sito prima di scaricare le immagini in base alle informazioni contenute in questo capitolo.

- Andare su https://www.firew4ll.com/download in un browser Web su un PC client.
- Fare clic su **Download**.
- Selezionare l'"**architettura**:

  AMD64 (64 bit) per hardware Intel o AMD x86- 64 bit.

  - Selezionare una **piattaforma** per un'installazione a 64 bit:
  - **Programma di installazione su una chiavetta USB** Un'immagine disco che può essere scritta su una chiavetta USB (memstick) e avviata sull'hardware di destinazione per l'installazione. - **VGA** Installa utilizzando un monitor e una tastiera collegati all'hardware di destinazione. - **Installazioni seriali** utilizzando una console seriale su COM1 dell'hardware di destinazione. Questa opzione richiede una porta della console fisica.
  - **Programma di installazione immagine su un CD (ISO)** Per l'installazione da supporti ottici o per l'uso con IPMI o hypervisor che possono essere avviati da immagini ISO.

- Fare clic su  **Scarica**.
- Copiare il checksum SHA-256 visualizzata dalla pagina per verificare il download in un secondo momento.

I nomi dei file per la versione 0.1-RELEASE-p3 del software Firew4LL sono:

- **USB Memstick Installer (VGA)**

Firew4ll-CE-memstick-0.1-RELEASE-p3-amd64.img.gz

- **USB Memstick Installer (seriale)** Firew4ll-CE-memstick-serial-0.1-RELEASE-p3-amd64.img.gz
- **ISO Image installer** Firew4ll-CE-0.1-RELEASE-p3-amd64.iso.gz

6.1.1 Verifica dell'integrità del download

L'integrità dell'immagine del programma di installazione può essere verificata confrontando un valore di hash calcolato del file scaricato con un hash calcolato dal progetto Firew4LL quando i file sono stati originariamente creati. Gli hash correnti forniti dal progetto utilizzano SHA-256.

La somma SHA-256 visualizzata nella pagina di download è la migliore fonte, in quanto non viene estratta dalla stessa directory delle immagini di download. Un file contenente la somma SHA-256 è disponibile anche sui mirror con lo stesso nome file dell'immagine di installazione scelta, ma termina con .sha256.

Utilizzare la somma SHA-256 di accompagnamento dal sito di download o dal file .sha256 per verificare che il download sia stato completato correttamente e che sia una versione ufficiale del software Firew4LL.

Avvertimento: Il checksum SHA-256 viene calcolato rispetto alle versioni compresse dei file scaricati. Confrontare l'hash prima di decomprimere il file.

6.1.2 Verifica hash su Windows

Gli utenti Windows possono installare HashTab o un programma simile per visualizzare gli hash SHA-256 per un determinato file. L'hash SHA-256 generato può essere confrontato con la somma SHA-256 dal sito di download o con il contenuto del file .sha256 dal server di download. Il file .sha256 è visualizzabile in qualsiasi editor di testo semplice come Blocco note.

Con HashTab installato, per verificare l'hash di un file:

- Fare clic con il tasto destro sul file scaricato.
- Fare clic sulla scheda **Hash file**. HashTab impiegherà alcuni istanti per calcolare l'hash.
- Passare il mouse sull'hash SHA-256 per visualizzare l'hash completo.
- Incollare la somma SHA-256 dal sito di download o dal file .sha256 nella casella Confronto hash per verificare automaticamente se l'hash corrisponde.
- Fare clic su **Annulla** per chiudere la finestra di dialogo delle proprietà del file senza apportare modifiche.

Se un hash SHA-256 non è visualizzato in HashTab:

- Fai clic su Impostazioni
- Selezionare la casella per **SHA-256**
- Fare clic su OK

6.1.3 Verifica hash su BSD e Linux

Il comando sha256 viene fornito di serie su FreeBSD e su molti altri sistemi operativi UNIX e simili a UNIX. Un hash SHA-256 può essere generato eseguendo il comando seguente all'interno della directory contenente il file scaricato:

```
# sha256 firew4ll-CE-memstick-0.1-RELEASE-p3-amd64.img.gz
```

Confronta l'hash risultante con la somma SHA-256 visualizzata sul sito di download o il contenuto del file .sha256 scaricato dal sito Web Firew4LL. I sistemi GNU o Linux forniscono un comando sha256sum che funziona in modo simile.

6.1.4 Verifica hash su OS X

OS X include anche il comando sha256, lo stesso di FreeBSD, ma ci sono anche applicazioni GUI disponibili come QuickHash. HashTab è disponibile anche per OS X.

6.2 Preparazione del supporto di installazione

L'immagine di installazione scaricata nella sezione precedente deve prima essere trasferita sul supporto corretto. I file non possono essere copiati direttamente sul supporto, ma devono essere scritti utilizzando strumenti appropriati.

La differenza principale tra la chiavetta USB e l'immagine ISO sta nel modo in cui le immagini vengono scritte su un disco di installazione. Entrambi i tipi di immagini installano il software Firew4LL su un disco di destinazione. Un'altra differenza è tra i tipi di console per le diverse immagini delle chiavette USB. Dopo l'installazione, ognuno mantiene le impostazioni della console appropriate.

Nota: Se l'hardware di destinazione non ha un'unità ottica e non può essere avviato da USB, installare il software sul disco di destinazione utilizzando un set diverso di hardware. Leggere *Tecniche di installazione alternative* per ulteriori informazioni.

6.2.1 Decomprimere il supporto di installazione

L'immagine del disco di installazione viene compressa quando viene scaricata per risparmiare larghezza di banda e memoria. Decomprimi il file prima di scrivere questa immagine su un disco di installazione.

L'estensione .gz sul file indica che il file è compresso con gzip. L'immagine può essere decompressa su Windows usando 7-Zip o su BSD / Linux/Mac con i comandi gunzip o gzip -d.

6.2.2 Scrittura del supporto di installazione

La creazione di un disco di installazione richiede una procedura diversa a seconda del tipo di supporto. Seguire le istruzioni nella sezione appropriata per il tipo di supporto selezionato.

Preparare una chiavetta USB

Avvertimento: Fate molta attenzione quando scrivete le immagini dei dischi con Firew4LL! Se il PC client contiene altri dischi rigidi è possibile selezionare il drive sbagliato e sovrascrivere una parte di quel drive con il disco di installazione. Questo rende il disco completamente illeggibile se non per alcuni programmi di recupero del disco.

Collegare la chiavetta USB alla workstation

Inizia collegando la chiavetta USB alla workstation contenente l'immagine del supporto di installazione.

Individua il nome del dispositivo designato dal PC client per l'unità. Il dispositivo varia in base alla piattaforma, ecco alcuni esempi:

- Linux: `/dev/sdX` dove X è una lettera minuscola. Cerca i messaggi sull'unità allegata nei file di registro di sistema o eseguendo dmesg.
- FreeBSD: `/dev/daX` dove X è una cifra decimale. Cerca i messaggi sull'unità allegata nei file di registro di sistema o eseguendo dmesg.
- Windows: l'unità avrà il nome di una singola lettera maiuscola, ad es. D. Utilizza Explorer o esamina il pannello di controllo del sistema e cerca i dischi disponibili per uno corrispondente all'unità.
- Su Mac OS X: `/dev/diskX` dove X è una cifra decimale. Esegui l'elenco diskutil da un prompt dei comandi o utilizza **Disco Utilità** GUI.

Nota: Su Mac OS X, se il disco è denominato diskX, il dispositivo da passare all'utilità di scrittura è effettivamente rdiskX che deve essere più veloce per questo tipo di operazioni di basso livello.

Nota: Assicurarsi inoltre che il nome del dispositivo si riferisca al dispositivo stesso anziché a una partizione sul dispositivo. Ad esempio, /dev/sdb1 su Linux è la prima partizione sul disco, quindi scriverà su una partizione sul dispositivo e l'unità potrebbe non essere avviabile. In tal caso, utilizzare /dev/sdb in modo che l'utilità dell'immagine del disco scriva sull'intero disco.

Pulizia della chiavetta USB

Questo passaggio è facoltativo a meno che l'immagine non riesca a scrivere sulla chiavetta USB.

L'unità di destinazione potrebbe già contenere partizioni che possono impedire che vengano scritte correttamente dagli strumenti di immagine del disco. Per ricominciare, cancella tutte le partizioni dal disco. Questo può essere fatto in diversi modi in Windows o in UNIX.

Windows

L'interfaccia **Gestione disco** in Windows è un mezzo per eliminare le partizioni da un disco ma spesso l'operazione è ha disabilitata. Il metodo più semplice e affidabile è utilizzare diskpart.

- Avviare un prompt dei comandi (cmd.exe) come amministratore
- Eseguire diskpart
- Immettere disk list per mostrare i dischi collegati al PC client
- Individuare la chiavetta USB di destinazione nell'elenco e annotare il suo numero di disco

- Immettere select disk n dove n è il numero del disco della chiavetta USB di destinazione dall'elenco nell'output del comando precedente
- Immettere clean per rimuovere le partizioni dal disco
- Immettere exit per interrompere diskpart e tornare a un prompt dei comandi
- Immettere di nuovo exit per chiudere la finestra del prompt dei comandi

Linux, FreeBSD, Mac OS X

Il comando dd è il modo più semplice per cancellare la tabella delle partizioni dalla chiavetta USB su sistemi operativi UNIX e simili a UNIX come Linux, FreeBSD e OS X.

```
$sudo dd if=/dev/zero of= memstick_disk_path bs=1M count=1
```

Sostituisci memstick_disk_path con il percorso del dispositivo del disco della chiavetta, ad es. `/dev/ sdb`, `/dev/ da1` o `/dev/rdisk3`.

Scrivere l'immagine

Ora è il momento di scrivere l'immagine sulla chiavetta USB. La procedura esatta varia in base al sistema operativo.

Nota: Le seguenti istruzioni presuppongono che il file di immagine del supporto di installazione sia stato prima decompresso da un'utilità appropriata. Per i dettagli, consultare *Decomprimere il supporto di installazione*.

Avvertimento: Le operazioni in questa sezione sovrascriveranno completamente qualsiasi contenuto esistente sulla chiavetta USB! Controllare prima la chiavetta USB per eventuali file da salvare o eseguire il backup.

Linux, FreeBSD, Mac OS X

Su Linux, FreeBSD e Mac OSX, scrivi l'immagine sull'unità usando il comando dd. Prende questa forma generale:

```
dd if=image_file_name of=usb_disk_device_name
```

Scrivere sul disco in questo modo richiede generalmente privilegi elevati, quindi l'utente che scrive l'immagine avrà molto probabilmente bisogno di usare sudo per eseguire il comando.

Esempio di comandi di scrittura su disco dd:

Writing to the disk in this way generally requires elevated privileges, so the user writing the image will most likely need to use sudo to run the command.

Example dd disk writing commands:

- Linux:

  sudo dd if=Firew4ll-CE-memstick-0.1-RELEASE-p3-amd64.img of=/dev/sdb bs=4M

- FreeBSD:

  sudo dd if=Firew4ll-CE-memstick-0.1-RELEASE-p3-amd64.img of=/dev/da1 bs=4m

- Mac OSX:

  sudo dd if=Firew4ll-CE-memstick-0.1-RELEASE-p3-amd64.img of=/dev/rdisk3 bs=4m

Il parametro bs = X è facoltativo e indica a dd di eseguire letture e scritture su blocchi di dati da 4 MB alla volta. La dimensione del blocco predefinita utilizzata da dd è 512 byte. Specificare una dimensione del blocco più grande può aumentare significativamente la velocità di scrittura.

Windows

Per scrivere un'immagine su un'unità da una workstation Windows, utilizzare uno strumento GUI come Win32 Disk Imager o Rufus. Lo stesso comando Linux dd sopra elencato può essere utilizzato anche da Cygwin se il prompt dei comandi di Cygwin viene avviato come amministratore.

Win32 Disk Imager

- Scaricare e installare Win32 Disk Imager
- Avviare Win32 Disk Imager come **amministratore**
- Fare clic sull'icona della cartella
- Passare alla posizione dell'immagine del supporto di installazione decompressa
- Selezionare l'immagine
- Scegliere l'unità della chiavetta USB di destinazione dal menu a discesa del **Dispositivo**
- Fare clic su **Scrivi**
- Attendere che l'immagine finisca di scrivere

Rufus

- Scaricare e installare Rufus
- Avviare Rufus come **amministratore**
- Scegliere l'unità della chiavetta USB di destinazione dal menu a discesa del **Dispositivo**
- Selezionare *Immagine DD* dall'elenco a discesa accanto a **Creare disco di avvio di utilizzo**
- Fare clic sull'icona del CD-ROM accanto a **Crea disco di avvio di utilizzo**
- Passare alla posizione dell'immagine del supporto di installazione decompressa
- Selezionare l'immagine
- Fare clic su **Avviare**
- Attendere che l'immagine finisca di scrivere

Risoluzione dei problemi

Se la scrittura del disco non riesce, specialmente su Windows, pulire la chiavetta USB come suggerito in *Pulizia della chiavetta USB* quindi riprovare. Se il problema persiste, provare con un'altra chiavetta USB.

Preparare un CD/DVD

Per utilizzare un file immagine ISO con un'unità disco ottico, l'immagine ISO deve essere masterizzata su un disco CD o DVD mediante un software di scrittura appropriato.

Poiché l'immagine ISO è un'immagine a disco intero, deve essere masterizzata in modo appropriato per i file di immagine non come un CD di dati contenente il singolo file ISO. Le procedure di masterizzazione variano in base al sistema operativo e al software disponibile.

Masterizzazione in Windows

Windows 7 e versioni successive includono la possibilità di masterizzare immagini ISO in modalità base senza software aggiuntivo. Inoltre, praticamente tutti i principali pacchetti software di masterizzazione di CD per Windows includono la possibilità di masterizzare immagini ISO. Consultare la documentazione per il programma di masterizzazione di CD. Una ricerca su Google con il nome del software di masterizzazione e burn iso aiuta anche a trovare le istruzioni.

Masterizzare con Windows

Per masterizzare un'immagine disco in modalità base in Windows 7 o versioni successive:

- Aprire Windows Explorer e individuare il file di immagine ISO decompresso
- Fare clic con il tasto destro del mouse sul file immagine ISO
- Fare clic su **Masterizzare immagine disco**
- Selezionare **l'unità di masterizzazione del disco** appropriata dall'elenco a discesa
- Inserire un disco CD o DVD vuoto
- Fare clic su **Masterizzare**

Le versioni successive come Windows 10 mostrano anche una scheda **Strumenti immagine disco** sulla barra multi-funzione quando si seleziona un'immagine ISO in Windows Explorer. Quella scheda ha un'icona **Masterizzare** che richiama anche la stessa interfaccia di masterizzazione del disco.

Masterizzare con Nero

Per masterizzare un'immagine ISO con Nero:

- Aprire Windoes Explorer e individuare il file di immagine ISO decompresso
- Fare clic con il tasto destro del mouse sul file immagine ISO
- Fare clic su **Aprire con**
- Selezionare **Nero**
- Seguire le istruzioni in Nero per scrivere il disco

Al primo utilizzo di Nero, potrebbe essere necessario selezionarlo dall'elenco **Scegliere programma predefinito**. Questo processo può funzionare anche con altri software commerciali di masterizzazione di CD.

Masterizzazione con ISO Recoder

Se il PC client utilizza Windows XP, 2003 o Vista, lo strumento di ISO Recoder disponibile gratuitamente può scrivere immagini ISO su disco.

- Scaricare e installare la versione appropriata di ISO Recorder
- Passare alla cartella sull'unità contenente il file di immagine ISO decompresso
- Fare clic con il tasto destro del mouse sul file immagine ISO
- Fare clic su **Copiare immagine su CD**

Altro software di masterizzazione gratuito

Altre opzioni gratuite per gli utenti di Windows includono CDBurnerXP, InfraRecorder e ImgBurn. Prima di scaricare e installare qualsiasi programma, controllare l'elenco delle caratteristiche per accertarsi che sia in grado di masterizzare un'immagine ISO.

Masterizzazione in Linux

Le distribuzioni Linux come Ubuntu in genere includono un'applicazione di masterizzazione di CD GUI in grado di gestire immagini ISO. Se un'applicazione di masterizzazione di CD è integrata con il gestore di finestre, provare una delle seguenti procedure:

- Fare clic con il tasto destro sul file di immagine ISO decompresso
- Scegliere **Aprire con**
- Scegliere **Masterizzazione Immagine del Disco**

O:

- Fare clic con il tasto destro sul file di immagine ISO decompresso
- Scegliere **Scrivere disco su**

Altre applicazioni popolari includono K3B e Brasero Disc Burner.

Se un programma di masterizzazione GUI non è disponibile, potrebbe essere possibile masterizzare dalla riga di comando.

Innanzitutto, determinare l'ID/LUN SCSI del dispositivo di masterizzazione (Numero unità logica) con il seguente comando:

```
$ cdrecord --scanbus
scsibus6:
6,0,0 600) 'TSSTcorp' 'CDDVDW SE-S084C ' 'TU00' Removable CD-ROM
```

Si noti che l'ID/LUN SCSI è 6,0,0 in questo esempio.

Masterizzare l'immagine come nell'esempio seguente, sostituendo <velocità massima> con la velocità del masterizzatore (ad es. 24) e <lun> con l'ID SCSI/LUN del registratore:

```
$ sudo cdrecord --dev=<lun> --speed=<max speed> Firew4ll-CE-0.1-RELEASE-p3-amd64.iso
```

Masterizzare in FreeBSD

FreeBSD può usare le stesse opzioni cdrecord di Linux installando sysutils/cdrtools da porte o pacchetti, e può anche usare applicazioni GUI come K3B o Brasero Disc Burner se sono installate da porte.

Vedere anche:

Per maggiori informazioni sulla creazione di CD in FreeBSD, vedere la voce per la masterizzazione di CD nel Manuale di FreeBSD.

Verifica del disco

Dopo aver scritto il disco, verificare che sia stato masterizzato correttamente visualizzando i file sul disco. Dovrebbero essere visibili più di 20 cartelle, inclusi bin, boot, cf, conf e altro. Se è visibile solo un file ISO di grandi dimensioni, il disco non è stato masterizzato correttamente. Ripetere i passaggi di masterizzazione elencati in precedenza e assicurarsi di masterizzare il file ISO come immagine CD e non come file di dati.

6.3 Connessione alla console

Una connessione alla console sull'hardware di destinazione è un requisito per eseguire il programma di installazione. Per l'hardware con una console VGA, è semplice come collegare un monitor e una tastiera.

Per l'hardware con una console seriale, il processo è più complesso e richiede un PC client con una porta e un software terminale appropriati. Seguire le istruzioni seguenti per connettersi utilizzando una console seriale.

6.3.1 Connessione a una console seriale

Le istruzioni in questa sezione trattano argomenti generali sulla console seriale. Alcuni dispositivi, come i firewall di Firew4LL Store, richiedono metodi leggermente diversi per connettersi alla console seriale. Per i dispositivi dal Firew4LL Store, visitare la documentazione di Netgate per istruzioni sulla console seriale specifica del modello.

6.3.2 Requisiti della console seriale

La connessione a una console seriale sulla maggior parte dei firewall richiede l'hardware corretto su ogni parte del collegamento, tra cui:

- Il PC client deve disporre di una porta seriale fisica o di un adattatore da USB a seriale
- Il firewall deve avere una porta seriale fisica
- Un cavo seriale e /o un adattatore null modem

Per la maggior parte dei firewall acquistati da Firew4LL Store, l'unico requisito hardware è un cavo da USB A a Mini-B. Vedere la documentazione di Netgate per dettagli.

Oltre alla corretta connessione hardware, sul PC client deve essere disponibile anche un programma client per console seriale e la velocità seriale e altre impostazioni devono essere disponibili.

6.3.3 Collegare un cavo seriale

Innanzitutto, un cavo seriale null modem deve essere collegato tra il firewall e un PC client. A seconda della porta seriale e del cavo in uso, potrebbe essere necessario un dispositivo di modifica del genere del cavo seriale per abbinare le porte disponibili.

Se un cavo seriale null modem reale non è disponibile, è possibile utilizzare un adattatore null modem per convertire un cavo seriale standard in un cavo null modem.

Se il PC client non dispone di una porta seriale fisica, utilizzare un adattatore da USB a seriale.

6.3.4 Individuare la porta seriale del client

Sul PC client, è necessario determinare il nome del dispositivo della porta seriale in modo che il software client possa essere utilizzato sulla porta corretta.

Windows

Sui client Windows, una porta seriale fisica è in genere COM1. Con un adattatore da USB a seriale, potrebbe essere COM3. Aprire **Gestione dispositivi** in Windows ed espandere **Porte** (**COM e LPT**) per trovare l'assegnazione delle porte.

Mac OS X

Su Mac OS X, il nome può essere difficile da determinare per un utente poiché varia in base al nome e al tipo di driver. Alcuni esempi comuni includono /dev/cu.SLAB_USBtoUART e /dev/cu.usbserial- <model>.

Linux

È probabile che il dispositivo associato a un adattatore da USB a seriale venga visualizzato come /dev/ttyUSB0. Cercare i messaggi sul dispositivo allegato nei file di registro di sistema o eseguendo dmesg.

Nota: Se il dispositivo non appare in `/dev/`, controllare se il dispositivo richieda driver aggiuntivi.

FreeBSD

È probabile che il dispositivo associato a un adattatore da USB a seriale venga visualizzato come /dev/cuaU0. Cercare i messaggi sul dispositivo allegato nei file di registro di sistema o eseguendo dmesg.

6.3.5 Determinare le impostazioni della console seriale

Le impostazioni per la porta seriale, compresa la velocità, devono essere note prima che un client possa connettersi correttamente a una console seriale.

Qualunque sia il client seriale utilizzato, assicurarsi che sia impostato per Speed (115200), Bit di dati (8), Parità (No) e Bit di stop (1) corretti. Questo è in genere scritto come 115200/8/N/1.

Nota: Per impostazione predefinita, alcuni componenti hardware hanno una velocità inferiore. PC Engines imposta automaticamente ALIX su 38400/8/N/1 e l'hardware Soekris su 19200/8/N/1. Ciò è rilevante per il BIOS e l'output iniziale, non per Firew4LL, che per impostazione predefinita è 115200.

Molti client seriali hanno un valore predefinito di 9600/8/N/1, quindi è necessario regolare queste impostazioni per connettersi. Utilizzare 115200/8/N/1 con Firew4LL indipendentemente dall'impostazione dell'hardware/BIOS.

Per hardware che utilizza velocità seriali del BIOS diverse da 115200, modificare la velocità di trasmissione in 115200 nell'impostazione del BIOS in modo che il BIOS e Firew4LL siano entrambi accessibili con le stesse impostazioni. Fare riferimento al manuale dell'hardware per informazioni sull'impostazione della sua velocità di trasmissione.

115200 è la velocità predefinita che Firew4LL utilizza per impostazione predefinita, ma la velocità seriale utilizzata da Firew4LL può essere modificata in un secondo momento. Vedere *Velocità cdella seriale*.

6.3.6 Individuare un client seriale

È necessario utilizzare un programma client seriale sul PC client. Il client più popolare per Windows è PuTTY, che è gratuito e funziona bene. PuTTY è disponibile anche per Linux e può essere installato su OS X utilizzando brew. Su UNIX e UNIX-

Come i sistemi operativi, il programma dello schermo è prontamente disponibile o facilmente installabile e può anche essere utilizzato per connettersi alle porte seriali da un programma terminale o da una console di sistema.

Windows

PuTTY è la scelta gratuita più popolare per la comunicazione seriale su Windows. SecureCRT è un altro client che funziona bene.

Avvertimento: Non usare Hyperterminal. Anche se è già presente sul PC client, è inaffidabile e incline alla formattazione errata e alla perdita di dati.

Mac OS X

Sui client Mac OS X, l'utilità dello schermo GNU è la scelta più semplice e più comune. ZTerm e cu (simili a FreeBSD) possono anche essere usati.

Linux

Sui client Linux, l'utilità dello schermo GNU è la scelta più semplice e più comune. Possono anche essere usati programmi come PuTTY, minicom o dterm.

FreeBSD

Sui client FreeBSD, l'utilità dello schermo GNU è la scelta più semplice e più comune.

In alternativa, utilizzare il programma integrato tip. Digitando tip com1 (O tip ucom1 se si utilizza un adattatore seriale USB) si collegherà alla prima porta seriale. Disconnettersi digitando ~. all'inizio di una riga.

6.3.7 Eseguire un Client seriale

Ora che tutti i requisiti sono stati soddisfatti, è tempo di eseguire il client seriale.

Se il software client non è trattato in questa sezione, consultare la sua documentazione per determinare come stabilire una connessione seriale.

PuTTY

- **Avviare PuTTY**
- **Selezionare Seriale per il Tipo di connessione**
- **Immettere il nome del dispositivo della porta seriale per la linea seriale, ad es. COM3 o /dev/ttyUSB0.**

- **Immettere la velocità appropriata, ad es. 115200**
- **Fare clic su Aprire**

Schermo GNU

- Aprire un terminale/prompt dei comandi
- Richiamare il comando screen usando il percorso alla porta seriale, ad esempio:

  $ sudo screen /dev/ttyUSB0 115200

In alcuni casi potrebbe esserci una mancata corrispondenza della codifica del terminale. In tal caso, eseguire la schermata in modalità UTF-8:

```
$ sudo screen -U /dev/cu.SLAB_USBtoUART 115200
```

6.4 Eseguire l'installazione

Questa sezione descrive il processo di installazione del software Firew4LL su un'unità di destinazione, come un SSD o un HDD. In breve, ciò comporta l'avvio dalla pennetta o dal disco CD/DVD e quindi il completamento dell'installer.

Nota: Se il programma di installazione rileva un errore durante il tentativo di avvio o installazione dal supporto di installazione, consultare *Risoluzione dei problemi di installazione*.

I seguenti elementi sono requisiti per eseguire il programma di installazione:

- Scaricare il supporto di installazione
- Preparare i supporti di installazione
- Connettersi alla console

6.4.1 Avvio del supporto di installazione

Per le installazioni da pennette USB, inserire la pennetta USB e quindi accendere il sistema di destinazione. Il BIOS potrebbe richiedere l'inserimento del disco prima dell'avvio dell'hardware.

Per le installazioni da CD/DVD, accendere l'hardware, quindi posizionare il CD in un'unità ottica.

Firew4LL inizierà l'avvio e avvierà automaticamente il programma di installazione.

Specificare l'ordine di avvio nel BIOS

Se il sistema di destinazione non si avvia dalla pennetta USB o dal CD, il motivo più probabile è che il dispositivo specificato non sia stato trovato abbastanza presto nell'elenco dei supporti di avvio nel BIOS. Molte schede madri più recenti supportano un menu di avvio singolo richiamato premendo un tasto durante il POST, comunemente Esc o F12.

In caso contrario, modificare l'ordine di avvio nel BIOS. Innanzitutto, accendere all'hardware e accedere alla configurazione del BIOS. L'opzione dell'ordine di avvio si trova in genere sotto un'intestazione **Boot** o **Priorità di avvio**, ma potrebbe essere ovunque. Se il supporto per l'avvio da un'unità USB o ottica non è abilitato o ha una priorità inferiore rispetto all'avvio da un disco rigido contenente un altro sistema operativo, l'hardware non si avvierà dal supporto di installazione. Consultare il manuale della scheda madre per informazioni più dettagliate sulla modifica dell'ordine di avvio.

6.4.2 Installazione sul disco rigido

Per i memstick USB con una connessione alla console seriale, il primo prompt chiederà il tipo di terminale da utilizzare per il programma di installazione. Per lo schermo PuTTY o GNU, xterm è il tipo migliore da usare. È possibile utilizzare i seguenti tipi di terminali:

- **ansi** Terminale generico con codice colore
- **vt100** Terminale generico senza colore, opzione più semplice/compatibile, selezionare se nessun altro funziona
- **xterm** finestra terminale. Compatibile con la maggior parte dei client moderni (ad es. PuTTY, schermo)
- **cons25w** Terminale stile console FreeBSD

Per le console VGA, cons25w è scelto dall'installer.

Nota: Si consiglia di accettare tutte le impostazioni predefinite e utilizzare un'installazione tipica, premere Invio a ciascun prompt fino al termine dell'installazione.

Una volta avviato il programma di installazione, la navigazione nelle sue schermate è abbastanza intuitiva e funziona come segue:

- Per selezionare gli elementi, utilizzare i tasti freccia per spostare lo stato attivo della selezione fino a quando l'elemento desiderato non viene evidenziato.
- Per le schermate del programma di installazione che contengono un elenco, utilizzare i tasti freccia su e giù per evidenziare le voci nell'elenco. Usa il tasti freccia sinistra e destra per evidenziare le azioni nella parte inferiore dello schermo come **Selezionare** e **Annullare**.
- Premendo Invio si seleziona un'opzione e si attiva l'azione associata a tale opzione.

Avvio del programma di installazione

Innanzitutto, il programma di installazione richiede di avviare il processo di **installazione** o **Rescue Shell**. Per continuare l'installazione, premere Invio mentre è selezionato **Installare**. L'opzione **Rescue Shell** avvia un prompt della shell di base a cui gli utenti esperti possono eseguire attività per preparare il sistema in modi non completamente supportati dal programma di installazione o per eseguire test diagnostici o riparazioni sul firewall.

La schermata di **selezione della mappa di tasti** è successiva. Per la maggior parte degli utenti con una tastiera standard per PC, premere Invio per selezionare Continuare con **la mappa dei tasti** predefinita. Se la tastiera utilizzata per la console ha un layout diverso, bisogna trovarla nell'elenco e selezionarla. Dopo aver effettuato una selezione, tornare all'inizio dell'elenco e scegliere **Test** o **Continuare**.

Selezionare la partizione

Il passo per la **partizione** preve la selezione del il filesystem per il disco di destinazione del firewall. In Firew4LL 2.3.x e versioni precedenti, l'unica opzione era **UFS**. Il nuovo tipo di filesystem **ZFS** è più affidabile e ha più funzionalità rispetto al vecchio formato UFS, tuttavia ZFS può avere maggiore bisogno di memoria. Entrambi i filesystem funzioneranno su hardware con diversi GB di RAM, ma se l'utilizzo della RAM è fondamentale per altre attività che verranno eseguite su questo firewall, UFS è una scelta più conservativa. Per l'hardware che richiede UEFI, utilizzare ZFS.

Il processo varia leggermente a seconda del tipo di filesystem selezionato, quindi segui la sezione seguente che corrisponde al tipo di filesystem utilizzato da questo firewall.

Nota: Se il programma di installazione non riesce a trovare alcuna unità o se mostra unità errate, è possibile che l'unità desiderata sia collegata a un controller non supportato o a un controller impostato per una modalità non supportata nel BIOS. Vedere *Risoluzione dei problemi di installazione* per assistenza.

UFS

- Selezionare **Auto** (**UFS**)
- Selezionare il disco di destinazione in cui il programma di installazione scriverà il software Firew4LL, ad es. ada0. Il programma di installazione mostrerà ogni disco rigido supportato, collegato al firewall, insieme a qualsiasi volume RAID o gmirror supportato.
- Selezionare **Disco Intero**
- Selezionare **Sì** per confermare che il programma di installazione può sovrascrivere l'intero disco
- Selezionare lo schema di partizione da utilizzare per il disco:
  - **GPT** Il layout della tabella delle partizioni GUID. Utilizzata dalla maggior parte dei moderni sistemi x86. Potrebbe non funzionare su versioni hardware/BIOS precedenti. **Provare prima questo metodo**.
  - **BSD** Etichette senza un MBR, che era noto come «modalità pericolosamente dedicata». Questo metodo dovrebbe funzionare sulla maggior parte dell'hardware che non può utilizzare GPT. Questo era il metodo utilizzato dalle versioni precedenti del software Firew4LL.
  - **MBR** Selezionare questa opzione solo se GPT e BSD non funzionano su un componente hardware specifico.
  - **Altri** Le altre opzioni non sono rilevanti per l'hardware in grado di eseguire il software Firew4LL.
- Selezionare **Fine** per accettare il layout di partizione automatica scelto dall'installatore.

Nota: Le dimensioni della partizione e simili possono essere personalizzate qui, ma non è consigliabile eseguire questo passaggio. Per quasi tutte le installazioni, le dimensioni predefinite sono corrette e ottimali.

- Selezionare **Eseguire** per scrivere il layout della partizione sul disco di destinazione.
- Passa avanti per *continuare con l'installazione*.

ZFS

- Selezionare **Auto** (**ZFS**)
- Selezionare **Tipo/Dischi pool**
- Selezionare il **tipo di dispositivo virtuale**. ZFS supporta più dischi in vari modi per ridondanza e/o capacità aggiuntiva. Sebbene l'utilizzo di più dischi con ZFS sia RAID software, è abbastanza affidabile e migliore dell'uso di un singolo disco.
  - **stripe** Un singolo disco o più dischi aggiunti insieme per creare un disco più grande. Per **i firewall con un singolo disco di destinazione, questa è la scelta corretta**. (RAID 0)
  - **mirror** Due o più dischi che contengono tutti lo stesso contenuto per ridondanza. Può continuare a funzionare anche se un disco si guasta. (RAID 1)

  - **raid10** RAID 1 + 0, n x mirror a 2 vie. Una combinazione di stripe e mirror, che conferisce ridondanza e capacità extra. Può perdere un disco da qualsiasi coppia in qualsiasi momento.
  - **raidzX** RAID ridondante singolo, doppio o triplo. Utilizza 1, 2 o 3 dischi di parità con un pool per fornire capacità e ridondanza extra, quindi uno, due o tre dischi possono fallire prima che un pool venga compromesso. Sebbene simile a RAID 5 e 6, il design RAIDZ presenta differenze significative.

- Selezionare i dischi da utilizzare con il **tipo di dispositivo virtuale** selezionato. Utilizzare i tasti freccia su e giù per evidenziare un disco e Spazio per selezionare i dischi. **Selezionare un disco anche se ce n'è solo uno nell'elenco**. Per mirror o tipi di RAID, selezionare abbastanza dischi per soddisfare i requisiti per il tipo scelto.
- Selezionare OK con i tasti freccia sinistra e destra.
- Scegliere uno **schema di partizione** alternativo solo se il GPT (BIOS) predefinito non funzionerà. Le possibili scelte includono:

  GPT (**BIOS**) Il layout della tabella delle partizioni GUID e l'avvio del BIOS. Utilizzato dalla maggior parte dei moderni sistemi x86. **Provare prima questo metodo**.

  GPT (**UEFI**) GPT con caricatore di avvio UEFI.

  GPT (**BIOS + UEFI**) GPT con avvio sia BIOS che UEFI.

  MBR (**BIOS**) Partizioni legacy in stile MBR con avvio del BIOS.

  GPT + Active (**BIOS**) GPT con la parte di avvio impostata su attivo, con l'avvio del BIOS.

  GPT + Lenovo Fix (**BIOS**) GPT con una correzione di avvio specifica per Lenovo.

  - Modificare le dimensioni di scambio predefinite (facoltativo) selezionando **Dimensione scambio** e immettendo un nuovo valore. In genere la dimensione ottimale è il doppio della RAM disponibile nel firewall, ma con dischi più piccoli potrebbe essere troppo.
  - Lasciare le altre opzioni sullo schermo ai loro valori predefiniti.
  - Riportare la selezione su **Installare** e assicurarsi che **Selezionare** sia evidenziato per l'azione nella parte inferiore dello schermo.
  - Premere Invio per continuare

- Selezionare **Sì** per confermare la selezione del disco di destinazione e riconoscere che il contenuto dei dischi di destinazione verrà distrutto.
- Passare avanti per *continuare con l'installazione*.

Continuare con l'installazione

- Sedetevi, aspettate e bevete qualche sorso di caffè mentre il processo di installazione formatta le unità e copia i file Firew4LL sui dischi di destinazione.
- Selezionare **No** quando viene richiesto di apportare le modifiche finali.
- Selezionare **Riavvire** per riavviare il firewall
- Rimuovere il supporto di installazione dal firewall durante il riavvio, quando l'hardware sta eseguendo il backup ma prima che si avvii dal disco.
- Congratulazioni, l'installazione del software Firew4LL è completa!

6.5 Assegnamento interfacce

Al termine dell'installazione e del riavvio del firewall, il software firewall cerca le interfacce di rete e tenta di assegnare automaticamente i mapping dell'interfaccia.

I profili di assegnazione automatica dell'interfaccia utilizzati dal firewall sono:

|firew4ll| WAN: re1, LAN: re2 **Altri dispositivi** Per altri dispositivi il firewall cerca interfacce comuni e tenta di assegnarle in modo appropriato, ad esempio:

WAN: igb0, LAN: igb1

WAN: em0, LAN: em1

WAN: re1, LAN: re2

Il firmware di fabbrica per i dispositivi dello store di Firew4LL includono mappature predefinite aggiuntive appropriate all'hardware, che varia a seconda dell'hardware ordinato con il dispositivo.

Se il firewall non è in grado di determinare automaticamente il layout dell'interfaccia di rete, presenterà una richiesta di assegnazione dell'interfaccia come nella Figura *Schermata di assegnazione dell'interfaccia*. È qui che alle schede di rete installate nel firewall viene assegnato il ruolo di WAN, LAN e interfacce opzionali (OPT1, OPT2 . . . OPTn).

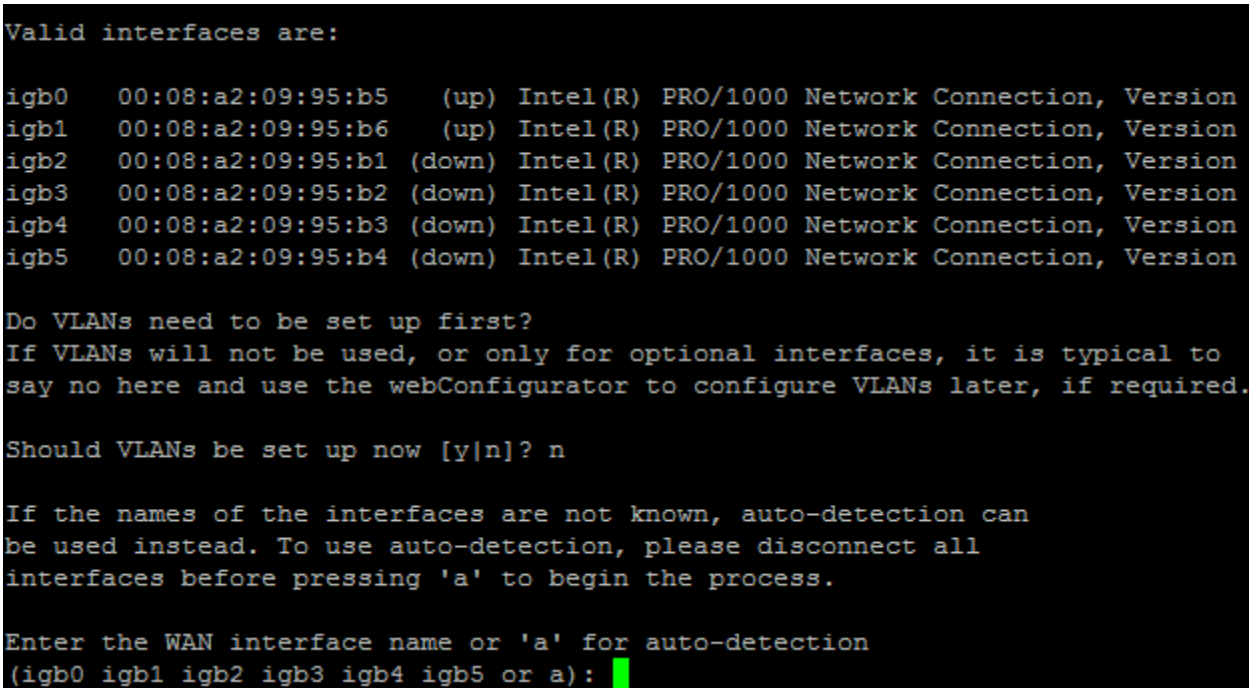


Fig. 1: Schermata di assegnazione dell'interfaccia

Il firewall visualizza un elenco di interfacce di rete rilevate e i relativi indirizzi MAC (Media Access Control), insieme a un'indicazione del loro stato di collegamento se supportato dalla scheda di rete. Lo stato del collegamento è indicato da (su) che appare dopo l'indirizzo MAC se viene rilevato un collegamento su quell'interfaccia.

Nota: L'indirizzo MAC (Media Access Control) di una scheda di rete è un identificatore univoco assegnato a ciascuna scheda e nessuna scheda di rete deve avere lo stesso indirizzo MAC. Se un indirizzo MAC duplicato è presente su una rete, per caso o per spoofing intenzionale, tutti i nodi in conflitto avranno problemi di connettività.

Dopo aver stampato l'elenco delle interfacce di rete, il firewall richiede la configurazione della VLAN. Se si desidera VLAN, rispondere Si, altrimenti, digitare No, quindi premere Invio.

Vedi anche:

Per informazioni sulla configurazione di VLAN, vedere *VLAN*.

Il firewall richiede di impostare prima l'interfaccia WAN. Poiché il firewall in genere contiene più di una scheda di rete, potrebbe presentarsi un dilemma: come stabilire quale scheda di rete è quale? Se l'identità di ogni carta è già nota, inserire i nomi dei dispositivi corretti per ciascuna interfaccia. Se la differenza tra le schede di rete è sconosciuta, il modo più semplice per capirlo è utilizzare la funzione di rilevamento automatico.

Per l'assegnazione automatica dell'interfaccia, attenersi alla seguente procedura:

- Scollegare tutti i cavi di rete dal firewall
- Digitare a e premere Invio
- Inserire un cavo di rete nell'interfaccia WAN del firewall
- Attendere qualche istante affinché il firewall rilevi il collegamento
- Premere Invio

Se tutto è andato bene, il firewall può determinare quale interfaccia utilizzare per WAN.

Ripetere la stessa procedura per la LAN e per le interfacce opzionali, se presenti. Se il firewall stampa un messaggio che indica «Nessun collegamento rilevato», consultare *Assegnazione manuale di interfacce* per ulteriori informazioni sull'ordinamento delle identità della scheda di rete.

Una volta che l'elenco delle interfacce per il firewall è corretto, premere Invio al prompt per ulteriori interfacce. Il firewall chiederà **Vuoi procedere (SN)?** Se l'elenco delle assegnazioni dell'interfaccia di rete è corretto, digitare S, quindi premere Invio. Se l'assegnazione non è corretta, digitare No e premere Invio per ripetere il processo di assegnazione.

Nota: Oltre alla normale modalità di routing/firewall con più interfacce, un firewall può anche funzionare in **modalità Appliance** in cui ha una sola interfaccia (**WAN**). Il firewall inserisce la regola di blocco della GUI sull'interfaccia WAN in modo che un client possa accedere all'interfaccia Web del firewall da quella rete. Le normali funzioni di routing e NAT non sono attive in questa modalità poiché non esiste alcuna interfaccia o rete interna. Questo tipo di configurazione è utile per dispositivi VPN, server DHCP e altri ruoli autonomi.

6.5.1 Assegnazione manuale di interfacce

Se la funzione di rilevamento automatico non ha funzionato, ci sono altri metodi per definire la differenza tra le schede di rete prima dell'installazione. Un modo è tramite l'indirizzo MAC, che il firewall stampa accanto ai nomi dell'interfaccia nella schermata di assegnazione:

```
vmx0  00:0c:29:50:a4:04
vmx1  00:0c:29:50:ec:2f
```

L'indirizzo MAC è talvolta stampato su un adesivo da qualche parte sulla scheda di rete. Per i sistemi virtualizzati, la configurazione della macchina virtuale di solito contiene l'indirizzo MAC per ciascuna scheda di rete. Gli indirizzi MAC sono assegnati dal produttore e ci sono diversi database online che offrono funzionalità di ricerca inversa per gli indirizzi MAC al fine di trovare la società che ha creato la scheda: http://www.8086.net/tools/mac/, http://www.coffer.com/mac_find/ e http://aruljohn.com/mac.pl, tra gli altri.

Schede di rete di marche, modelli o talvolta chipset diversi possono essere rilevate con driver diversi. Potrebbe essere possibile distinguere una scheda basata su Intel utilizzando il driver igb oltre a una scheda Broadcom utilizzando il driver bge guardando le carte stesse e confrontando i nomi stampati sul circuito.

L'ordine di analisi delle schede di rete può essere imprevedibile, a seconda di come è progettato l'hardware. In alcuni casi, i dispositivi con un numero elevato di porte possono utilizzare diversi chipset che analizzano in modi diversi, determinando un ordine imprevisto. Le schede NIC add-on e multiporta sono generalmente analizzate nell'ordine del bus, ma possono variare da scheda a scheda. Se l'hardware ha schede di rete integrate che hanno lo stesso marchio di una scheda di rete aggiuntiva, tenere presente che alcuni sistemi elencheranno prima la scheda di rete integrata e altri no. Nei casi in cui l'ordine di analisi renda ambigue più schede NIC dello stesso tipo, potrebbero essere necessari tentativi ed errori per determinare il posizionamento delle porte e le combinazioni nome/numero del driver.

Dopo aver identificato le schede di rete, digitare il nome di ciascuna scheda nella schermata di assegnazione dell'interfaccia quando richiesto. Nell'esempio sopra, vmx0 sarà WAN e vmx1 sarà LAN. Per assegnare loro questi ruoli, seguire questa procedura:

- Digitare vmx0 e premere Invio quando viene richiesto l'indirizzo WAN
- Digitare vmx1 e premere Invio quando viene richiesto l'indirizzo LAN
- Premere di nuovo Invio per interrompere il processo di assegnazione, poiché questo esempio non contiene alcuna interfaccia opzionale.
- Digitare S e premere Invio per confermare le assegnazioni dell'interfaccia

6.6 Tecniche di installazione alternative

Questa sezione descrive metodi di installazione alternativi che potrebbero essere più facili per determinati requisiti hardware rari.

6.6.1 Installazione con il drive su un'altra macchina

Se è difficile o impossibile eseguire l'avvio da USB o da un'unità DVD/CD all'hardware di destinazione, è possibile utilizzare un altro computer per installare il software Firew4LL sul disco rigido di destinazione. L'unità può quindi essere spostata sulla macchina originale.

Dopo l'installazione, consentire al computer di installazione di riavviarsi e spegnerlo una volta tornato alla schermata del BIOS. Rimuovere il disco rigido dalla macchina di installazione e posizionarlo nel firewall di destinazione. Dopo l'avvio, il firewall richiederà l'assegnazione dell'interfaccia e quindi il resto della configurazione potrebbe essere eseguito normalmente.

Nota: Le versioni attuali del software Firew4LL utilizzano tecniche come ID GPT, ID UFS e metadati ZFS per montare i dischi, quindi anche se il dispositivo potrebbe apparire utilizzando un driver del disco diverso sull'hardware di destinazione effettivo, il sistema operativo sarà comunque in grado di individuare e montare il disco appropriato.

6.6.2 Installazione completa in VMware con reindirizzamento USB

Il reindirizzamento USB in VMware Player e Workstation può essere utilizzato per l'installazione su un disco rigido. Quasi tutti gli adattatori da USB a SATA/IDE o simili funzioneranno a questo scopo. Le seguenti istruzioni sono specifiche per VMware Workstation 12, ma funzioneranno anche su altre versioni recenti.

- Collegare l'unità di destinazione all'adattatore SATA/IDE o al writer SD/CF
- Collegare l'adattatore/scrittore al PC client
- Aprire VMware Workstation sul PC client
- Creare una macchina virtuale, che dovrebbe avere l'USB abilitato (è abilitato per impostazione predefinita)

- Impostare per collegare l'immagine ISO del programma di installazione all'avvio nell'unità CD/DVD virtuale
- Avviare la macchina virtuale
- Premere Esc durante la schermata del BIOS VM per caricare il menu di avvio
- Trovare l'icona dell'adattatore USB nella parte inferiore della finestra di VMware
- Fare clic sull'icona dell'adattatore USB
- Fare clic su **Connettere (Disconnetti dall'host)**
- Selezionare **Unità CD-ROM** dal menu di avvio
- Continuare l'installazione normalmente, assicurarsi che durante il processo di installazione sia selezionata l'unità corretta
- Arrestare
- Rimuovere il disco di destinazione dal PC client
- Collegare il disco di destinazione all'hardware del firewall previsto

Le versioni precedenti della workstation VMware possono utilizzare il reindirizzamento USB automatico per raggiungere lo stesso obiettivo. Scollegare il dispositivo USB, fare clic all'interno della VM per attivarlo, quindi collegare il dispositivo USB. La macchina virtuale deve essere collegata all'unità USB.

6.7 Risoluzione dei problemi di installazione

La maggior parte delle volte, le installazioni finiranno senza problemi. Se così non fosse, le seguenti sezioni descrivono i problemi più comuni e i passaggi per risolverli.

6.7.1 L'avvio dal supporto di installazione non riesce

A causa della vasta gamma di combinazioni hardware in uso, non è raro che un CD o pennetta USB si avvii in modo errato (o per niente). Data la natura imprevedibile del supporto hardware delle materie prime, l'utilizzo dell'hardware da Firew4LL Store è l'unico percorso garantito per il successo.

Detto questo, i problemi e le soluzioni più comuni sono:

Supporto pennetta USB Alcune implementazioni del BIOS possono essere pignoli sul supporto della pennatta USB. Se l'avvio da una levetta non riesce, provane una diversa.

Porte USB 3 Alcune combinazioni di porte e stick USB, in particolare le porte USB 3.0, potrebbero non funzionare correttamente. Prova una pennetta USB una porta USB 2.0.

Problemi del BIOS Aggiornare al BIOS più recente e disabilitare tutte le periferiche non necessarie come Firewire, Floppy Drives e Audio.

Unità ottica sporca Pulire l'unità con un disco di pulizia o una bomboletta di aria compressa o provare un'altra unità.

Supporti ottici difettosi Masterizzare un altro disco e/o masterizzare il disco a una velocità inferiore. Forse provare un'altra marca.

Problemi relativi al cavo SATA/IDE Provare un cavo SATA/IDE diverso tra l'unità CD-ROM e il controller o la scheda madre

Problemi con il caricatore di avvio Ci sono stati casi in cui versioni specifiche del caricatore di avvio da CD di FreeBSD non funzionavano su determinati hardware. In questi casi, consultare *Tecniche di*

installazione alternative per eseguire l'installazione dell'unità di destinazione su un PC separato e quindi spostarlo sull'hardware di destinazione.

Esistono altre tecniche di risoluzione dei problemi elencate nella Wiki della documentazione di Firew4LL in *Risoluzione dei problemi di avvio*.

6.7.2 Avvio da disco rigido dopo l'installazione non riuscita

Al termine dell'installazione e del riavvio del firewall, esistono condizioni che potrebbero impedire l'avvio completo del sistema operativo. I motivi più comuni sono in genere correlati al BIOS. Ad esempio, un'implementazione del BIOS potrebbe non avviarsi da un disco utilizzando GPT o ZFS o potrebbe richiedere UEFI.

Alcuni di questi possono essere aggirati scegliendo diverse opzioni per il layout della partizione durante il processo di installazione. Anche l'aggiornamento del BIOS all'ultima versione disponibile può essere d'aiuto.

La modifica delle opzioni SATA nel BIOS ha migliorato l'avvio anche in alcune situazioni. Se si utilizza un disco rigido SATA, provare a modificare le opzioni SATA nel BIOS per impostazioni come AHCI, Legacy o IDE. AHCI è la modalità migliore da utilizzare con le versioni attuali del software Firew4LL.

Come nella sezione precedente, ci sono altre tecniche di risoluzione dei problemi elencate nella documentazione online in *Risoluzione dei problemi di avvio*.

6.7.3 Collegamento dell'interfaccia non rilevato

Se il firewall lamenta di non aver rilevato il collegamento dell'interfaccia durante l'assegnazione automatica, assicurarsi innanzitutto che il cavo sia scollegato e che l'interfaccia non abbia una spia di collegamento prima di scegliere l'opzione di rilevamento del collegamento. Dopo aver selezionato l'opzione, ricollegare il cavo all'interfaccia e assicurarsi che abbia una luce di collegamento prima di premere Invio. Provare o sostituire il cavo in questione se non mostra una luce di collegamento sullo switch e/o sulla porta NIC una volta collegato.

Se un cavo di rete è collegato direttamente tra due computer e non a uno switch e uno di quei componenti hardware è più vecchio (ad esempio NIC 10/100), assicurarsi che venga utilizzato un cavo crossover. Tutti gli adattatori Gigabit supportano Auto-MDIX e lo gestiranno internamente, ma molti adattatori 10/100 precedenti non lo fanno. Allo stesso modo, se si collega un firewall che esegue il software Firew4LL a uno switch che non supporta Auto-MDIX, utilizzare un cavo patch diretto.

Se l'interfaccia è correttamente connessa ma il firewall continua a non rilevare il collegamento, l'interfaccia di rete potrebbe non rilevare correttamente o segnalare lo stato del collegamento al sistema operativo o al driver. In questo caso, è necessario assegnare manualmente le interfacce.

6.7.4 Risoluzione dei problemi hardware

I seguenti suggerimenti ti aiuteranno a risolvere problemi hardware generali.

Avvio da USB

Se l'avvio si interrompe con al prompt `mountroot>` durante l'avvio dal CD live, in genere con unità CD/DVD USB, passare al prompt dell'installazione dal menu di avvio ed eseguire quanto segue:

```
set kern.cam.boot_delay=10000
boot
```

A quel punto l'avvio continuerà normalmente.

Se il firewall è in esecuzione in modo permanente da un supporto che richiede questo ritardo, modificare `/boot/loader.conf.local` e inserire la seguente riga:

```
kern.cam.boot_delay=10000
```

Rimuovere l'hardware non necessario

Se il firewall contiene hardware che non verrà utilizzato, rimuoverlo o disabilitarlo. Questo di solito non è un problema, ma può causare problemi e ha il potenziale per ridurre le prestazioni. Se un componente hardware non utilizzato è rimovibile, estrarlo dal firewall o disabilitarlo nel BIOS.

Disabilitare il sistema operativo PNP nel BIOS

Questa è una correzione comune per l'hardware precedente. Le schermate di configurazione del BIOS possono contenere un'impostazione per il **sistema operativo PNP** o il **sistema operativo Plug and Play**, che deve essere impostato su disabilitato o no. Alcuni hanno un'impostazione per il sistema operativo, che di solito dovrebbe essere impostata su altri.

Aggiornare il BIOS

La seconda soluzione più comune per i problemi hardware è l'aggiornamento del BIOS all'ultima revisione. Le persone sembrano avere difficoltà a crederci, ma fidati di noi, fallo. Gli aggiornamenti del BIOS risolvono comunemente i bug nell'hardware. Non è raro incontrare problemi indotti da bug hardware su sistemi che sono stati stabili con Windows in esecuzione per lunghi periodi di tempo. Windows non attiva il bug o ha una soluzione, come abbiamo riscontrato in più occasioni. Le cose che gli aggiornamenti del BIOS possono risolvere includono: mancato avvio, problemi di mantenimento del tempo, instabilità generale e altri problemi come la compatibilità hardware.

Ripristinare le impostazioni del BIOS ai valori predefiniti di fabbrica

I sistemi riciclati possono avere una configurazione BIOS atipica. La maggior parte contiene un'opzione che consente di caricare le opzioni predefinite di fabbrica. Utilizzare questa opzione per resettare le impostazioni del BIOS.

Altre impostazioni del BIOS

Se il BIOS consente la configurazione della gestione dell'alimentazione, provare ad attivare questa opzione. Cercare qualsiasi altra cosa non funzioni, ma che sembri rilevante per l'installazione. Se si è arrivati questo punto, l'hardware di destinazione è probabilmente una causa persa e potrebbe essere necessario un hardware alternativo. Controllare anche se il BIOS ha un registro eventi che potrebbe elencare errori hardware come errori del test di memoria.

Se l'hardware utilizza un chipset nuovo o recente, potrebbe funzionare una versione di sviluppo del software Firew4LL. Controllare la pagina Snapshots per vedere se c'è uno sviluppo (ad esempio Beta o release candidate) da provare

Altri problemi hardware

L'hardware di destinazione potrebbe essere difettoso, il che potrebbe rivelare un test con software diagnostico. Testare il disco rigido con software diagnostico dell'OEM e testare la memoria con un programma come memtest86+. Questi e altri strumenti sono disponibili sul «Ultimate Boot CD», che è precaricato con molti strumenti diagnostici hardware gratuiti.

Assicurati anche che tutte le ventole girino a velocità elevata e che nessun componente si surriscaldi. Se si tratta di unhardware riutilizzato più vecchio, la pulizia dell'aria compressa/in scatola delle ventole e dei dissipatori di calore può fare miracoli.

6.8 Aggiornamento di un'installazione esistente

Il software Firew4LL può essere aggiornato in modo affidabile da una versione precedente a una versione corrente.

Mantenendo un firewall che esegue il software Firew4LL aggiornato con una versione supportata corrente, il firewall non sarà mai obsoleto. Rilasciamo periodicamente nuove versioni che contengono nuove funzionalità, aggiornamenti, correzioni di errori e varie altre modifiche. Nella maggior parte dei casi, aggiornare un'installazione di Firew4LL è semplice.

Il problema più comune riscontrato durante gli aggiornamenti sono le regressioni specifiche dell'hardware da una versione di FreeBSD a un'altra, sebbene siano rare. Le versioni aggiornate riparano più hardware di quanto non si rompano, ma le regressioni sono sempre possibili.

Pubblichiamo note di aggiornamento insieme a rilasci per aiutare a guidare eventuali potenziali insidie di aggiornamento. Queste note variano da versione a versione, la versione più recente è disponibile nella Guida all'aggiornamento.

6.8.1 Effettuare un backup... e un piano di backup

Prima di apportare modifiche a un firewall, è consigliabile eseguire un backup utilizzando WebGUI:

- Passare a **Diagnostica> Backup/Ripristino**
- Impostare l'"**area di backup** su *TUTTI* nella sezione **Configurazione backup** della pagina
- Fare clic  su **Scaricare**
- Salvare questo file in un luogo sicuro

Conservare più copie del file di backup in diverse posizioni sicure. I clienti che utilizzano il pacchetto Backup configurazione automatica possono effettuare un backup manuale con una nota che identifica la modifica, che è crittografata e memorizzata sui nostri server.

6.8.2 Aggiornamento

Esistono diversi metodi disponibili per l'aggiornamento di una normale installazione del software Firew4LL. È possibile utilizzare WebGUI o la console.

Aggiornamento tramite WebGUI

La funzione di **aggiornamento automatico** contatta un server Firew4LL e determina se esiste una versione di rilascio più recente della versione sul firewall. Questo controllo viene eseguito quando un amministratore visita la dashboard o **Sistema> Aggiornamento**.

Fare clic su  **Confermare** su **Sistema> Aggiornamento** per avviare l'aggiornamento, se disponibile.

L'aggiornamento richiede alcuni minuti per il download e l'applicazione, a seconda della velocità della connessione Internet utilizzata e della velocità dell'hardware del firewall. Il firewall si riavvierà automaticamente al termine.

Aggiornamento tramite la console

Un aggiornamento può anche essere eseguito dalla console. L'opzione console è disponibile da qualsiasi mezzo disponibile per l'accesso alla console: video/tastiera, console seriale o SSH. Una volta connesso alla console del firewall, avviare il processo di aggiornamento selezionando l'opzione di menu 13.

In alternativa, da un prompt della shell in esecuzione come root, eseguire manualmente il seguente comando:

```
# pfSense-upgrade
```

Reinstallazione/Aggiornamento della configurazione

Se un aggiornamento non funzionerà correttamente su un'installazione esistente, il file di configurazione può essere ripristinato su una copia appena installata del software Firew4LL. Una configurazione precedente può sempre essere importata in una nuova versione. Il codice di aggiornamento apporterà le modifiche necessarie alla configurazione in modo che funzioni con la versione corrente del software.

6.8.3 Impostazioni di aggiornamento

Branch/Tracking Snapshots

Per impostazione predefinita, il controllo degli aggiornamenti cerca solo le versioni rilasciate ufficialmente del software Firew4LL, ma questo metodo può essere utilizzato anche per tenere traccia degli snapshot di sviluppo. La posizione di aggiornamento può essere modificata visitando **Sistema> Aggiornamento**, scheda **Impostazioni aggiornamento** e selezionando un altro **Branch** nella sezione **Branch del firmware**.

Le versioni stabili sono l'opzione migliore, in quanto vedono il maggior numero di test e sono ragionevolmente sicure e senza problemi. Tuttavia, come con qualsiasi aggiornamento, visitare il sito Web Firew4LL e leggere le note di aggiornamento per quella versione e consultare la Guida all'aggiornamento.

Scegliere *Snapshot di sviluppo* per passare da un firewall al monitoraggio delle build di snapshot di sviluppo. In genere si tratta di Snapshot per la prossima versione secondaria del branch di manutenzione.

In alcuni casi, l'opzione *Versione più recente* sarà nell'elenco. Questa opzione consente al firewall di tenere traccia delle snapshot per la prossima versione di aggiornamento principale. Questo è più rischioso, ma in alcuni casi potrebbe essere necessario per un hardware più recente o nuove funzionalità non ancora rilasciate. Consultare il forum e testare in un laboratorio per vedere se queste snapshot sono stabili in un ambiente particolare. Non consigliamo generalmente di eseguirli in produzione.

Controllo dalla Dashboard

La casella di **controllo della dashboard** su **Sistema> Aggiornamento**, nella scheda delle **Impostazioni dei aggiornamento** controlla se un aggiornamento è o meno adatto al widget delle i**nformazioni di sistema** sulla dashboard. Sui firewall con risorse ridotte o dischi lenti, la disabilitazione di questo controllo ridurrà il carico causato dall'esecuzione del controllo ogni volta che un amministratore visualizza la dashboard.

GitSync

Questa sezione è destinata agli sviluppatori e non deve essere utilizzata dagli utenti finali. Lasciare le impostazioni in quest'area vuote o disabilitate.

6.9 Ottimizzazione filesystem

Le impostazioni predefinite per il filesystem sono le migliori per la maggior parte degli ambienti, tuttavia ci sono occasioni che richiedono lievi modifiche per migliorare la stabilità, le prestazioni o la longevità del filesystem.

6.9.1 Abilitazione del supporto TRIM

Il programma di installazione per la versione di fabbrica di Firew4LL imposta automaticamente TRIM. Sia la versione di fabbrica che la versione CE di Firew4LL 2.4 supporta TRIM in modo originale quando si utilizza ZFS.

Sebbene sia possibile abilitare manualmente TRIM, il supporto è imprevedibile nell'hardware, quindi non forniamo istruzioni su come abilitare la funzione.

Attivazione di un controllo del filesystem

Firew4LL eseguirà un controllo del filesystem (fsck) all'avvio quando rileva un filesystem impuro, in genere dopo un'interruzione di corrente o altri improvvisi riavvii o arresti impuri. In rari casi, non è sempre sufficiente, poiché un filesystem può essere danneggiato in altri modi che potrebbero non lasciare sempre l'unità contrassegnata come sporca.

In questi casi:

- Connettersi alla console
- Scegliere l'opzione di menu per riavviare dal menu della console (5)
- Immettere F («f» maiuscola) per forzare un controllo del filesystem durante la sequenza di avvio anche se l'unità è considerata pulita

Tale opzione non è presente su tutti i firewall in quanto non è compatibile con alcune implementazioni del BIOS. Se tale opzione non è presente:

- Riavviare il firewall in modalità utente singolo selezionando l'opzione 2 dal menu di avvio
- Premere Invio quando richiesto per una shell
- Inserire `fsck -y /`
- Ripetere il comando almeno 3 volte o fino a quando non vengono rilevati errori, anche se il filesystem viene rilevato come pulito

CAPITOLO 7

Configurazione Firew4ll

7.1 Configurazione guidata

La prima volta che un utente a accede ad un Firew4LL, il firewall presenta automaticamente la configurazione guidata. La prima pagina della guida è presentata nella figura *Schermata di avvio della configurazione guidata.*

Fare clic su » **Avanti** per avviare il processo di configurazione con la guida

Suggerimento: Usare la configurazione guidata è opzionale. Fare clic sul logo di Firew4LL in alto a sinistra della pagina per uscire dalla guida in ogni momento.

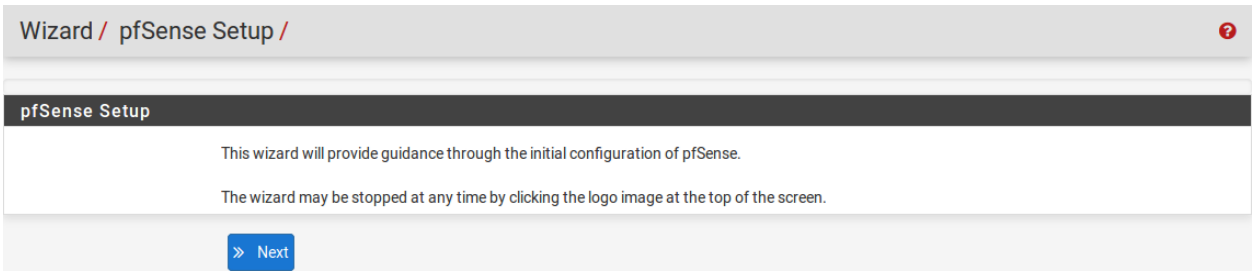


Fig. 1: Schermata di avvio della configurazione guidata

7.1.1 Schermata per le Informazioni generali

La prossima schermata (Figura *Schermata delle informazioni generali*) configura il nome di questo firewall, il dominio in cui risiede, il server ei del DNS per il firewall.

Nome dell'Host Il nome dell'host può essere qualcosa di simile, ma deve iniziare con una lettera e deve contenere solo lettere, numeri, o un trattino.

Dominio Inserire un dominio, per esempio esempio.com. Se questa rete non ha un dominio, usare <Qualcosa> .dominiolocale, dove <Qualcosa> è un altro identificatore: un nome di azienda, cognome, nickname, ecc Per esempio, azienda.dominiolocale Il nome dell'host e il nome del dominio sono combinati per formare un nome di dominio pienamente qualificato per questo firewall.

Server del DNS primario/secondario L'Indirizzo IP del server DNS primario e del server DNS secondario possono essere riempiti, se richiesto e se conosciuti

Questi server DNS possono essere lasciati vuoti se il risolutore del DNS rimane attivo usando le impostazioni predefinite. La configurazione di Firew4LL predefinita ha il risolutore del DNS attivo nella modalità risolutore (non nella modalità d'inoltro), quando si imposta questa modalità, il risolutore del DNS non ha bisogno dei server di DNS del d'inoltro perché comunicherà direttamente con i server DNS della root e con i server di DNS autorizzati. Per forzare il firewall di usare questi server DNS configurati, abilitare la modalità d'inoltro nel risolutore DNS o usare il forwader del DNS

Se questo firewall ha un tipo di WAN dinamico come DHCP, PPTP o PPPoE, queste potrebbero essere assegnate automaticamente dall'ISP e possono essere lasciate vuote.

DNS di Override Quando selezionato, un provider di servizi Internet della WAN dinamica può fornire i server di DNS del che ereditano quelle impostazioni manualmente. Per forzare l'utilizzo dei soli server DNS configurati manualmente, disabilitare questa opzione.

Vedi anche:

Per maggiori informazioni sulla configurazione del risolutore del DNS, vedere *Risolutore DNS*

Fare clic su » **Avanti** per continuare

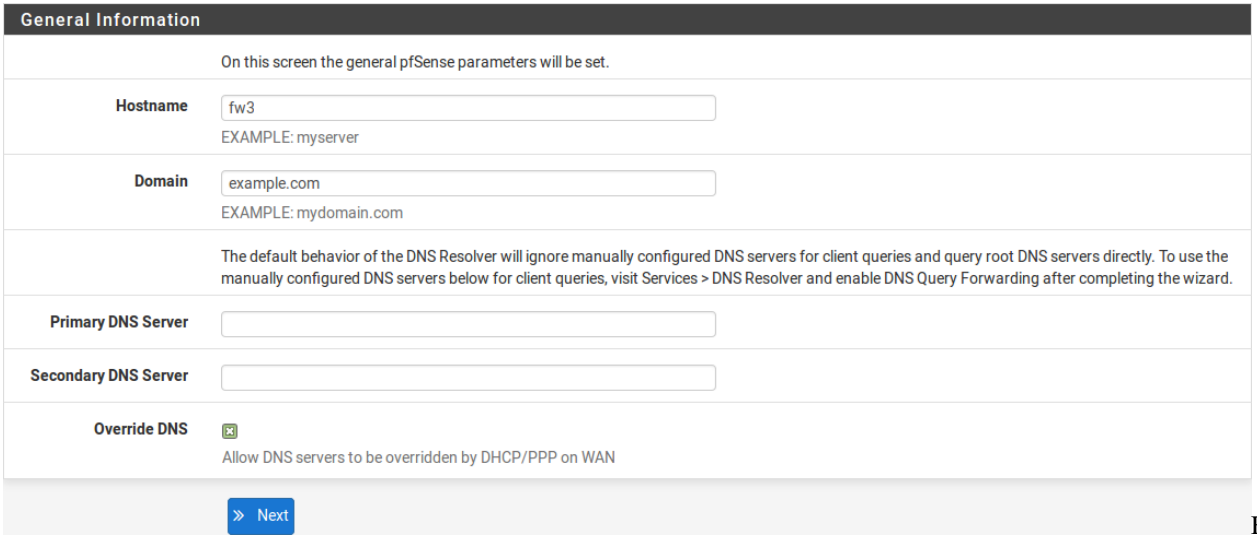


Fig. 2: Schermata delle informazioni generali

7.1.2 Configurazione del NTP e della zona oraria

La prossima schermata (Figura *Schermata del NTP e della timezone*) contiene impostazioni relative all'ora.

Hostname del server dell'ora Un nome dell'host del server con protocollo dell'ora della rete (NTP) o indirizzo IP. Fintanto un server con NTP specifico non sia richiesto, come uno sulla LAN, la cosa migliore è lasciare l'hostname del server dell'orario predefinito 0.|firew4ll|.pool.ntp.org. Questo valore prenderà un server qualsiasi da un pool di host noti.

Questa numerazione è specifica in modo che .pool.ntp.org operi e assicuri che ogni indirizzo sia preso da un pool di server con NTP unici così che lo stesso server non sia utilizzato due volte

Zona oraria Scegliere una zona nominata geograficamente che corrisponda meglio al luogo di questo firewall, o qualsiasi altra zona desiderata.

Fare clic su » **Avanti** per continuare

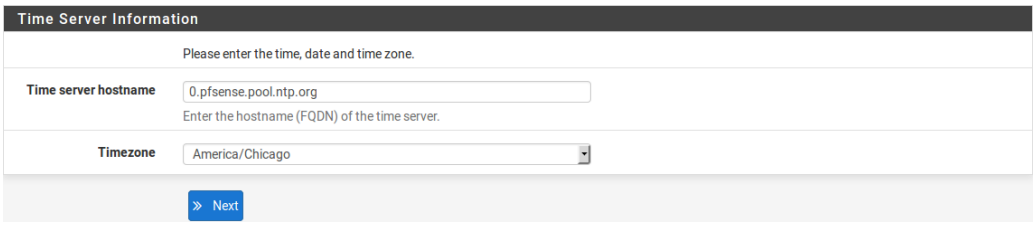


Fig 3: Schermata del NTP e della zona oraria

7.1.3 Configurazione dell'interfaccia WAN

La prossima pagina della guida configura l'interfaccia WAN del firewall. Questa è la rete esterna che affronta l'ISP o il router di upstream, così che la guida offra scelte di configurazione che supportino diversi tipi di connessione ISP comuni.

Tipologia WAN La tipologia selezionata (Figura *Configurazione della WAN*) deve corrispondere alla tipologia di WAN dall'ISP richiesta, o qualsiasi sia il precedente firewall o il router che sia stato configurato da utilizzare. Le scelte possibili sono *statica*, *DHCP*, *PPPoE*, e *PPTP*. La scelta predefinita è DHCP per il fatto che è una delle più comuni, e per la maggioranza dei casi queste impostazioni permettono al firewall di "lavorare" senza una configurazione aggiuntiva. Se la tipologia di WAN non è nota, o le impostazioni specifiche per la Wan non sono conosciute, questa informazione deve essere ottenuta dall'ISP. Se la tipologia di WAN richiesta non è disponibile nella guida, o per avere maggiori informazioni sulle diverse tipologie di WAN, vedere *Configurazione e tipologie di interfaccia*

Nota: Se l'interfaccia WAN è wireless, saranno presentate opzioni aggiuntive dalla guida che non sono illustrate da questa guida della installazione di base. Fare riferimento a *Wireless* , che ha una sezione sulla WAN wireless del maggiori informazioni. Se qualcuna si queste informazioni fosse poco chiara, saltare la configurazione della WAN per ora, e poi eseguire la configurazione del wireless in un secondo momento.

Fig. 4: Configurazione dell'interfaccia WAN

Indirizzo MAC Questo campo, mostrato in Figura *Configurazione generale della WAN*, cambia l'Indirizzo MAC usato sull'interfaccia di rete WAN. E" anche conosciuto come 'sproofing' dell'indirizzo MAC.

Nota: I problemi attenuati dallo sproofing dell'indirizzo MAC sono di solito temporanei e facilmente aggirabili. La migliore procedura è mantenere l'indirizzo MAC originale dell'hardware, ricorrendo allo spoofing solo quando assolutamente necessario.

Cambiare l'indirizzo MAC può risultare utile per rimpiazzare un pezzo esistente delle apparecchiature di rete. Alcuni ISP, in primo luogo quelli forniti di cavi, non funzionano perfettamente se il nuovo indirizzo MAC è rilevato. Alcuni provider internet richiedono un ciclo di potenza del modem, altri richiedono la registrazione del nuovo indirizzo sul telefono. In aggiunta, se questa connessione WAN è su un segmento di rete con altri sistemi che lo posizionano via ARP, cambiare il MAC da corrispondere e il vecchio pezzo potrebbe anche rendere la transizione più facile, piuttosto che dover pulire le memorie cache ARP o aggiornare le voci dell'ARP statica.

Unità di Trasmissione Massima (MTU) Il campo MTU, mostrato nella figura *Configurazione generale della WAN*, può essere lasciato vuoto di solito, ma può essere cambiato se necessario. Alcune situazioni possono richiedere un MTU più basso per assicurare che i pacchetti sia dimensionati in maniera appropriata per la connessione internet. Nella maggior parte dei casi, l'impostazione predefinita assumer valori per cui la tipologia di connessione WAN possa funzionare correttamente.

Dimensione del segmento massimo (MSS) L'MSS, mostrato nella figura *Configurazione generale della WAN*, è lasciato vuoto di solito, ma può essere cambiato se necessario. Questo campo abilita il clamping del MSS, che assicura che la dimensione dei pacchetti TCP rimanga adeguatamente piccola per connessioni internet particolari.

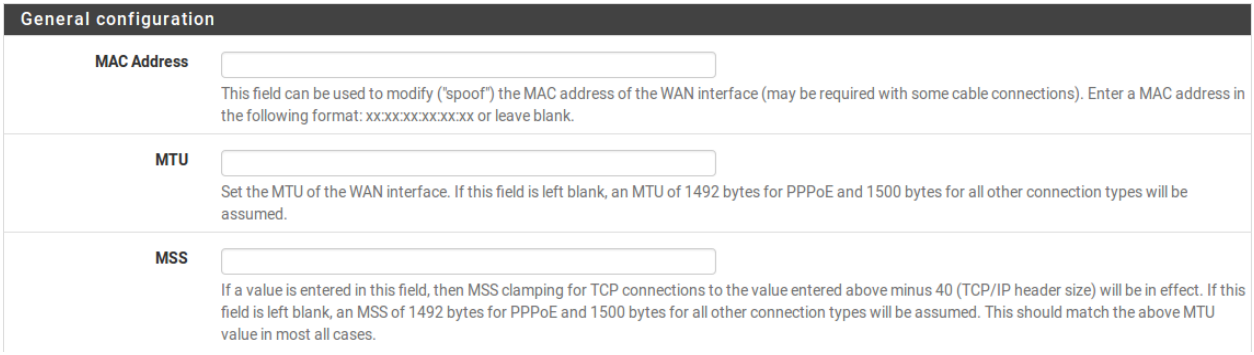


Fig. 5: Configurazione generale della WAN

Configurazione dell'IP statico Se è selezionata la scelta «Statica» per il tipo di WAN, l'"**indirizzo IP**, la **maschera di sottorete** e il **gateway upstream** devono essere tutti compilati (Figura *Impostazioni degli IP statici*). Queste informazioni devono essere ottenute dall'ISP o da chi controlla la rete dal lato WAN di questo firewall. L'"**indirizzo IP** e il **gateway di upstream** devono risiedere entrambi nella stessa sottorete.

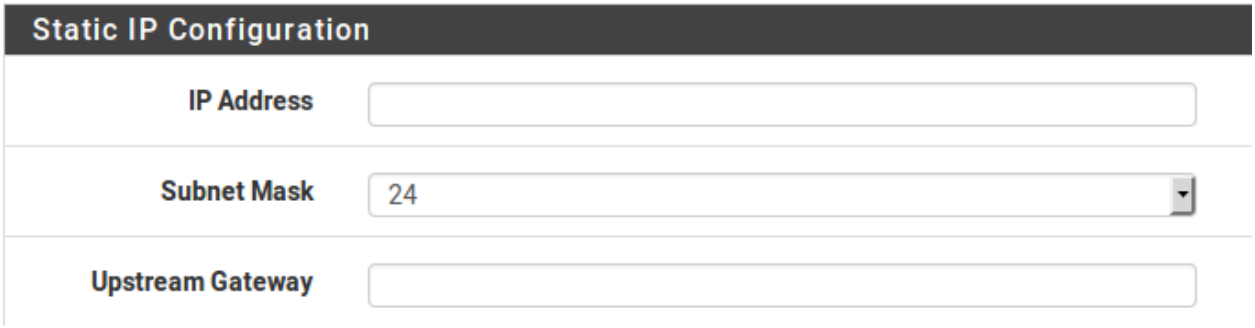


Fig. 6: Impostazioni degli IP statici.

Nome dell'host DHCP Questo campo (Figura *Impostazioni del nome dell'host DHCP*) è richiesto solo da pochi ISP. Questo valore è inviato insieme alla richiesta da parte del DHCP di ottenere l'indirizzo IP

della WAN. Se Il valore di questo campo è sconosciuto, lasciare vuoto fintanto che non sia indirizzato diversamente dall'ISP.

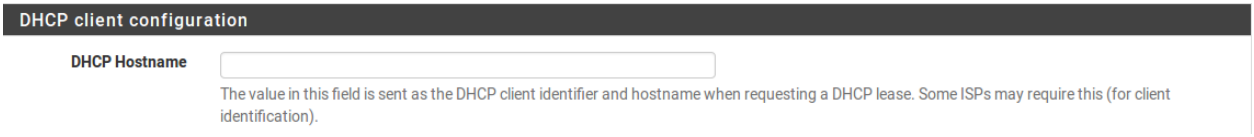


Fig. 7: Impostazioni del nome dell'host DHCP

Configurazione PPPoE Quando si usa la tipologia PPPoE (Protocollo Point-to-Point per Ethernet) della WAN (Figura Configurazione PPPoE), i campi **nome utente** e **password PPPoE** Sono richiesti, al minimo. I Valori per questi campi sono determinati dall'ISP.

Nome utente del PPPoE Il nome d'accesso per l'autenticazione PPPoE. Il formato è controllato dall'ISP, ma di solito usa un indirizzo e-mail come mionome@esempio.com.

Password PPPoE La password per accedere all'account di posta specificato dal nome utente. La password è mascherata per impostazione predefinita. per vedere la password inserita, selezionare **Rivelare i caratteri della password**.

Nome del servizio PPPoE Il nome del servizio PPPoE può essere richiesto da un ISP, ma di solito è lasciato vuoto. Quando è in dubbio, lasciare vuoto o contattare l'ISP e domandare se è necessario.

Chiamata PPPoE su richiesta Fa in modo che pSsense lasci la connessione down/offline fino a quando i dati richiesti hanno bidogno di una connessione internet. Gli accessi PPPoE avvengono abbastanza velocemente, quindi nella maggior parte dei casi il ritardo, mentre la connessione è impostata, è trascurabile. Se i servizi pubblici sono ospitati all'interno di this firewall, non selezionare questa opione perché una connessione online deve essere mantenuta il più possibile in quel caso. Da notare, inoltre, che questa scelta non lascerà cadere una connessione già esistente.

Minimo tempo di attesa PPPoE Specifica quanto tempo Firew4LL concederà alla connessione PPPoE per rimanere up senza trasmettere dati prima di disconnetterla. Questo è utile solo quando accoppiato alla chiamata su richiesta, e di solito è lasciato vuoto (disabilitato)

Nota: questa opzione richiede anche la disattivazione del monitoraggio del gateway, altrimenti la connessione non sarà mai inattiva.

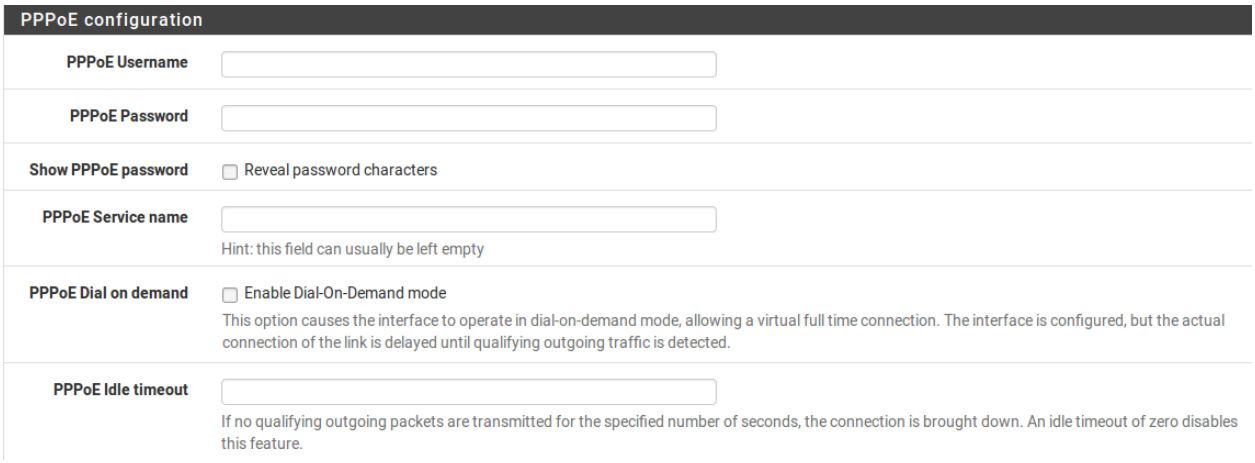


Fig. 8: Configurazione PPPoE

Configurazione PPPTP La tipologia PPTP (Protocollo di tunneling point-to-point) della WAN (Figura *Configurazione della WAN PPTP*) è per gli ISP che richiedono un accesso PPTP, non per connettersi a

una VPN PPTP da remoto. Queste impostazioni, molto simili alle impostazioni PPPoE, saranno fornite dall'ISP. Sono richieste alcune opzioni aggiuntive:

Indirizzo IP locale L'Indirizzo locale (di solito privato) usato da questo firewall è stabilito dalla connessione PPTP.

Maschera di Sottorete CIDR La maschera di sottorete per l'indirizzo locale.

Indirizzo IP da remoto L'Indirizzo server PPTP, che è di solito all'interno della stessa sottorete come **Indirizzo IP locale**

Queste ultime opzioni, viste nella Figura *Opzioni di filtraggio dell'ingresso integrate*, sono utili per prevenire che il traffico non valido entri della rete protetta attraverso questo firewall, è anche conosciuto come "Filtro d'ingresso".

Reti RFC 1918 private bloccate Blocca le connessioni provenienti da reti registrate privato come 192.168.xx e 10.xxx che tentano di entrare nell'interfaccia WAN. Una lista completa di queste reti si trova nella sezione *Indirizzi IP privati*.

Reti bogon bloccate Quando Attiva, il firewall blocca il traffico in entrata se proviene da uno spazio riservato o da uno spazio IP non ancora assegnato che non dovrebbe essere utilizzato. la lista di reti bogon è aggiornata periodicamente in background, e non richiede alcuna manutenzione. Le reti bogon sono spiegate in maniera approfondita nella sezione *Reti bogon bloccate*.

Fare clic su » **Avanti** per continuare una volta che le impostazioni della WAN sono state inserite

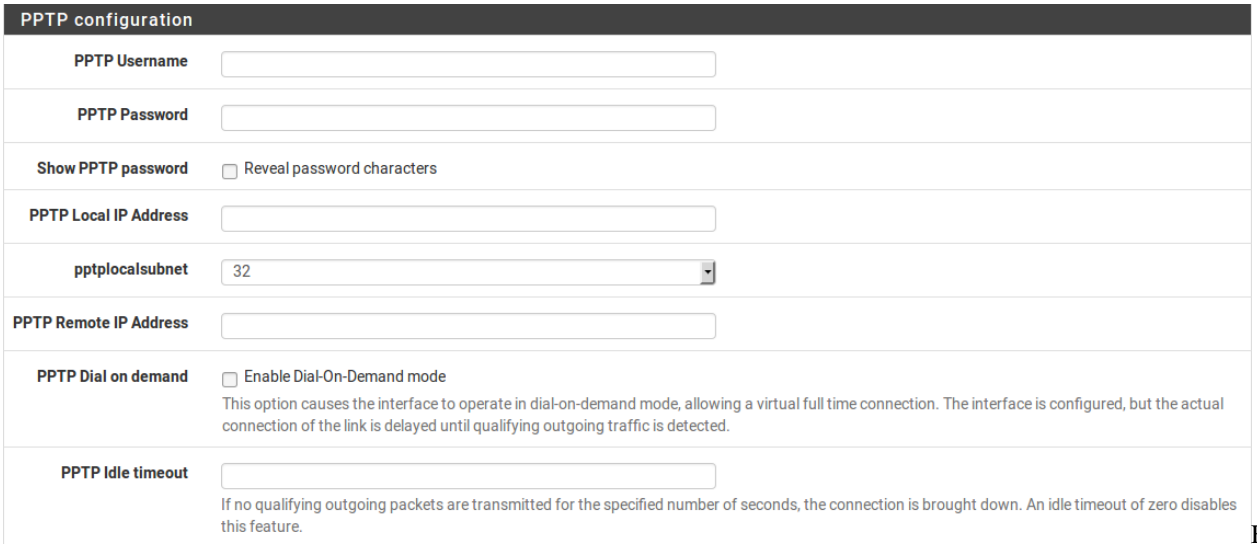


Fig. 9: Configurazione della WAN PPTP

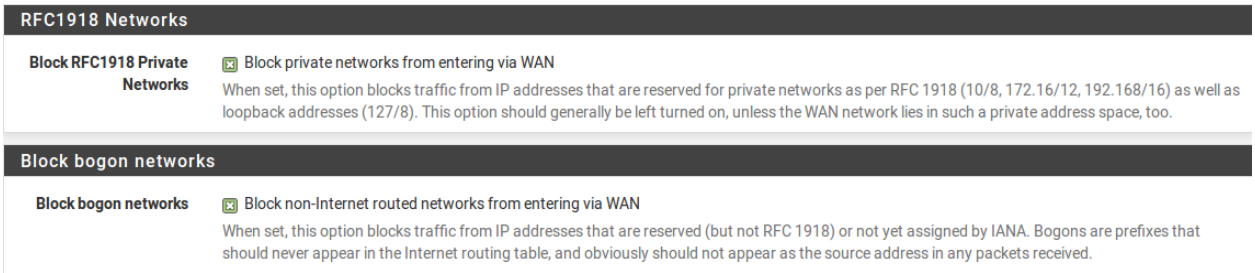


Fig. 10: Opzioni di filtraggio dell'ingresso integrate

7.1.4 Configurazione dell" interfaccia LAN

Questa pagina della guida configura l"**indirizzo IP della LAN** e la **maschera di sottorete** (Figura *Configurazione della LAN*).

Se questo firewall non si connette a nessun'altra rete via VPN, la rete predefinita 192.168.1.0/24 può essere accettabile. Se questa rete deve essere connessa a un'altra rete, che includa la via VPN da locazioni a distanza, scegliere un intervallo di indirizzi IP privati molto più oscuro dell'impostazione predefinita comune 192.168.1.0/24. Lo spazio IP all'interno del blocco di indirizzi privati RFC 1918 172.16.0.0/12 è generalmente il meno frequentemente usato, quindi scegliere qualcuno tra 172.16.xx e 172.31.xx per evitare problemi con la connettività VPN.

Se la LAN è 192.168.1.x e un client da remoto è in un hotspot wireless che usa 192.168.1.x (molto comune), il client non potrà comunicare attraverso la VPN. In quel Caso, 192.168.1.x è la rete locale per il cliente nell'hotspot, non la rete remota sulla VPN.

Se l"**indirizzo IP della** LAN deve essere cambiato, inserirlo qui insieme alla nuova **maschera di sottorete**. Se queste impostazioni sono cambiate, anche l'indirizzo IP del computer usato per completare la guida deve essere cambiato, se è connesso attraverso la rete LAN. Rilasciare/rinnovare la locazione DHCP, o eseguire una "riparazione" o "diagnosi" sull'interfaccia di rete quando la configurazione guidata è finita.

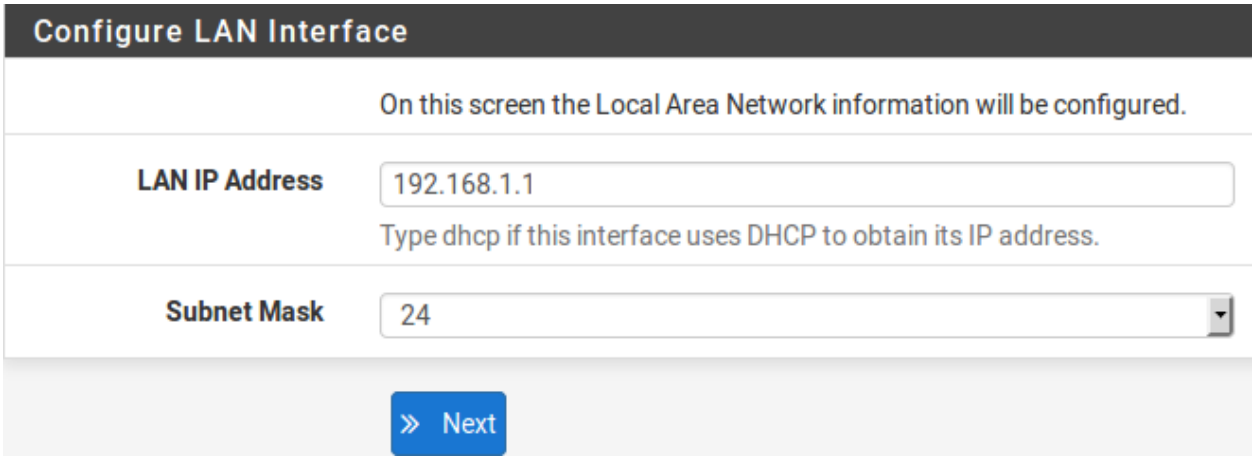


Fig. 11: Configurazione della LAN.

Fare clic su » **Avanti** per continuare

7.1.5 Impostare la password amministrativa

Il prossimo passo è cambiare le password amministrativa per la WebGUI come mostrato nella Figura *Cambiare la password amministrativa*. La maniera migliore è usare la password forte e sicura, ma nessuna restrizione è imposta automaticamente. Inserire la password nella casella della **password amministrativa** e nella casella della conferma per essere sicuri che sia stata inserita correttamente.

Fare clic su » **Avanti** per continuare

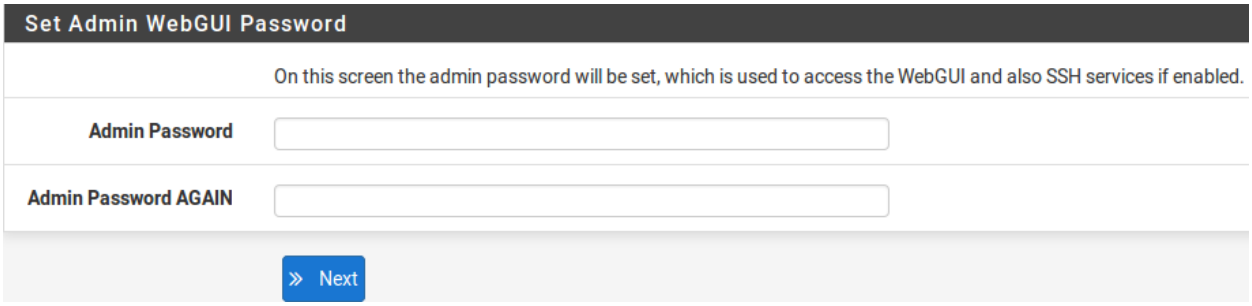


Fig. 12: Cambiare la password Amministrativa.

7.1.6 Completare la configurazione guidata

Questa procedura completa la configurazione guidata delle impostazioni. Fare clic su **ricaricare** (Figura *Ricaricare la WebGUI di \firew4ll*) e la WebGUI applicherà le impostazioni dalla procedura guidata e ricaricherà i servizi modificati dalla procedura guidata.

Suggerimento: Se l'Indirizzo IP della LAN è stato cambiato dalla guida e la guida è stata iniziata dalla lan, regolare l'indirizzo IP del computer client di conseguenza dopo aver fatto click su ricaricare.

Quando viene richiesto di effettuare nuovamente l'accesso, inserire la password nuova. il nome utente rimane admin.

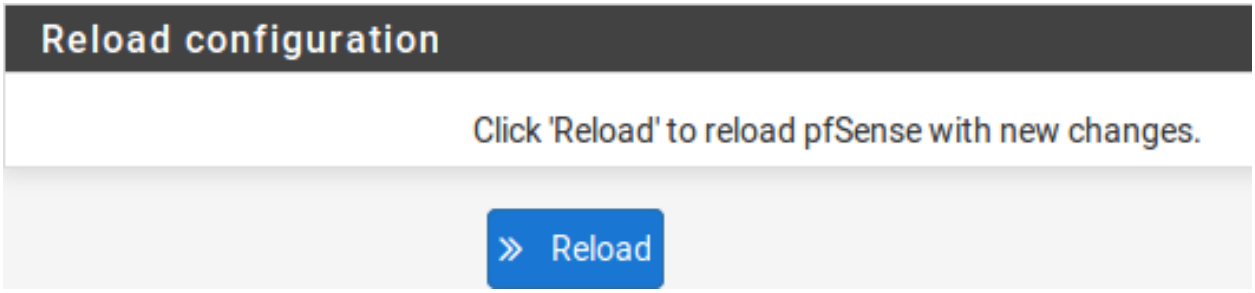


Fig. 13: Ricaricare la WebGUI di Firew4LL

A questo punto il firewall avrà connettività di base a internet tramite WAN e client sul lato LAN saranno in grado di raggiungere i siti internet attraverso questo firewall.

Se in qualsiasi momento questa configurazione iniziale deve essere ripetuta, rivisitare la procedura guidata **di Sistema> Configurazione guidata** dall'interno della WebGUI.

7.2 Configurazione dell'interfaccia

Gli aspetti fondamentali della configurazione dell'interfaccia possono essere eseguiti alla console e nella procedura guidata di configurazione per l'avvio, ma le modifiche apportate possono anche essere fatte dopo la configurazione iniziale visitando le pagine del menu **Interfacce**. Alcuni elementi di base sono trattati qui, i dettagli possono essere trovati in *Tipi di interfaccia e configurazione*.

7.2.1 Assegnare le Interfacce

A ulteriori interfacce aggiunte dopo la configurazione iniziale possono essere assegnati ruoli visitando **Interfacce> (assegnare)**. Ci sono numerose schede in quella pagina utilizzate per l'assegnazione e la creazione di diversi tipi di interfacce. Le due schede più comunemente utilizzate sono **assegnazioni di interfaccia** e **VLAN**.

Vedi anche:

La configurazione VLAN è inclusa nelle *LAN virtuali (VLAN)*.

La scheda delle assegnazioni di interfaccia mostra un elenco di tutte le interfacce attualmente assegnate: WAN, LAN, e tutte le voci OPTX configurate sul firewall. Accanto Ad ogni interfaccia c'è un elenco a discesa di tutte le interfacce/porte di rete presenti nel sistema. Questo elenco comprende le interfacce hardware, le interfacce vlan e altri tipi di interfaccia virtuale. L'indirizzo MAC, il tag VLAN o altre informazioni di identificazione sono stampate lungo il lato del nome dell'interfaccia per facilitare l'identificazione.

Le altre schede, molto simili alla scheda VLAN, sono lì per creare interfacce aggiuntive che possono essere assegnate dopo. Tutti questi tipi di interfaccia sono trattati in *Tipi e configurazioni di interfaccia*.

Per modificare l'assegnazione di un'interfaccia esistente a un'altra porta di rete:

- Andare alla pagina **Interfacce> (assegnare)**
- Individuare l'interfaccia da modificare nella lista
- Selezionare una la nuova porta di rete dall'elenco a discesa sulla riga per quella interfaccia
- Cliccare su **Salvare**

Per aggiungere una nuova interfaccia dall'elenco delle porte di rete inutilizzate:

- Andare alla pagina alle **Interfacce> (assegnare)**
- Seleziona una la porta da usare dall'elenco a discesa etichettato porte di rete disponibili
- Fare clic su  **aggiungere**

Questa azione aggiungerà un'altra linea con una nuova interfaccia OPT numerata superiore a qualsiasi interfaccia OPT esistente, o se questa è la prima interfaccia aggiuntiva, *OPT1*.

7.2.2 Nozioni di base sulla configurazione dell'interfaccia

Le interfacce sono configurate scegliendo la loro voce dal menu **interfacce**. Per esempio, per configurare l'interfaccia WAN, scegliere **Interfacce> WAN**. Quasi tutte le opzioni trovate in **Interfacce> WAN** sono identiche a quelle menzionate nella parte WAN della procedura guidata di configurazione.

Ogni interfaccia è configurata nello stesso modo e qualsiasi interfaccia può essere configurata come qualsiasi tipo di interfaccia (Statica, DHCP, PPPoE, ecc). Inoltre, il blocco delle reti private e delle reti bogon può essere eseguito su qualsiasi interfaccia. Ogni interfaccia può essere rinominata, comprese WAN e LAN, con un nome personalizzato. Inoltre, ogni interfaccia può essere abilitata e disattivata a piacimento, a condizione che almeno un'interfaccia rimanga abilitata.

Vedi anche:

Per informazioni dettagliate sulla configurazione dell'interfaccia, vedere *Tipi e configurazione di interfaccia.*

La configurazione IPv4 può essere modificata tra *statico, DHCP, PPPoE, PPP, PPTP, L2TP,* o *niente* per lasciare l'interfaccia senza un indirizzo IPv4. Quando si utilizza *IPv4 statico*, è possibile impostare un indirizzo IPv4, una subnet mask e il gateway IPv4. Se si sceglie una delle altre opzioni, i campi specifici del tipo appaiono per essere configurati.

La configurazione IPv6 può essere impostata su *statico*, *DHCP6, SLAAC, Tunnel 6rd, Tunnel 6to4, Track interface,* o *niente* per lasciare l'interfaccia senza un indirizzo l'IPv6. Quando si seleziona *statico*, è possibile mpostare l'indirizzo IPv6, la lunghezza del prefisso e il gateway IPv6.

Se questa è un'interfaccia wireless, la pagina conterrà molte opzioni aggiuntive per configurare l'interfaccia. Consultare *Wireless* per i dettagli.

Nota: Selezionando un **Gateway** dall'elenco a discesa, o aggiungendo un nuovo gateway e selezionandolo, Firew4LL tratterà quella interfaccia come un'interfaccia di tipo WAN per il NAT e le funzioni correlate. Questo non è auspicabile per interfacce interne come LAN o DMZ. I gateway possono ancora essere utilizzati su tali interfacce per percorsi statici e altri scopi *senza* selezionare un gateway qui sulla pagina delle interfacce.

7.3 Gestione delle liste nella GUI

La WebGUI di Firew4LL ha un gruppo comune di icone che sono usate per la gestione di liste e collezioni di oggetti del firewall. Non tutte le icone sono usate in ogni pagina, ma i loro significati sono coerenti al contesto in cui sono viste. Esempi di tali lista includono regole del firewall, regole del NAT, IPsec, OpenVPN e certificati.

 Aggiungere un nuovo elemento ad un elenco

 Aggiungere elemento all'inizio di una lista

 Aggiungere un elemento alla fine di un elenco

 Modificare un elemento esistente

 Copiare un elemento (Crea un nuovo elemento della base all'elemento selezionato)

 Disabilitare un elemento attivo

 Abilitare un elemento disabilitato

 Eliminare un elemento

 Usato per spostare voci dopo aver selezionato uno o più elementi. Fare clic per spostare gli elementi selezionati sopra questa riga. Fare clic su Shift per spostare gli elementi selezionati sotto questa riga.

Le sezioni possono avere le proprie icone specifiche per ogni zona. Consultare le sezioni appropriate di questo libro per le specifiche sulle icone trovate in altre parti del firewall. Per esempio, per trovare il significato delle icone usate solo nella gestione dei certificati, guardare in *Gestione dei certificati*

Suggerimento: Per determinare quale azione un'icona eseguirà, passare il mouse sopra l'icona con il puntatore e un suggerimento mostrerà una breve descrizione dello scopo dell'icona.

7.4 Navigare velocemente nella GUI con le scorciatoie

Molte aree della GUI hanno icone di scelta rapida presenti nella zona conosciuta come la «barra di Breadcrumb», come visto in Figura *Esempio di scorciatoie*. Queste icone di scelta rapida riducono la ricerca necessaria per individuare le pagine correlate, consentendo ad un amministratore di firewall di navigare rapidamente tra la pagina di stato di un servizio, i registri e la configurazione. Le scorciatoie per un determinato argomento sono presenti in ogni pagina relativa un argomento racconto.

Per esempio, in Figura *Esempio di scorciatoie*, le scorciatoie hanno i seguenti effetti:

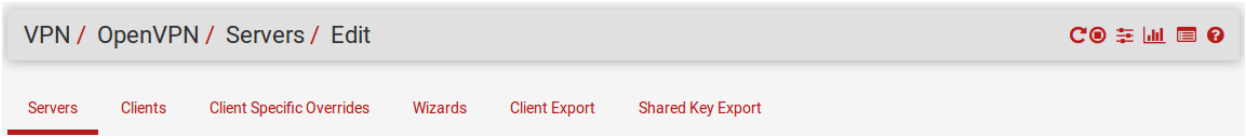


Fig. 14: Esempio di scorciatoie


Avviare il servizio Se il servizio di posta è interrotto, questa icona avvia il servizio.


Riavviare il servizio Se il servizio di posta è in esecuzione, questa icona riavvia il servizio.


Fermare il servizio Se il servizio di posta è in esecuzione, questa icona ferma il servizio.


Impostazioni correlate Quando questa icona appare, si passa alla pagina delle impostazioni di questa sezione.


Collegamento della pagina di stato Un collegamento alla pagina di stato di questa sezione, se esiste.


Collegamento alla pagina di log Se questa sezione ha una pagina di registro correlata, questa icona ne indica il collegamento.


Collegamento all'aiuto Carica un aiuto coerente a questa pagina

La pagina *Stato del servizio* (**Stato> Servizi**) ha anche controlli di scelta rapida per le pagine relative a ciascun servizio, come mostrato nella figura *Scorciatoie sullo stato del servizio*. Le icone hanno lo stesso significato della sezione precedente.

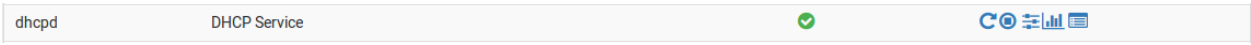


Fig. 15: Scorciatoie sullo stato del servizio

7.5 Opzioni Configurazione Generale

Sistema> Configurazione generale contiene opzioni che impostano elementi di configurazione di base per Firew4LL e la GUI. Alcune di queste opzioni si trovano anche nella *Procedura guidata di configurazione*.

Nome dell'host è Il nome abbreviato per questo firewall, come firewall1, hq-fw, o sito1. Il nome deve iniziare con una lettera e può contenere solo lettere, numeri o un trattino.

Dominio INSERIRE il nome di dominio per questo firewall, ad es. esempio.com. Se questa rete non ha un dominio, usare <qualcosa>.dominiolocale, dove <qualcosa> è un altro identificatore: un nome aziendale, cognome, nickname, ecc. Per esempio, azienda.dominiolocale

Il **nome dell'host** e il nome di dominio sono combinati per comporre il nome di dominio completamente qualificato (FQDN) di questo firewall. Per esempio, se il **hostname** è fw1 e il dominio è esempio.com, allora l'FQDN è fw1.esempio.com.

7.5.1 Impostazioni del server DNS

Le opzioni in questa sezione controllano come il firewall risolva i nomi host usando il DNS.

Indirizzo dei server DNS 1-4 Gli indirizzi IP dei server DNS possono essere compilati, se necessario e se sono noti.

Questi server DNS possono essere lasciati vuoti se il risolutore DNS rimarrà attivo utilizzando le impostazioni predefinite. La configurazione predefinita di Firew4LL ha il risolutore DNS attivo in modalità risolutore (non in modalità d'inoltro). Quando impostato in questo modo il risolutore DNS non ha bisogno di inoltrare i server DNS quindi comunicherà direttamente con i server della root del DNS e altri server autorevoli DNS. Per forzare il firewall ad usare questi server DNS configurati, abilitare la modalità di inoltro nel risolutore del DNS o utilizzare l'inoltro del DNS.

Per ulteriori informazioni sulla configurazione del risolutore del DNS vedere *Risolutore del DNS*

Se questo firewall ha un tipo di WAN dinamico come DHCP, PPTP o PPPoE questi possono essere assegnati automaticamente dall'ISP e possono essere lasciati vuoti.

Gateway dei server DNS 1-4 Oltre ai loro indirizzi IP, questa pagina fornisce un modo per impostare il Gateway utilizzato per raggiungere ogni server DNS. Questo è particolarmente utile in uno scenario di Multi-WAN dove, idealmente, il firewall avrà almeno un server DNS configurato per WAN. Maggiori informazioni sul DNS per Multi-WAN si possono trovare in *Server DNS Server e route statiche*.

Sostituzione del server DNS Quando selezionata, un provider di servizi internet della WAN dinamica può fornire un server DNS che sostituiranno quelli impostati manualmente. Per forzare l'uso dei soli server DNS configurati manualmente, deselezionare questa opzione.

Disabilitare l'inoltro DNS Per impostazione predefinita, Firew4LL consulta il risolutore del DNS o l'inoltro del DNS in esecuzione sul firewall per risolvere i nomi host da solo. Lo fa elencando host locali (127.0.0.1) come suoi server DNS primari. L'attivazione di questa pzione disabilita questo comportamento, costringendo il firewall ad usare i server DNS configurati sopra invece dei suoi.

7.5.2 Localizzazione

Le opzioni in questa sezione controllano la lingua e il visualizzazione dell'orario del firewall.

Zona dell'orario Scegliere una zona con nome geografico che corrisponda meglio alla posizione di questo firewall, o una zona comune come UTC. L'orologio del firewall, le voci di log e le altre aree del firewall basano il loro orario su questa zona. Cambiare la zona può richiedere un riavvio per attivarsi completamente in tutte le aree del firewall.

Server dell'orario Nome dell'host o indirizzo IP del server NTP (Protocollo dell'orario della rete). A meno che non sia richiesto uno specifico server NTP, come uno sulla LAN, la migliore pratica è lasciare il valore dei server dell'orario al valore predefinito 0.lfirew4lll.pool.ntp.org. Questo valore sceglierà un server casuale da un pool di host NTP noti e buoni.

Per utilizzare Più di server di orario, aggiungerli Nella STESSA casella, separando OGNI Server da uno spazio. Per esempio, per usare tre server NTP dal pool, inserire:

Questa numerazione è specifica per far in modo che .pool.ntp.org operi e assicuri che ogni indirizzo sia estratto da un pool di server NTP unici in modo che lo stesso server non venga usato due volte.

Lingua La GUI di Firew4LL è stata tradotta in altre lingue oltre all'inglese predefinito. Le lingue alternativa sono il *Portoghese (Brasile)* e il *Turco*.

7.5.3 Configuratore web

Le opzioni in questa sezione controllano vari aspetti del comportamento della GUI.

Tema Cambiare il tema controlla l'aspetto e la percezione della GUI. Diversi temi sono inclusi nel sistema di base, e modificano solo aspetti estetici e non funzionali della WebGUI

Navigazione Superiore Questa opzione controlla il comportamento della barra del menu dei nella parte superiore di ogni pagina. Ci sono due scelte possibili:

Scorrere la pagina Il comportamento predefinito. Quando la pagina è scorrevole, la navigazione rimane nella parte superiore della pagina, così quando si scorre verso il basso non è più visibile perché esce fuori dalla visuale della finestra. Questa è l'opzione migliore per la maggior parte delle situazioni.

Fisso Quando selezionato, la navigazione rimane fissa nella parte superiore della finestra, sempre visibile e disponibile per l'uso. Questo comportamento può essere conveniente, ma su schermi più piccoli come tablet e dispositivi mobili, menù lunghi possono essere tagliati, rendendo irraggiungibili le opzioni in basso.

Nome dell'host nel menu Quando impostato, il **nome dell'host** del firewall o il **nome di dominio completamente qualificato** saranno inclusi nella barra dei menù per riferimento. Questo può aiutare quando si mantengono più firewall, rendendo più facile distinguerli senza guardare il titolo del browser o la scheda di testo.

Colonne della dashboard La dashboard è limitata a 2 colonne per impostazione predefinita. Su schermi più ampi, è possibile aggiungere più colonne per utilizzare meglio lo spazio dello schermo orizzontale. Il numero massimo di colonne è 4.

Mostrare/Nascondere i pannelli associati Alcuni settori della GUI di Firew4LL contengono pannelli pieghevoli con impostazioni. questi pannelli occupano spazio in più sullo schermo, quindi sono nascosti per impostazione predefinita. Per gli amministratori del firewall che usano frequentemente i pannelli, questo può diventare un fattore di lentezza e inefficienza, quindi le opzioni di questo gruppo permettono che i pannelli siano mostrati come impostazione predefinita invece che nascosti.

Widget disponibili Controlla il pannello dei widget disponibili sulla dashboard.

Filtro di registro Controlla il pannello di filtraggio del log ( ) utilizzato per la ricerca di voci di registro nella sezione **Stato> Registro di sistema**.

Registro di gestione Controlla le impostazioni del registro nel pannello **Registro di gestione** ( ) disponibile per ogni registro nella sezione **Stato>Registri di sistema**.

Controllo delle impostazioni Controlla il pannello delle opzioni utilizzato per modificare i grafici di **Stato> Monitoraggio**.

Etichette della colonna cinistra Quando è selezionata, le etichette delle opzioni nella colonna sinistra vengono impostate per commutare le opzioni quando si fa clic. Questo può essere conveniente se l'amministratore del firewall è abituato a questo comportamento, ma può anche essere problematico sul cellulare o in casi in cui il comportamento è inaspettato.

Periodo di aggiornamento della dashboard Controlla l'intervallo in cui i dati della dashboard vengono aggiornati. Di Molti dei widget si aggiornano dinamicamente usando AJAX. Con molti widget caricati,

un veloce intervallo di aggiornamento può causare un alto carico sul firewall, dipende dall'hardware in uso. Consentire più tempo tra gli aggiornamenti ridurrebbe il carico complessivo.

7.6 Opzioni Configurazione Avanzata

Sistema> Avanzate contiene numerose opzioni di natura avanzata. Alcune di queste opzioni richiedono la regolazione per il routing di base/distribuzioni NAT, queste opzioni possono aiutare a personalizzare la configurazione del firewall in modi vantaggiosi per ambienti più complessi.

Alcune di queste opzioni sono trattate più in dettaglio nelle altre sezioni del libro in cui la loro discussione è più coerente o rilevante, ma sono tutti menzionati qui con una breve descrizione.

7.6.1 Scheda accesso amministrazione

Le opzioni presenti nella scheda di **accesso all'amministrazione** regolano i vari metodi di gestione del firewall, anche tramite interfaccia web, SSH, console seriale e fisica.

Configuratore web (WebGUI)

Protocollo

Il protocollo WebGUI può essere impostato su **HTTP** o **HTTPS**. La migliore Pratica è Quella di utilizzare HTTPS in modo che il traffico da e per la WebGUI sia crittografato

Certificato SSL

Se si sceglie HTTPS, anche un certificato deve essere scelto dall'elenco a discesa del **certificato SSL**. Il certificato predefinito di posta è un certificato auto-firmato generatore automaticamente. Questa non è una situazione ideale, ma e meglio che non avere affatto crittografia.

Suggerimento: Per usare un certificato e una chiave SSL firmati esternamente, importarli utilizzando gestione dei certificati, quindi selezionare qui il certificato.

---

il principale inconveniente nell'utilizzare un certificato personalizzato auto-generato è la mancanza di garanzia dell'identità dell'host, dal momento che il certificato non è firmato da un'autorità di certificazione di fiducia del browser. Inoltre, perché per la maggior parte degli utenti di internet un certificato non valido dovrebbe essere considerato un rischio, i browser moderni reprimono la loro gestione. Firefox, per esempio, da una schermata di avvertimento e costringe l'utente a importare il certificato e consentire un'eccezione permanente. Internet Explorer mostrerà una schermata di avvertimento con un link per continuare, come Chrome. opera mostrerà una finestra di avviso.

Suggerimento: Per generare un nuovo certificato auto-firmato per la GUI, connettersi utilizzando la consola o ssh e da un prompt della shell, eseguire il following comando:: pfSsh.php playback generateguicert

---

Porta TCP

Spostare la WebGUI su una porta alternativa è da preferito da alcuni amministratori per sicurezza per motivi di oscurità, anche se tali pratiche non dovrebbero essere considerate non offrendo alcun beneficio per la sicurezza. Spostare la

GUI in un'altra porta libererà le porte web standard per l'uso con inoltro di porta o altri servizi come un HAproxy. Per impostazione predefinita la WebGUI utilizza HTTPS sulla porta 443 con un reindirizzamento dalla porta 80 per la migliore compatibilità e facilitá di configurazione iniziale. Per modificare la porta, inserire un nuovo numero di porta nel campo **Porta TCP**.

Numero Massimo di Processi

Se amministratori multipli visualizzano la GUI allo stesso tempo e le pagine impiegano troppo tempo per caricare, o non riescono a caricare, aumentare il numero massimo di processi. Per impostazione predefinita, il valore e impostato su 2, quindi il firewall esegue due processi per operatore del server web.

Reindirizzamento alla WebGUI

Per impostazione predefinita, per facilità di accesso e compatibilità, il firewall esegue un reindirizzamento sulla porta 80 in modo che se un browser tentasse di accedere al firewall con HTTP, il firewall accetterebbe la richiesta e quindi reindirizzerebbe il browser allo HTTPS sulla porta 443. Questo reindirizzamento può essere disabilitato selezionando disabilitare la **regola di reindirizzamento del configuratore web**. Disabilitare il reindirizzamento permette anche ad un altro daemon di collegarsi alla porta 80.

Completamento automatico dell'accesso alla WebGUI

Per comodità, il modulo di accesso consente il completamento automatico in modo che i browser possano salvare le credenziali di accesso. In ambienti ad alta sicurezza, come quelli che devono aderire a specifici requisiti di conformità di sicurezza, this comportamento non è accettabile. Può essere disabilitato selezionando **disabilitare il completamento automatico dell'accesso del configuratore web**. Questo controlla solo il completamento automatico del modulo di accesso.

Avvertimento: Pochi browser rispettano questa opzione. Molti di loro offrono comunque la possibilità di salvare le password anche quando il modulo specifica che non dovrebbe essere consentito. Questo comportamento deve essere controllato o modificato utilizzando le opzioni del browser.

Messaggi di accesso alla WebGUI

Gli accessi di successo comportano la stampa di un messaggio sulla console, e su alcuni hardware questi messaggi di consolarlo fanno sentire un «beep» dal dispositivo. Per fermare questo messaggio di log (e il segnale acustico risultante), controllare **disabilitare la registrazione degli accessi del configuratore web**.

Anti-Blocco

L'accesso alla porta WebGUI e alla porta SSH sull'interfaccia LAN è consentito per impostazione predefinita indipendentemente dalle regole definite di filtro dall'utente, una causa della regola anti-blocco. Quando due o più interfacce sono presenti, e la regola anti-blocco è attiva sull'interfaccia LAN; se è configurata solo un'interfaccia, la regola anti-blocco sarà attiva su quell'interfaccia.

Selezionare **disabilitare la regola anti-blocco del configuratore web** rimuove la regola di blocco automatico. Con questa regola disabilitata, è possibile controllare quali indirizzi IP LAN possono accedere alla WebGUI utilizzando le regole del firewall.

Nota: Il ripristino dell'indirizzo IP LAN dalla console di sistema ripristina anche la regola anti-blocco. Se l'accesso amministrativo è bloccato dopo l'abilitazione, scegliere l'opzione del menù della console 2, quindi scegliere di impostare l'indirizzo IP LAN, e inserire nello stesso esatto indirizzo IP e le informazioni di accompagnamento.

Controllo rebind del DNS

Il firewall blocca le risposte di un indirizzo IP privato da server DNS configurati per impostazione predefinita, per evitare attacchi rebinding al DNS. Marcare questa casella per disabilitare la protezione rebinding del dns se interferisce con l'accesso al configuratore web o la risoluzione del nome.

Vedi anche:

Maggiori dettagli sugli attacchi di rebinding del DNS possono essere trovati su Wikipedia.

Il caso più comune per disabilitare questo sarebbe quando il firewall di posta è impostato per utilizzare un server DNS interno che restituirà risposte private (RFC1918) per il nome dell'host. Quando si accede al firewall tramite indirizzo IP, questi controlli non vengono eseguiti perché l'attacco è rilevante solo quando si usa un hostname.

Suggerimento: Invece di disabilitare tutte le protezioni del rebinding del DNS, può essere selettivamente disabilitato per il dominio nel risolutore o l'inoltro del DNS. Vedere *Risolutore del DNS e protezione del rebinding del DNS* e *Inoltro del DNS e protezione del rebinding del DNS*.

Applicazione del HTTP_REFERER del browser

La GUI controlla l'URL di riferimento quando si accede per impedire un modulo su un altro sito dall'inviare una richiesta al firewall, cambiare un'opzione quando l'amministratore non intendeva che ciò accadesse. Anche questo rompe anche alcuni comportamenti convenienti e desiderabili, come avere una pagina che collega un vari dispositivi firewall. Per disattivare questo comportamento, selezionare **disabilitare il controllo dell'applicazione HTTP_REFERER**.

Hostname alternativi

Per mantenere il controllo sul rebind del DNS e attiva l'applicazione del HTTP_REFERER, ma controllare leggermente il loro comportamento, compilare nomi host alternativi nella casella. Per impostazione predefinita il sistema consentirà l'accesso al nome dell'host configurato sul firewall e a tutti gli indirizzi IP configurati sul firewall. L'aggiunta di un hostname nel campo permetterà di utilizzare questi nomi dellìhost per l'accesso alla GUI e per l'URL di riferimento.

Attacco MITM (Man-in-the-Middle)/Attenzione

Se un browser tenta di accedere alla GUI utilizzando un indirizzo IP non configurato sul firewall, come un inoltro della porta da un altro firewall, verrà stampato un messaggio che indica che l'accesso al firewall può essere compromesso a causa di un attacco man-in-the-middle (MITM).

Se un inoltro s Stato deliberatamente configurato sul firewall o su un firewall prima di questo, il messaggio può essere tranquillamente ignorato. Se l'accesso al firewall doveva essere diretto, allora fare molta attenzione prima di effettuare l'accesso per assicurarsi che le credenziali di accesso non vengano instradate attraverso un sistema non fidato. L'accesso non è disabilitato in questo caso, c'è solo un avvertimento, quindi non c'è alcuna opzione per disabilitare questo comportamento.

Testo nella scheda del browser

Per impostazione predefinita, la GUI del firewall stampa il nome dell'host del firewall prima del titolo della pagina/scheda, seguito dal nome della pagina. Per invertire questo comportamento e mostrare il nome della pagina prima e il nome dell'host dopo, controllare **Visualizzare il nome della pagina prima nella scheda del browser.**

Gli amministratori che accedono a molti firewall contemporaneamente in schede separate tendono a preferire il nome dell'host prima (impostazione predefinita). Gli amministratori che accedono a un firewall con molte pagine in schede separare tendono a preferire il nome della pagina prima.

SSH

Il server SSH può essere abilitato per consentire l'accesso da remoto alla console e la gestione dei file. Un utente può connettersi con qualsiasi client standard ssh, come il client ssh della linea di comando OpenSSH, PuTTY, SecureCRT o iTerm. Per accedere all'account admin, si può usare il nome utente amministratore o l'account root, ed entrambi accettano la password di amministratore della WebGUI per il login.

Gli utenti del gestore utente che hanno il privilegio Utente - Sistema – accesso dell'account hanno anche il permesso per accedere su ssh. Questi utenti non hanno privilegi di accesso alla root, e non stampano il menù quando fanno il login perché molte delle opzioni richiedono privilegi di root.

Suggerimento: Per concedere agli utenti ulteriori privilegi di shell, usa il pacchetto sudo.

I trasferimenti di file da e verso il firewall Firew4LL sono possibili anche utilizzando un client di copia sicura (SCP), come la riga di comando di OpenSSH scp, FileZilla, WinSCP o Fugu. Per usare SCP, connettersi come utente della root, non come admin. Se un utente personalizzato ha il permesso Utente - Sistema - Copia i file o tutti gli accessi, allora possono anche utilizzare SCP.

Suggerimento: I client SSH devono essere aggiornati. Col tempo, gli standard di sicurezza evolvono e le impostazioni del server SSH utilizzate da Firew4LL cambiano. I client obsoleti potrebbero non essere in grado di connettersi utilizzando le chiavi di sicurezza forti e gli algoritmi richiesti da sshd su Firew4LL. Se un client non si connette, controllare per un aggiornamento dal fornitore.

Abilitare SSH

Per abilitare il servizio SSH, selezionare **Abilitare la shell sicura**. Dopo aver salvato con questa opzione abilitata, il firewall genererà le chiavi SSH se non sono già presenti e poi avviare il servizio SSH.

Metodo di autenticazione

SSH può essere configurato per consentire solo accessi basati su chiavi e non sulla password. Gli accessi basati sulle chiavi sono una pratica molto più sicura, anche se ci vuole più preparazione per configurare.

Per forzare l'autenticazione Basata Sulle chiavi, selezionare **Disabilitare l'accesso con password per la shell sicura**.

Le chiavi per l'utente per accesso basato sulle chiavi vengono aggiunte modificando gli utenti in **Gestione Utente** (*Gestione Utente e Autenticazione*). Quando si modifica un utente, incollare le chiavi pubbliche consentite nel campo di testo chiavi autorizzate per il loro account.

Porta SSH

Spostare il server SSH su una porta alternativa fornisce un miglioramento trascurabile della sicurezza, e libera la porta per altri usi. Per cambiare la porta, digitare la porta nuova nella casella **Porta SSH**.

Suggerimento: Gli scanner SSH con brute-force si concentrano sul colpire la porta TCP 22 ma se il daemon è aperto a Internet su un'altra porta, verrà trovato e colpito dagli scanner.

Le migliori pratiche per SSH

Se questo firewall è installato in un ambiente che richiede di lasciare l'accesso SSH senza restrizioni da regole firewall, il che è pericoloso, è fortemente raccomandato di spostare il servizio SSH su una porta alternativa casuale e forzare l'autenticazione con la chiave. Spostandosi su una porta alternativa si eviterà il fastidio di un registro da molti, ma non tutti, tentativi di login SSH con forza bruta e scansioni casuali. Questo può essere ancora trovato con una scansione della porta, quindi il passaggio all'autenticazione basata su chiave deve sempre essere fatto su ogni server SSH accessibile al pubblico per eliminare la possibilità di attacchi di forza bruta.

Più accessi non riusciti dallo stesso indirizzo IP comporteranno il blocco dell'indirizzo IP che cerca di autenticarsi.

Comunicazione seriale

Se Firew4LL è in esecuzione su hardware senza un monitor o se verrà eseguito «headless» (senza tastiera e video collegati), la console seriale può essere abilitata per mantenere il controllo fisico, purché l'hardware abbia una porta seriale (non USB).

Se viene rilevato l'hardware che non ha una porta VGA, la console seriale è forzata e non può essere disabilitata, e le opzioni seriali sono tutte nascoste tranne la velocità.

Terminale seriale

Quando il terminale seriale è impostato, la console è abilitata sulla prima porta seriale. Questa console riceverà i messaggi di avvio del kernel e un menu dopo che il firewall avrà terminato l'avvio. Questo non disabiliterà la tastiera onboard e la console video.

Per connettersi alla console seriale, utilizzare un cavo null modem collegato at a porta seriale o ad un adattatore su un altro PC o dispositivo seriale.

Vedi anche:

Per ulteriori informazioni sul collegamento a una console seriale, vedere *Collegamento a una console seriale* e *Avviare un client seriale*. Quando si apportano modifiche alla console seriale, il firewall deve essere riavviato prima che abbia effetto.

Velocità della console seriale

La velocità della console seriale per impostazione predefinita è di 115200bps e quasi tutto l'hardware funziona bene con quella velocità. In casi rari, può essere richiesta una velocità più lenta, che può essere impostata qui selezionando la velocità desiderata dall'elenco a discesa della **Velocità seriale**.

Durante l'aggiornamento da una versione precedente, questo può rimanere ad un valore più vecchio come 9600 o 38400 per abbinare il BIOS su un hardware più vecchio. Aumentare la Velocità di 115200 è quasi sempre sicuro e più utile rispetto a velocità più lente.

Console primaria

Sull'hardware con la console seriale abilitata e una porta VGA disponibile, il selettore della **console primaria** sceglie quale è la console preferita, quindi riceverà i messaggi del log di avvio da Firew4LL. Altri messaggi del kernel del sistema operativo appariranno su tutte le connessioni della console, ed entrambe le console avranno un menù utilizzabile.

Nei casi in cui l'avvio non possa essere completato, la console preferita deve essere utilizzata per risolvere il problema, come riassegnare le interfacce.

Menu console

Normalmente il menù della console è sempre mostrato sulla console di sistema, e il menù sarà disponibile fino a quando qualcuno ha accesso fisico alla console. In ambienti ad alta sicurezza questo non è auspicabile. Questa opzione permette alla console di essere protetta da password. Lo stesso nome utente e la password possono essere utilizzati qui per la WebGUI. DOPO Aver impostato questa opzione, il firewall deve essere riavviato prima che abbia effetto.

Nota: Mentre questo fermerà l'accidentale pressione di tasti e terrà fuori gli utenti occasionali, questo non è affatto un metodo di sicurezza perfetto. Una persona informata con accesso fisico può ancora ripristinare le password (vedere *Password dimenticata con una console bloccata*). Considerare altri metodi fisici di sicurezza se la sicurezza della console è un requisito.

7.6.2 Scheda Firewall/NAT

Opzioni avanzate del firewall

Compatibilità con IP non frammentati

Questa opzione è una soluzione per i sistemi operativi che generano pacchetti frammentati con il set di bit da non frammentare (DF). Linux NFS (Sistema di File della rete) è noto per questo, cosi come alcuni sistemi VoIP.

Quando questa opzione è abilitata, il firewall non lascerà cadere questi pacchetti, ma eliminerà il bit da non frammentare. Il firewall randomizzerà anche il campo di identificazione IP dei pacchetti in uscita per compensare i sistemi operativi che impostano il bit DF ma impostano un campo di intestazione di identificazione IP zero.

Generazione ID casuale dell'IP

Se il **Filtro per inserire un ID più forte nell'intestazione IP dei pacchetti che passano** è selezionato, il firewall sostituisce il campo di identificazione IP dei pacchetti con valori casuali per compensare i sistemi operativi che utilizzano valori prevedibili. Questa opzione si applica ai soli pacchetti che non sono frammentati dopo il riassemblaggio opzionale del pacchetto.

Opzioni di ottimizzazione del firewall

La modalità di ottimizzazione controlla come il firewall termini le voci della tabella di stato:

Normale L'algoritmo di ottimizzazione di serie, che è ottimale per la maggior parte degli ambienti

Alta latenza Usato per collegamenti ad alta latenza, come i collegamenti satellitari. Termina le connessioni inattive più tardi delle opzioni predefinite.

Aggressivo Termina connessioni inattive più velocemente. Si ottiene un uso più efficiente della CPU e della memoria, ma può far cadere connessioni legittime prima del previsto. Questa opzione può anche migliorare le prestazioni in distribuzioni ad alto traffico con un sacco di connessioni, come VoIP.

Conservativo Cerca di evitare di interrompere tutte le connessioni legittime a scapito di un maggiore utilizzo della memoria e della CPU. Può aiutare in ambienti che richiedono una lunga vita, ma per lo più è inattivo con connessioni UDP, come VoIP.

Disabilitare il firewall

Quando il filtro Disabilitare tutti i pacchetti è impostato, il firewall Firew4LL viene trasformato in una piattaforma che funziona solo come routing. Ciò avviene disabilitando completamente pf, e di conseguenza, NAT è disabilitato in quanto è anche gestito da pf.

Suggerimento: Per disabilitare solo il NAT, non utilizzare questa opzione. Consultare *Disabilitare il NAT in uscita* per ulteriori informazioni sul controllo del comportamento NAT in uscita.

Disabilitare la normalizzazione nel firewall

Quando impostata, l'opzione di pulizia in pf è disabilitata. L'azione di pulizia in pf può interferire con NFS, e in rari casi, anche con il traffico VoIP. Per impostazione predefinita, Firew4LL usa l'opzione riassemblaggio dei frammenti che riassembla i pacchetti frammentati prima di mandarli a destinazione, quando è possibile. Si possono trovare maggiori Informazioni sulla funzione di pulizia di pf nella sezione *Documentazione della pulizia di pf in OpenBSD*.

Nota: Disabilitare la pulizia disabilita anche altre caratteristiche che si basano sulla pulizia per funzionare, come il clearing dei bit del DF e la randomizzazione ID. Disabilitare la pulizia non disabilita il clamping MSS se è attivo per VPN, o quando un valore MSS è configurato su un'interfaccia.

Timeout adattivo del Firewall

I **timeout adattivi** controllano la gestione dello stato in pf quando la tabella di stato è quasi completa. Utilizzando questi timeout, un amministratore del firewall può controllare come gli stati sono scaduti o eliminati quando c'è poco o nessuno spazio rimanente per l'archivio dei nuovi stati di connessione.

I **timeout adattivi** sono abilitati per impostazione predefinita e i valori di impostazione predefinita vengono calcolati automaticamente sulla base del valore configurato di **Stati massimi del firewall.**

Inizio adattivo La scala adattiva viene avviata una volta che la tabella di stato raggiunge questo livello, espresso come un certo numero di stati. Il valore predefinito dell'inizio adattivo è pari al 60% degli stati massimi del firewall.

Fine adattiva Quando le dimensioni della tabella di stato raggiungono questo valore, espresso come un numero di voci della tabella di stato, tutti i valori di timeout sono considerati pari a zero, il che fa sì che pf elimini immediatamente tutte le voci di stato. uesta Questa impostazione definisce il fattore di scala, dovrebbe essere maggiore del numero totale di stati consentiti. Il valore predefinito della fine adattiva è pari al 120% degli stati massimi del firewall.

Quando il numero di stati di connessione supera la soglia impostata dall'inizio adattivo, i valori di timeout vengono scalati linearmente con il fattore nella base di al numero di stati utilizzati tra i conteggi di stato inizio e fine. Il fattore di aggiustamento del timeout è calcolato come segue: (Numero di stati fino al raggiungimento del valore finale adattivo)/(Differenza tra i talori di fine adattivo e di inizio adattivo).

Nota: Per esempio, si consideri un firewall con **inizio adattivo** impostato su 600000, **fine adattiva** impostata su 1200000 e **stati massimi del firewall** impostati su 1000000. In questa situazione, quando la dimensione della tabella di stato raggiunge 900.000 voci il timeout di stato sarà scalato al 50% del suo valore normale. (1.200.000 - 900.000)/(1.200.000 - 600.000) = 300.000/600.000 = 0.50, 50%. Continuando l'esempio, quando la tabella di stato è piena a 1.000.000 di stati i valori di timeout saranno ridotti a un terzo dei loro valori originali.

Stati massimi del firewall

Questo valore è il numero massimo di connessioni che il firewall può contenere nella sua tabella di stato. La dimensione predefinita è calcolata in base al 10% della RAM totale. Questo vuesto vQuestoalore predefinito è sufficiente per la maggior parte delle installazioni, ma può essere regolato più o meno a seconda del carico e della memoria disponibile.

Ogni stato consuma circa 1 KB di RAM, o circa 1 MB di RAM per ogni 1000 stati. Il firewall deve avere RAM libera adeguata per contenere l'intera tabella di stato prima di aumentare questo valore. Gli stati del firewall sono discussi ulteriormente nella *Filtrazione stateful*.

Suggerimento: Su un firewall con 8GB di RAM la tabella di stato avrebbe una dimensione predefinita di circa 800.000 stati. Un valore personalizzato di stati massimi del firewall di 4.000.000 consumerebbe circa 4 GB di RAM, la metà del totale disponibile di 8GB.

Voci di tabella massime del firewall

Questo valore definisce il numero massimo di voci che possono esistere all'interno delle tabelle degli indirizzi utilizzate dal firewall per le raccolte di indirizzi come alias, ssh/voci del blocco della GUI, gli host bloccati da avvisi di snort, e così via. Per impostazione predefinita si tratta di 200.000 voci. Se il firewall ha funzionalità abilitate che possono caricare grandi blocchi di spazio per gli indirizzi alias come alias nella tabella URL o il pacchetto pfBlocker, allora aumentare questo valore per includere comodamente almeno il doppio della quantita totale di voci contenute in tutti gli alias combinati.

Entrate Massime di Frammenti del Firewall

Quando la normalizzazione è abilitata il firewall mantiene una tabella di frammenti di pacchetti in attesa di essere riassemblati. Per impostazione predefinita questa tabella può contenere 5000 frammenti. In rari casi una rete può avere un tasso insolitamente alto di pacchetti frammentati che possono richiedere più spazio in questa tabella.

quando questo limite è raggiunto, il messaggio di log seguente apparirà nel registro di sistema: `kernel: [zone: pf frag entries] PF frag entries limit reached`

Filtro rotta statica

L'opzione delle **Regole di bypass del firewall per il traffico sulla stessa interfaccia** si applica se il firewall ha una o più route statiche definite. Se questa opzione è abilitata, il traffico che entra e esce attraverso la stessa interfaccia non sarà controllato dal firewall. Ciò può essere richiesto in situazioni in cui più sottoreti sono collegate alla stessa

interfaccia, per evitare di bloccare il traffico che passa attraverso il firewall in una sola direzione solo a causa di un routing asimmetrico. Vedere *Tutte le regole di esclusione del firewall per il traffico sulla stessa interfaccia* per una discussione più approfondita su racconto argomento.

Disabilitare le regole VPN aggiunte automaticamente

Per impostazione predefinita, quando IPsec è abilitato le regole del firewall vengono automaticamente aggiunte all'interfaccia appropriata che permettera di stabilire il tunnel. Quando l'opzione **Disabilitare le regole VPN aggiunte automaticamente** è selezionata, il firewall non aggiungerà automaticamente queste regole. Disabilitando queste regole automatiche, l'amministratore del firewall ha il controllo su quali indirizzi possono connettersi a una VPN. Ulteriori informazioni su queste regole possono essere trovate su *Tutte le regole del firewall e VPN*.

Disabilitare la risposta a (reply-to)

In una configurazione Multi-WAN il firewall ha benefici con il comportamento predefinito che assicura che il traffico lasci la stessa interfaccia attraverso cui è arrivato. Questo si ottiene utilizzando la parola chiave pf reply-to che viene aggiunta automaticamente alle regole del firewall della scheda dell'interfaccia per tipo di interfacce WAN. Quando una connessione corrisponde a una regola con reply-to, il firewall ricorda il percorso attraverso cui la connessione è stata stabilita e instrada il traffico di risposta al gateway per quell'interfaccia.

Suggerimento: Le interfacce di tipo WAN sono interfacce che hanno un gateway impostato sulla configurazione del menu di **interfacce**, o interfacce che hanno un gateway dinamico come DHCP, PPPoE, o con interfacce OpenVPN, GIF o GRE assegnate.

In situazioni come il bridging questo comportamento è indesiderabile se l'indirizzo IP del gateway di WAN è diverso dall'indirizzo IP del gateway degli host dietro l'interfaccia con il ponte. La disattivazione di reply-to permetterà ai client di comunicare con il gateway corretto.

Un altro caso che ha problemi con reply-to comporta l'instradamento statico as altri sistemi in una più grande sottorete WAN. Disabiltare reply-to contribuirebbe a garantire che le risposte ritornino al router corretto invece di essere reindirizzate al gateway.

Questo comportamento può essere anche disabilitato sulle regole individuali del firewall piuttosto che globalmente usando questa opzione.

Intervallo risoluzione alias hostname

Questa opzione controlla la frequenza con cui gli alias degli hostname vengono risolti e aggiornati dal daemon filterdns. Per impostazione predefinita è 300 secondi (5 minuti). Nelle configurazioni con un piccolo numero di nomi di host o un server DNS veloce/con basso carico, diminuire questo valore per accettare le modifiche più velocemente.

Controllare il certificato dell'URL dell'alias

Quando l'opzione **Verificare i certificati HTTPS con il download di URL alias** è impostato, il firewall richiederà un certificato HTTPS valido per i server web utilizzati in alias della tabella URL. Questo comportamento è più sicuro, ma se il server Web è privato e utilizza un certificato auto-firmato, può essere più conveniente ignorare la validità del certificato e consentire di scaricare i dati.

Reti bogon

L'elenco a discesa della **Frequenza di aggiornamento** per le **Reti Bogon** controlla con quale frequenza vengono aggiornate queste liste. Ulteriori informazioni sulle reti bogon può essere trovata in *Reti di bogon bloccate*.

NAT

Refection NAT per il Port Forward

L'opzione **Modalità di Refection NAT per il Port Forward** controlla come la reflection del NAT venga gestita dal firewall. Queste regole di reindirizzamento del NAT consentono ai client di accedere alle porte d'inoltro utilizzando gli indirizzi IP pubblici sul firewall dalle reti locali interne.

Vedi anche:

Fare riferimento a *Reflection NAT* per una discussione sul merito della reflection NAT rispetto ad altre tecniche come Split DNS.

Ci sono tre possibili modalità per il reflection NAT:

Disabilitato Valore predefinito. Quando è disabilitata, le porte d'inoltro sono accessibili dalla WAN e non solo da reti locali interne.

NAT Puro Questa modalità utilizza un insieme di regole NAT per dirigere i pacchetti alla destinazione della porta d'inoltro. Ha migliore scalabilità, ma deve essere possibile determinare con precisione l'interfaccia e l'indirizzo IP del gateway utilizzato per la comunicazione con l'oggetto al momento in cui le regole vengono caricate. Non ci sono limiti inerenti al numero di porte d'inoltro diversi dai limiti dei protocolli. Sono supportati tutti i protocolli disponibili per le porte d'inoltro.

Quando questa opzione è abilitata, **NAT automatico in uscita per la reflection** deve essere attivata anche se i client e i server sono nella stessa rete locale.

NAT + Proxy La modalità *NAT + proxy* utilizza un programma di aiuto per inviare i pacchetti alla destinazione della porta d'inoltro. La connessione viene ricevuta dal deemon per reflection e agisce come un proxy, creando una nuova connessione al server locale. Questo comportamento mette un onere più grande sul firewall, ma è utile in situazioni in cui l'interfaccia e/o l'indirizzo IP del gateway utilizzati per la comunicazione con l'oggetto non possono essere determinati con precisione al momento in cui le regole vengono caricate. Le regole di reflection *NAT + proxy* non sono create per intervalli più grandi di 500 porte e non saranno utilizzate per più di 1000 porte in totale tra tutte le porte forward. Solo le porte d'inoltro TCP sono supportate.

Singole regole NAT hanno la possibilità di sostituire la configurazione della reflection NAT globale, quindi possono avere reflection NAT forzata o disattivata caso per caso.

Reflection Timeout

L'impostazione del ** reflection timeout** forza un timeout sulle connessioni fatte durante l'esecuzione della reflection NAT per le porte d'inoltro in modalità *NAT + proxy*. Se le connessioni sono aperte e consumano risorse, questa opzione può mitigare tale questione.

Reflection NAT per NAT 1: 1

Se selezionata, questa opzione aggiunge regole di reflection aggiuntive che consentono l'accesso a mappature 1:1 di indirizzi IP esterni da reti interne. Questo dà la stessa funzionalità che già esiste per la porta d'inoltro, ma per NAT 1: 1. Ci sono scenari di routing complessi che possono rendere questa opzione inefficace.

Questa opzione ha effetto solo sul percorso *in entrata* per NAT 1: 1 NAT, non in uscita. Lo stile della regola di base è simile alla modalità *NAT puro* per le porte d'inoltro. Come con la porta forward, ci sono opzioni per le voci per ignorare questo comportamento.

Reflection per il NAT automatico in uscita

Se selezionata, questa opzione consente di creare automaticamente in uscita regole di NAT che assistono regole di reflection che dirigono il traffico verso la stessa sottorete da cui ha avuto origine. Queste regole aggiuntive permettono al NAT puro e alla reflection del NAT 1:1 di funzionare pienamente quando i client e i server sono nella stessa sottorete. Nella maggior parte dei casi, questa casella deve essere selezionata per far operare la reflection del NAT.

Nota: Questo comportamento è necessario perché quando i client e server si trovano nella stessa sottorete, la fonte di traffico deve essere modificata in modo che la connessione sembri provenire dal firewall. In caso contrario, il traffico di ritorno potrà bypassare il firewall e la connessione non avrà successo.

TFTP Proxy

Il proxy incorporato del TFTP sarà un proxy di connessione ai server TFTP all'esterno del firewall, in modo che le connessioni client possano essere fatte per i server TFTP da remoto. Premere Ctrl-clic o Shift-clic per selezionare più voci dalla lista. Se non vengono scelte interfacce, il servizio proxy del TFTP è disattivato.

Timeout di stato

La sezione **Timeout di stato** permette la messa a punto dei timeout di stato per diversi protocolli. Questi sono in genere gestiti automaticamente dal firewall e i valori sono dettate dalle *Opzioni di ottimizzazione del firewall*. In rari casi, questi timeout possono avere bisogno di essere regolati verso l'alto o verso il basso per tenere conto di irregolarità nel comportamento del dispositivo o di esigenze specifiche dei siti.

Tutti i valori sono espressi in *secondi* e controllono per quanto tempo un collegamento in quello stato verrà trattenuto nella tabella di stato.

Vedi anche:

Le descrizioni delle seguenti opzioni si riferiscono a condizioni di stato del firewall come descritto in *Sti di interpretazione*.

Prima TCP Il primo pacchetto di una connessione TCP. **Apertura TCP** Lo stato prima che l'host di destinazione abbia risposto (ad es: SYN_SENT: CHIUSO). **Stabilita TCP** La connessione TCP stabilita in cui l'handshake a tre vie è stata completata. **Chiusura TCP** Un lato ha inviato un pacchetto TCP FIN. **Attesa del FIN TCP** Entrambe le parti si sono scambiate pacchetti FIN e la connessione verrà arrestata. Alcuni server possono continuare a inviare pacchetti durante questo tempo. **Chiusura TCP** Un lato ha inviato un pacchetto di ripristino della connessione (TCP RST). **Prima UDP** Il primo pacchetto UDP di una connessione è stato ricevuto. **UDP singolo** L'host di origine ha inviato un singolo pacchetto ma la destinazione non ha risposto (es: SINGLE: NO_TRAFFIC). **UDP multipla** Entrambe le parti hanno inviato pacchetti. **Prima ICMP** Un pacchetto ICMP è stato ricevuto. **Errore ICMP** Un errore ICMP è stato ricevuto in risposta a un pacchetto ICMP. **Prima altro, Singolo altro, Multiplo altro** Come per UDP, ma per altri protocolli.

7.6.3 Scheda per le reti

Opzioni IPv6 Consentire IPv6

Quando l'opzione `Consentire IPv6` non è selezionata, tutto il traffico IPv6 sarà bloccato.

Questa opzione è selezionata per impostazione predefinita in nuove configurazioni in modo che il firewall sia in grado di trasmettere e ricevere il traffico IPv6 se le regole lo permettono. Questa opzione controlla un insieme di regole di blocco che impediscono al traffico IPv6 di essere gestito dal firewall per consentire la compatibilità con le configurazioni importate da o aggiornate da versioni di Firew4LL precedenti alla 2.1.

Nota: Questa opzione non disabilita le funzioni di IPv6 o evita che venga configurato, controlla solo il flusso del traffico.

Tunneling IPv4 su IPv6

L'opzione **Abilitare l'incapsulamento del Nat con IPv4 di pacchetti IPv6** consente al protocollo IP 41/RFC 2893 di inoltrare a un indirizzo IPv4 specificato nel campo **indirizzo IP**.

Una volta configurata, questa inoltra tutto il traffico in entrata con protocollo 41/IPv6 a un host dietro questo firewall, invece di gestirlo localmente.

Suggerimento: L'attivazione di questa opzione non aggiunge regole firewall per consentire il traffico del protocollo 41. Una regola deve esistere sull'interfaccia WAN per consentire al traffico di passare attraverso la ricezione locale di host.

Preferire IPv4 su IPv6

Quando è impostata, questa opzione farà sì che il firewall stesso preferisca l'invio di traffico per host IPv4 invece di host IPv6 quando una query DNS restituisce i risultati a entrambi.

In rari casi in cui il firewall ha parzialmente configurato, ma non completamente indirizzato, l'IPv6, questo può consentire al firewall di continuare a raggiungere gli host di internet su IPv4.

Nota: Questa opzione controlla il comportamento del firewall stesso, come ad esempio il polling per gli aggiornamenti, le installazioni dei pacchetti, le regole dei download, e il recupero di altri dati. Non può influenzare il comportamento dei clienti dietro il firewall.

Interfacce di rete

Polling del dispositivo

Il polling dei dispositivi è una tecnica che consente al sistema di esaminare periodicamente i dispositivi di rete per i nuovi dati invece di fare affidamento sulle interruzioni. Questo impedisce che il firewall WebGUI, SSH, ecc. sia inaccessibile a causa di interruzioni quando è sotto carico estremo, al costo di una maggiore latenza. La necessità di polling è stata quasi eliminata grazie ai progressi del sistema operativo e a metodi più efficienti di gestione degli interrupt come MSI/MSIX.

Nota: Con il polling abilitato, il sistema sembrerà utilizzare il 100% della CPU. Questo è normale, perchè il thread di polling sta usando CPU per cercare i pacchetti. Il thread di polling viene eseguito con una priorità più bassa in modo che se gli altri programmi hanno bisogno ditempo sulla CPU, sospenderà l'attività per il tempo necessario. Lo svantaggio è che questa opzione rende il grafico della CPU meno utile.

Hardware Checksum Offloading

Se selezionata, questa opzione disabilita lo scaricamento del checksum dell'hardware sulle schede di rete. Lo scaricamento del checksum è generalmente vantaggioso in quanto consente al checksum di essere calcolato (in uscita) o verificato (in entrata) nell'hardware ad un tasso molto più veloce di quanto potrebbe essere gestito via software.

Nota: Quando lo scaricamento del checksum è attivato, la cattura di un pacchetto vedrà vuoti (tutti zero) o checksum di pacchetti segnalati come errati. Questi sono normali quando la manipolazione del checksum avviene nell'hardware.

Lo scaricamento del checksum viene interrotto in alcuni hardware, in particolare le schede Realtek e le schede virtualizzate/emulate come quelle su Xen/KVM. I sintomi tipici di scaricamento del checksum interrotto includono pacchetti corrotti e scarse prestazioni di throughput.

Suggerimento: In casi di virtualizzazione come Xen/KVM può essere necessario disattivare lo scaricamento del checksum sull'host, nonché sulla VM. Se le prestazioni sono ancora scarse o si hanno errori su questi tipi di macchine virtuali, cambiare il tipo di scheda di rete, se possibile.

Hardware TCP Segmentation Offloading

Selezionando questa opzione verrà disabilitato lo scaricamento della segmentazione TCP dell'hardware (TSO, TSO4, TSO6). Il TSO fa sì che il NIC gestisca la suddivisione dei pacchetti in blocchi di dimensioni MTU piuttosto che gestirli a livello si sistema operativo. Questo può essere più veloce per i server e gli apparecchi in quanto consente al sistema operativo di relegare il compito all'hardware dedicato, ma quando agisce come un firewall o un router questo comportamento è altamente indesiderabile in quanto in realtà aumenta il carico perché questo compito è già stato eseguito in altre parti della rete, rompendo così il principio end-to-end modificando i pacchetti che non sono stati originati su questa struttura.

Avvertimento: Questa opzione non è auspicabile per i router e i firewall, ma può giovare alle postazioni di lavoro e agli elettrodomestici. E" disabilitato per impostazione predefinita, e dovrebbe rimanere disabilitato a meno che il firewall non agisca principalmente o esclusivamente in un ruolo di appliance/endpoint.

Hardware Large Receive Offloading

Selezionare questa opzione disabiliterà lo scaricamento della grande ricezione dell'hardware (LRO). LRO è simile a TSO, ma per il percorso è in entrata anziché in uscita. Esso consente al NIC di ricevere un gran numero di pacchetti più piccoli prima di passarli al sistema operativo come un agglomerato più grande. Questo può essere più veloce per i server e gli apparecchi in quanto alleggerisce quello che normalmente sarebbe un compito di elaborazione pesante per la scheda di rete. Quando agisce come un firewall o router questo è altamente indesiderabile in quanto ritarda la ricezione e la trasmissione di pacchetti che non sono destinati a questa struttura, e dovranno essere divisi nuovamente sul percorso in uscita, aumentando il carico di lavoro in modo significativo e rompere la end-to-end.

Sopprimere i messaggi arp

Il firewall crea una voce nel registro di sistema principale quando un indirizzo IP sembra passare a un indirizzo MAC diverso. Questa voce di registro rileva che il dispositivo ha spostato gli indirizzi, e registra l'indirizzo IP e i vecchi e nuovi indirizzi MAC.

Questo evento può essere completamente benigno comportamento (ad es. teaming del NIC su un server Microsoft, un dispositivo che viene sostituito) o un legittimo problema client (ad es. conflitto di IP), e potrebbe apparire costantemente o raramente, se non mai. Tutto dipende dall'ambiente di rete.

Si consiglia di consentire la stampa di questi messaggi ARP per effettuare il log poiché c'è la possibilità che riporti un problema degno dell'attenzione di un amministratore di rete. Tuttavia, se l'ambiente di rete contiene sistemi che generano questi messaggi mentre funzionano normalmente, sopprimere gli errori può rendere il registro di sistema più utile in quanto non sarà ingombrato con messaggi di log non necessari.

7.6.4 Schede varie

Supporto proxy

Se questo firewall risiede in una rete che richiede un proxy per l'accesso a Internet in uscita, immettere le opzioni proxy in questa sezione in modo che le richieste da parte del firewall per elementi quali pacchetti e aggiornamenti saranno inviati attraverso il proxy.

URL del proxy

Questa opzione specifica la posizione del proxy per effettuare i collegamenti esterni. Deve essere un indirizzo IP o un nome di dominio completo.

Porta del proxy

La porta da utilizzare per la connessione al' URL del proxy. Per impostazione predefinita, la porta è 8080 per l'URL del proxy HTTP e 443 per gli URL dei proxy SSL. La porta è determinata dal proxy, e può essere un valore completamente diverso (ad esempio 3128). Verificare con l'amministratore proxy per trovare il valore della porta corretta.

Nome utente del proxy

Se necessario, questo è il nome utente che viene inviato per l'autenticazione proxy.

Password del proxy

Se necessario, questa è la password associata al nome utente impostato nell'opzione precedente.

BIlanciamento del carico

Sticky connections

Quando Firew4LL è diretto ad eseguire il bilanciamento del carico, le connessioni successive saranno reindirizzate in modo round-robin verso un server web o gateway, bilanciando il carico su tutti i server o percorsi disponibili. Quando Sticky Connections è attivo questo comportamento viene modificato in modo che le connessioni dalla stessa sorgente

vengano inviate allo stesso server web o attraverso lo stesso gateway, piuttosto che essere inviate in modo puramente round-robin.

Sticky Connections influisce sia sul bilanciamento del carico in uscita (Multi-WAN) che sul carico del server quando è attivato. Questa associazione «appiccicosa» esisterà finché gli stati saranno nella tabella per le connessioni da un dato indirizzo di origine. Una volta che gli stati per quella fonte scadono, così sarà l'associazione appiccicosa. Ulteriori connessioni da quell'host sorgente saranno reindirizzate al prossimo server web nel pool o al successivo gateway disponibile nel gruppo.

Per il traffico in uscita utilizzando un gruppo di gateway di bilanciamento del carico, l'associazione appiccicosa è tra l'utente e un gateway. Finché l'indirizzo locale ha degli stati nella tabella dello stato, tutte le sue connessioni fluiranno da un unico gateway. Questo può aiutare con protocolli come HTTPS e FTP, dove il server può essere rigoroso su tutte le connessioni provenienti dalla stessa fonte, o dove un ulteriore collegamento in entrata deve essere ricevuto dalla stessa fonte. Lo svantaggio di questo comportamento è che il bilanciamento non è così efficiente, un utente pesante potrebbe dominare un singolo WAN piuttosto che avere le loro connessioni sparse.

Per il bilanciamento del carico del server, descritto ulteriormente nel *Bilanciamento del carico del server*, sono auspicabili connessioni appiccicose per applicazioni che si basano sugli stessi indirizzi IP del server che vengono mantenuti per un utente durante una data sessione. Le applicazioni Web sui server potrebbero non essere abbastanza intelligenti da consentire una sessione utente di esistere su più server backend allo stesso tempo, quindi questo permette all'utente di raggiungere sempre lo stesso server fino a quando sta navigando in un sito. Questo comportamento potrebbe non essere richiesto a seconda del contenuto del server.

Suggerimento: Per un maggiore controllo su come le connessioni utente sono associate con i server in uno scenario di bilanciamento del carico, prendere in considerazione l'utilizzo del pacchetto HAProxy invece del bilanciatore di carico relayd integrato. HAProxy supporta diversi metodi per garantire che gli utenti siano correttamente indirizzati verso un server di backend.

Il **Timeout di tracciamento della sorgente** per connessioni appiccicose controlla per quanto tempo l'associazione appiccicosa sarà mantenuta per un host dopo che tutti gli stati da quell'host scadono. Il valore è specificato in secondi. Per impostazione predefinita, questo valore non è impostato, quindi l'associazione viene rimossa non appena gli stati scadono. Se le connessioni appiccicose sembrano funzionare inizialmente, ma sembrano interrompere parte attraverso le sessioni, aumentare questo valore per mantenere un'associazione più a lungo. I browser Web spesso tenere connessioni aperte per un po" perché gli utenti sono su un sito, ma se c'è un sacco di tempo di inattività, connessioni possono essere chiuse e gli stati possono scadere.

Commutazione Gateway predefinita

Abilitare la commutazione predefinita del gateway consente l'acquisizione di altri gateway non predefiniti se il gateway predefinito non è raggiungibile. Questo comportamento è disabilitato per impostazione predefinita. Con più WAN, la commutazione automatica del gateway predefinito garantirà che il firewall abbia sempre un gateway predefinito per far sì il traffico dal firewall stesso possa arrivare a Internet per DNS, aggiornamenti, pacchetti e servizi aggiuntivi come squid.

Suggerimento: quando si utilizza il risolutore DNS Resolver in modalità predefinita non d'inoltro, è necessario il passaggio predefinito del gateway per il funzionamento corretto di Multi-WAN. Se non è possibile utilizzare la commutazione predefinita del gateway, considerare di utilizzare invece la modalità di inoltro.

Ci sono casi in cui cambiare il gateway predefinito non è desiderabile, tuttavia, come quando il firewall ha altri gateway che non sono collegati a Internet. In futuro questa opzione sarà ampliata in modo da poter essere controllata sulla base del gateway.

Vedi anche:

Attenzione: Questa opzione è nota per non funzionare correttamente con una WAN di tipo PPP (PPPoE, L2TP, ecc.) come impostazione predefinita gateway.

Risparmio energetico

Quando è selezionata **Abilitare powerD,** il daemon powerD viene avviato. Questo daemon controlla il sistema e può abbassare o aumentare la frequenza della CPU in base all'attività del sistema. Se i processi hanno bisogno di potenza, la velocità della CPU sarà aumentata se necessario. Questa opzione ridurrà la quantità di calore generata da una CPU, e può anche ridurre il consumo di energia..

Nota: Il comportamento di questa opzione dipende molto dall'hardware in uso. In alcuni casi, la frequenza della CPU può diminuire, ma non ha alcun effetto misurabile sul consumo di energia e/o di calore, dove altri si raffredderanno e useranno meno energia considerevolmente. Si considera sicuro da eseguire, ma è lasciato fuori per impostazione predefinita a meno che l'hardware supportato viene rilevato.

La modalità per il poker può essere selezionato anche per tre stati del sistema:

Alimentazione a corrente alternata Funzionamento normale collegato alla corrente alternata.

Alimentazione a batteria Modalità da utilizzare quando il firewall è alimentato dalla batteria. Il supporto per il rilevamento della batteria varia a seconda dell'hardware.

Alimentazione sconosciuta Modalità utilizzata quando powerD non può determinare la sorgente di alimentazione.

Esistono quattro modalità scelte per ciascuno di questi stati:

Massimo Mantiene le prestazioni al livello più alto possibile in ogni momento.

Minimo Mantiene le prestazioni a livelli più bassi, per ridurre il consumo di energia.

Adattabile Cerca di bilanciare il risparmio energetico diminuendo le prestazioni quando il sistema è inattivo e aumentandole quando occupato.

Altamente adattabile Simile all'adattivo ma studiato per mantenere elevate le prestazioni a costo di un maggiore consumo di potenza. Alza la frequenza della CPU più velocemente e la abbassa più lentamente. Questa è la modalità predefinita.

Nota: Alcuni hardware richiedono l'esecuzione di powerD per funzionare alla sua massima frequenza della CPU raggiungibile. Se il dispositivo firewall non è abilitato, ma funziona sempre a quella che sembra essere una bassa frequenza della CPU, abilitare powerD e impostarlo al massimo per almeno lo stato di **Alimentazione a corrente alternata**.

Cane da guardia (Watchdog)

Alcuni hardware del firewall includono una funzione Watchdog che può ripristinare l'hardware quando il daemon del watchdog non può più interfacciarsi con l'hardware dopo un timeout specificato. Questo può aumentare l'affidabilità resettando un'unità quando si incontra un blocco rigido che potrebbe altrimenti richiedere un intervento manuale.

Lo svantaggio di qualsiasi hardware watchdog è che qualsiasi sistema sufficientemente occupato può essere indistinguibile da uno che ha subito un blocco rigido.

Abilitare Watchdog Se selezionata, viene eseguito il daemon del watchddogd che tenta di agganciarsi ad un dispositivo di controllo hardware supportato.

Timeout del watchdog Il tempo, in secondi, dopo il quale il dispositivo sarà ripristinato se non riesce a rispondere a una richiesta del watchdog. Se un firewall ha regolarmente un elevato carico e fa scattare il watchdog accidentalmente, aumentare il timeout.

Hardware termico e crittografico

Hardware crittografico

Ci sono alcune opzioni disponibili per accelerare le operazioni crittografiche tramite hardware. Alcune sono incorporate nel kernel, altre sono moduli caricabili. Un modulo opzionale è selezionabile qui: *AES-NI* (Advanced Encryption Standard, New Instructions). Se si sceglie l'*Accelerazione basata sulla CPU AES-NI* (aesni), allora il suo modulo del kernel verrà caricato quando salvato, e all'avvio. Il modulo *aesni* accelererà le operazioni per AES-GCM, disponibile in IPsec.

Il supporto per AES-NI è integrato in molte CPU Intel recenti e alcune AMD. Controllare con l'OEM per specifiche CPU o il supporto SoC.

Le velocità con AES-NI variano in base al supporto del software sottostante. Alcuni software basati su OpenSSL come OpenVPN possono funzionare in modo diverso con AES-NI scaricati poiché OpenSSL ha il supporto integrato per AES-NI. Il supporto IPsec sarà notevolmente aumentato caricando AES-NI a condizione che AES-GCM sia utilizzato e configurato correttamente.

Questi driver si collegano al framework crypto(9) di FreeBSD, così molti aspetti del sistema useranno automaticamente l'accelerazione per i cifrari supportati.

Ci sono altri dispositivi crittografici supportati, come *hifn(4)* e ubsec(4). Nella maggior parte dei casi, se viene rilevato un chip acceleratore supportato, verrà visualizzato nel widget **Informazioni di sistema** sula dashboard.

Sensori termici

Firew4LL è in grado di leggere i dati di temperatura da alcune fonti da visualizzare sulla dashboard. Se il firewall ha una CPU supportata, selezionare un sensore termico caricherà il driver appropriato per leggere la sua temperatura.

Sono supportati i seguenti tipi di sensori:

Nessuno/ACPI Il firewall cercherà di leggere la temperatura da un sensore della scheda madre compatibile con ACPI, se presente, altrimenti non sono disponibili letture del sensore.

Processore Intel Carica il modulo coretemp che supporta la lettura di dati termici dalle CPU della serie Intel core e altre moderne CPU Intel utilizzando i loro sensori on-die, tra cui i processori basato su Atom.

AMD K8, K10, e K11 Carica il modulo amdtemp che supporta la lettura di dati termici da CPU moderne AMD utilizzando i loro sensori on-die.

Se il firewall non ha un chip sensore termico supportato, questa opzione non avrà alcun effetto. Per scaricare il modulo selezionato, impostare questa opzione su Nessuno/ACPI e quindi riavviare il sistema.

Nota: I moduli coretemp e amdtemp riportano dati termici direttamente dal core della CPU. Questo può o non può essere indicativo della temperatura in altre parti del sistema. Le temperature del case possono variare notevolmente dalle temperature sulla matrice CPU.

Pianificazioni

L'opzione **Non terminare le connessioni quando scade la pianificazione* controlla se gli stati sono cancellati o meno quando una regola per le pianificazione passa in uno stato che bloccherebbe il traffico. Se deselezionata, le connessioni vengono interrotte quando il tempo di pianificazione è scaduto. Se selezionata, le connessioni vengono lasciate sole e non verranno automaticamente chiuse dal firewall.

Monitoraggio del gateway

Cancellare gli stati quando il gateway è down

Quando si utilizza la Multi-WAN, per impostazione predefinita il processo di monitoraggio non azzera gli stati quando un gateway va in down. Gli stati di flusso per ogni evento del gateway possono essere distruttivi in situazioni in cui un gateway è instabile.

L'opzione **Cancellare tutti gli stati quando un gateway è down** sovrascrive il comportamento predefinito, lo stato di compensazione per **tutte** le connessioni esistenti quando **qualsiasi** gateway non riesce. La cancellazione degli stati può aiutare a reindirizzare il traffico per le connessioni di lunga durata come VoIP telefono/tronco di registrazioni ad un altro WAN, ma può anche interrompere le connessioni in corso se un gateway meno utilizzato è sbattere che ancora uccidere tutti gli Stati quando non riesce.

Maggiori informazioni su come questo impatti sulla Multi-WAN può essere trovato in *Uccisione degli stati/Switch forzato*.

Nota: Quando questa opzone viene attivata, l'intera tabella di stato viene cancellata. Ciò è necessario perché non è possibile uccidere tutti gli Stati per la WAN non funzionante e per gli stati LAN associati alla WAN non funzionante. Rimuovere di stati sul lato WAN da solo è inefficace, pure gli stati lato LAN devono essere cancellati.

Salta le regole quando il Gateway è giù

Per impostazione predefinita, quando una regola ha un insieme di gateway specifici e questo gateway è down, il gateway è omesso dalla regola e il traffico viene inviato tramite il gateway predefinito.

L'opzione **Non creare regole quando il gateway è down** sovrascrive quel comportamento e l'intera regola viene omessa dal set di regole quando il gateway è down. Invece di scorrere attraverso il gateway predefinito, il traffico corrisponderà invece a una regola diversa. Questo è utile se il traffico deve sempre e solo utilizzare una specifica WAN e non scorrere mai su qualsiasi altra rete WAN.

Suggerimento: Quando si utilizza questa opzione, creare una regola di rifiuto o di blocco in accordo con la politica della regola di routing con gli stessi criteri di corrispondenza. Questo consentirà di evitare il traffico da altre regole potenzialmente corrispondenti al di sotto di essa nel set di regole e di prendere un percorso non intenzionale.

Impostazioni del disco RAM

Le directory /tmp e /var sono usate per scrivere file e contenere dati temporanei e/o volatili. Utilizzando un disco RAM si può ridurre la quantità di scrittura che avviene sui dischi del firewall. SSD moderne non hanno problemi di scrittura del disco come le vecchie unità, ma può ancora essere una preoccupazione quando si esegue da memoria flash di qualità inferiore, come le unità USB.

Questo comportamento ha il vantaggio di mantenere la maggior parte delle cancellazioni dal disco nel sistema di base, ma i pacchetti possono ancora scrivere frequentemente sul disco rigido. Richiede inoltre un trattamento aggiuntivo per garantire che i dati come i grafici RRD e le locazioni DHCP siano mantenuti in tutti i riavvii. I dati per entrambi vengono salvati durante un corretto spegnimento o riavvio, e anche periodicamente se configurato.

Utilizzare i dischi RAM Quando è selezionata, un disco di memoria viene creato all'avvio per /tmp e /var e la struttura associata viene inizializzata. Quando questa impostazione è attivata, si richiede un riavvio e viene forzato il salvataggio.

Dimensioni del disco di RAM /tmp La dimensione del disco RAM /tmp, in MiB. Il valore predefinito è 40, ma deve essere impostato su un valore più alto se non c'è RAM disponibile.

Dimensioni del disco di RAM /var La dimensione del disco RAM /var, in MiB. Il valore di default è 60, ma dovrebbe essere impostato con un valore molto più alto, soprattutto se verranno utilizzati i pacchetti. 512-1024 è un punto di partenza migliore, a seconda della RAM disponibile del firewall.

Backup periodico dei RRD Il tempo, in ore, tra i backup periodici dei file RRD. Se il firewall viene riavviato inaspettatamente, l'ultimo backup viene ripristinato quando lo firewall loavvia. Più basso è il valore, minori sono dati che verranno persi in tal caso, ma backup più frequenti scrivere di più sul disco.

Backup periodico delle locazioni DHCP Il tempo, in ore, tra i backup periodici dei database delle locazioni di DHCP. Se il firewall viene riavviato inaspettatamente, l'ultimo backup viene ripristinato quando il firewall lo avvia. Più basso è il valore, meinri sono i dati che verranno persi in tal caso, ma backup più frequenti scrivono di più sul disco.

Avvertimento: Attenzione: A parte i punti di cui sopra, ci sono diversi elementi per cui essere cauti quando si sceglie se utilizzare o meno l'opzione del disco di RAM. Usato impropriamente, questa opzione può portare alla perdita di dati o altri guasti imprevisti. I log di sistema sono mantenuti in /var ma non sono sottoposti a backup come i database RRD e DHCP. I log verranno reimpostati nuovamente ad ogni riavvio. Per i log persistenti, utilizzare syslog da remoto per inviare i log a un altro dispositivo in rete. I pacchetti potrebbero non tener conto dell'uso dei dischi della RAM e potrebbero non funzionare correttamente al momento dell'avvio o in altri modi. Provare ogni pacchetto, anche se non funziona immediatamente dopo il riavvio. Questi sono dischi RAM, quindi la quantità di RAM disponibile per altri programmi sarà ridotta dalla quantità di spazio utilizzato dai dischi RAM. Per esempio se il firewall ha 2GB di RAM, e ha 512MB per /var e 512MB per /tmp, allora solo 1GB di RAM sarà disponibile al sistema operativo per uso generale. Particolare attenzione deve essere presa quando si sceglie un formato di disco RAM, ciò è discusso nella sezione seguente.

Dimensioni del disco RAM

Impostare una dimensione troppo piccola per /tmp e /var può essere controproduttivo, specialmente quando si tratta di pacchetti. Le dimensioni suggerite sulla pagina sono un minimo assoluto e spesso sono richieste dimensioni molto più grandi. Il guasto più comune si ottiene quando un pacchetto è installato, e parti del pacchetto risiedono in entrambi /tmp e /var e si può infine riempire il disco RAM e causare la perdita di altri dati. Un altro errore comune è impostare /var come un disco RAM e poi dimenticare di spostare una cache squid in una posizione al di fuori di /var - se lasciato deselezionato, riempirà il disco RAM.

Per /tmp è richiesto un minimo di 40 MiB. Per /var è richiesto un minimo di 60 MiB. Per determinare la dimensione corretta, controllare l'uso corrente delle directory /tmp e /var prima di fare uno scambio. Controllare l'uso più volte nel corso di un paio di giorni in modo da non essere catturato in un punto basso. Tenere d'occhio l'uso durante l'installazione di un pacchetto aggiunge un altro utile punto per i dati.

7.6.5 Scheda dei parametri sintonizzabili del sistema

La scheda **Sistema dei parametri sintonizzabili** in **Sistema> Avanzate** fornisce un mezzo per impostare in fase di esecuzione settaggi di sistema FreeBSD, noto anche come *sysctl *OID. In quasi tutti i casi, si consiglia di lasciare questi parametri sintonizzabili sui valori predefiniti. Gli amministratori di firewall hanno familiarità con FreeBSD, o agli utenti che lo fanno sotto la direzione dello sviluppatore o di un rappresentante del supporto, possono decidere di modificare o aggiungere i valori in questa pagina in modo che essi siano impostati all'avvio del sistema.

Nota: I parametri sintonizzabili in questa pagina sono diversi dai Parametri sintonizzabili del caricatore. I Parametri sintonizzabili del caricatore sono valori di sola lettura dopo l'avvio del sistema, e questi valori devono essere impostati in /boot/loader.conf.local.

Creazione e modifica dei parametri sintonizzabili

Per modificare un sintonizzabile esistente, fare clic su  .

Per creare un nuovo sintonizzabile, fare clic su  **Nuovo** in cima alla lista.

Durante la modifica o la creazione di un sintonizzabile, i seguenti campi sono disponibili:

sintonizzabile L'OID sysctl da impostare

Valore Il valore a cui verrà impostato il sintonizzabile.

Nota: Alcuni valori hanno requisiti di formattazione. A causa del gran numero di OID sysctl, la GUI non convalida che il dato valore funzionerà per il sintonizzabile prescelto.

Descrizione Una descrizione facoltativa per riferimento.

Fare clic su **Salvare** quando il modulo è completo.

OID accordabili e valori

Ci sono molti OID disponibili da sysctl, alcuni di essi possono essere impostati, alcuni sono uscite di sola lettura, e altri devono essere impostati prima dell'avvio del sistema come parametri sintonizzabili del caricatore. L'elenco completo dei OID e i loro possibili valori è al fuori della portata di questo libro, ma per chi è interessato a scavare un poco più profondo, la pagina *sysctl *del manuale di FreeBSD contiene istruzioni dettagliate e informazioni.

7.6.6 Notifiche

Firew4LL notifica all'amministratore eventi ed errori importanti mediante la visualizzazione di un avviso nella barra dei menu, indicato dall'icona  . Firew4LL può anche inviare queste notifiche da remoto via e-mail utilizzando il protocollo SMTP o tramite Growl.

SMTP e-mail

Le notifiche e-mail sono fornite da una connessione SMTP diretta ad un server di posta. Il server deve essere configurato per consentire l'inoltro dal firewall o accettare connessioni SMTP autenticate.

Disabilitare SMTP Se selezionata, non verranno inviate le notifiche SMTP. Questo è utile per mettere a tacere le notifiche, mantenendo attive le impostazioni SMTP per altri utilizzi come ad esempio i pacchetti che utilizzano e-mail.

Server dell'e-mail L'hostname o l'indirizzo IP del server di posta elettronica tramite cui verranno inviate le notifiche.

Porta SMTP del server di e-mail La porta da utilizzare durante la comunicazione con il server SMTP. Le porte più comuni sono 25 e 587. In molti casi, la 25 non funziona a meno che non sia quella di un server di posta locale o interna. I fornitori bloccano di frequente le connessioni in uscita alla porta 25, in modo da utilizzare 587 (la porta di invio) quando possibile.

Timeout della connessione al server dell'e-mail Il periodo di tempo, in secondi, che il firewall attende che una una connessione SMTP sia completata.

Connessione SMTP sicura Quando impostato, il firewall tenterà una connessione SSL/TLS per l'invio di e-mail. Il server deve avere un certificato SSL valido e accettare connessioni SSL/TLS.

Indirizzo e-mail DA L'indirizzo di posta elettronica che verrà utilizzato nel campo DA: intestazione, che specifica la fonte del messaggio. Alcuni server SMTP tentano di convalidare questo indirizzo, la pratica migliore è quella di utilizzare un indirizzo reale in questo campo. E' comunemente impostato lo stesso indirizzo di quello di notifica e-mail.

Indirizzo di notifica e-mail L'indirizzo di posta elettronica per la A: intestazione del messaggio, che è la destinazione in cui le e-mail di notifica saranno consegnate dal firewall.

Nome utente per l'autenticazione delle E-Mail di notifica Opzionale. Se il server di posta richiede un nome utente e una password per l'autenticazione, inserire il nome utente qui.

Password per l'autenticazione delle E-Mail di notifica Opzionale. Se il server di posta richiede un nome utente e una password per l'autenticazione, inserire la password qui e nel campo di conferma.

Meccanismo per l'autenticazione delle E-Mail di notifica Questo campo specifica il meccanismo di autenticazione richiesto dal server di posta. La maggior parte dei server delle e-mail lavora con l'autenticazione PLAIN, altri, come MS Exchange potrebbe richiedere l'autenticazione stile LOGIN.

Cliccare su  **Salvare** per memorizzare le impostazioni prima di procedere.

Cliccare su  **Impostazioni SMTP di prova** per generare una notifica di prova e inviarlo tramite SMTP utilizzando le impostazioni memorizzate in precedenza. Salvare le impostazioni prima di fare clic su questo pulsante.

Suono all" avvio/arresto

Se l'hardware firewall ha un altoparlante PC Firew4LL gimmetterà un suono quando l'avvio finisce e di nuovo quando viene avviato un arresto.

Selezionare **Disattivare il segnale acustico di avvio/arresto** per evitare che il firewall emetta questi suoni.

Growl

Growl fornisce un metodo discreto di fornire notifiche sul desktop. Queste notifiche pop-up compaiono sul desktop e poi si nascondono o svaniscono. Growl è disponibile in App Store per Mac OSX, ed è accessibile s Windows e anche su FreeBSD/Linux.

Disattivare le notigiche Growl Se selezionata, il firewall non invierà notifiche Growl.

Nome di registrazione Il nome del servizio che il firewall utilizza per registrare con il server Growl. Per default è Firew4LL-Growl. Consideriamo questo come il *tipo* di notifica vista dal server Growl.

Nome di notifica Il nome del sistema che produce le notifiche. Il valore predefinito di avviso growl Firew4LL può essere sufficiente, personalizzarlo con l'hostname firewall o qualsiasi altro valore per differenziarlo.

Indirizzo IP L'indirizzo IP a cui il firewall invierà notifiche Growl.

Password La password richiesta dal server Growl.

Cliccare su **Salvare** per memorizzare le impostazioni prima di procedere.

Cliccare su **Impostazioni Growl per la prova** per inviare una notifica di test tramite Growl utilizzando le impostazioni salvate in precedenza. Salvare prima di tentare un test.

7.7 Nozioni di base del menu della console

Le operazioni di configurazione e manutenzione di base possono essere eseguite dalla console di sistema. La console è disponibile tramite tastiera e monitor, console seriale o SSH. I metodi di accesso variano a seconda dell'hardware. Di seguito è riportato un esempio di come apparirà il menu della console, ma può variare leggermente a seconda della versione e della piattaforma:

|image49|

7.7.1 Assegnare Interfacce

Questa opzione riavvia il compito di **Assegnazione di interfaccia**, che è coperto in dettaglio in *Assegnare Interfacce* e *Assegnazione manualmente le Interfacce*. Questa opzione di menu è possibile creare interfacce VLAN, riassegnare le interfacce esistenti, o assegnarne di nuove.

7.7.2 Impostare indirizzo IP dell'interfaccia (delle interfaccee)

Lo script per impostare un indirizzo IP interfaccia può impostare gli indirizzi IP di interfacce WAN, LAN, o OPT, ma ci sono anche altre utili funzioni su questo script:

- I prompt del firewall per abilitare o disabilitare il servizio DHCP per un'interfaccia, e per impostare l'intervallo di indirizzi IP DHCP se è abilitato.
- Se la GUI del firewall è configurato per HTTPS, i prompt di menu per passare a HTTP. Questo aiuta nei casi in cui la configurazione SSL non funziona correttamente.
- Se la regola anti-blocco sulla LAN è stata disabilitata, lo script consente la regola anti-blocco nel caso in cui l'utente è stato bloccato fuori dalla GUI.

Reimpostazione della password del configuratore web

Questa opzione di menu richiama uno script per reimpostare la password e lo stato di account dell'admin. La password viene reimpostata al valore predefinito di Firew4LL.

Lo script prevede anche un paio di altre azioni per contribuire a recuperare l'ingresso al firewall:

- Se la fonte di autenticazione GUI è impostato su un server remoto, come RADIUS o LDAP, viene richiesto di restituire la fonte di autenticazione al database locale.
- Se l'account amministratore è stato rimosso, lo script ricrea l'account.

- Se l'account dell'amministratore è disattivato, lo script riattiva l'account.

7.7.3 Ripristino delle impostazioni di fabbrica

Questa opzione del menu ripristina la configurazione del sistema alle impostazioni di fabbrica. Tenterà inoltre di rimuovere tutti i pacchetti installati.

Nota: Questa azione non apportare altre modifiche al file system. Se i file di sistema sono stati danneggiati o alterati in modo indesiderato, la pratica migliore è quella di fare una copia di backup, e reinstallare dal supporto di installazione.

Questa azione è disponibile anche nella WebGUI in **Diagnostica>Impostazioni di fabbrica**.

7.7.4 Riavvio del sistema

Questa scelta del menu arresterà in modo pulito Firew4LL e riavvierà il sistema operativo.

Alcune opzioni avanzate possono essere visualizzate anche in questa pagina, a seconda del supporto hardware:

Riavviare normalmente Esegue un riavvio normale in modo tradizionale.

Reroot Questa opzione non esegue un riavvio completo, ma un yb riavvio in stile "reroot". Tutti i processi in esecuzione vengono terminati, tutti i file system vengono rimontati, e quindi la sequenza di avvio del sistema viene eseguita nuovamente. Questo tipo di riavvio è molto più veloce in quanto non ripristina l'hardware, ricarica il kernel, o necessita di passare attraverso il processo di rilevamento dell'hardware.

Riavviare in modalità utente singolo Questa operazione riavvierà il firewall in modalità singolo utente per scopi diagnostici. Il firewall non può recuperare automaticamente da questo stato, l'accesso alla console è necessario per utilizzare la modalità utente singolo e riavviare il firewall.

Avvertimento: Attenzione: In modalità utente singolo, le impostazioni predefinite filesystem di root di sola lettura e altri file system non sono montati. Il firewall inoltre non dispone di una connessione di rete attiva. Questa opzione deve essere utilizzata solo sotto la guida di un rappresentante del supporto o un utente di FreeBSD con conoscenze avanzate.

Riavviare ed eseguire un controllo del filesystem Questo riavvia il firewall e forze un controllo del filesystem utilizzando fsck, si esegue per cinque volte. Questa operazione in genere può correggere i problemi con il file system sul firewall.

Nota: La modalità utente singolo e le opzioni di controllo del filesystem richiedono una lettera maiuscola da inserire per confermare l'azione. Ciò è necessario per evitare di attivare le opzioni accidentalmente. Le opzioni di riavvio e reroot possono essere inserite in maiuscolo o minuscolo.

Questa azione è disponibile anche nella WebGUI in **Diagnostica>Riavvio**

7.7.5 Arresta il sistema

Questa scelta di menu interrompe in modo pulito il firewall e allo stesso tempo lo ferma o lo spegne a seconda del supporto hardware.

Questa azione è anche disponibile nella WebGUI in **Diagnostica>Arresta il sistema**

7.7.6 Ping host

Questa opzione del menu esegue uno script che tenta di contattare un host per confermare se è raggiungibile tramite una rete collegata. Lo script richiede all'utente un indirizzo IP, e poi invia all'host di destinazione tre richieste ICMP echo.

Lo script visualizza l'output del test, incluso il numero di pacchetti ricevuti, i numeri di sequenza, i tempi di risposta e la percentuale di perdita di pacchetto.

Lo script usa ping quando viene dato un indirizzo IPv4 o un hostname, e ping6 quando viene dato un indirizzo IPv6.

7.7.7 Shell

Questa scelta del menù avvia una linea di comando nella shell. Una shell è molto utile e molto potente, ma ha anche il potenziale per essere molto pericolosa.

Nota: La maggior parte degli utenti Firew4LL non hanno bisogno di usare la shell, o anche di sapere che esiste.

Le attività di configurazione complesse possono richiedere l'impiego della shell, e alcuni compiti di risoluzione dei problemi sono facilmente eseguibili dalla shell, ma c'è sempre la possibilità di causare un danno irreparabile al sistema.

Gli utenti veterani di FreeBSD possono sentirsi un po "come a casa lì, ma ci sono molti comandi che non sono presenti in un sistema Firew4LL in quanto le parti non necessarie del sistema operativo vengono rimosse per vincoli di sicurezza e dimensioni.

Una shell avviata in questo modo usa tcsh, e l'unica altra shell disponibile è sh. Anche se è possibile installare altre shell per la comodità degli utenti, non è consigliabile o supportato l'utilizzo di altre shell.

7.7.8 pfTop

Questa opzione del menu richiama pftop che mostra una visione in tempo reale degli stati del firewall, e la quantità di dati che hanno inviato e ricevuto. Può aiutare le sessioni di pinpoint che attualmente utilizzano grandi quantità di larghezza di banda, e può anche aiutare a diagnosticare altri problemi di connessione di rete.

Vedi anche:

Vedere *Guardare gli stati con pfTop* per ulteriori informazioni su come utilizzare pfTop.

7.7.9 Filtri Log

L'opzione di menu **Filtri Log** visualizza le voci di registro del firewall in tempo reale, nella loro forma grezza. I registri grezzi contengono molte più informazioni per linea della vista del registro nella WebGUI (**Stato> Registri di sistema, scheda Firewall**), ma non tutte queste informazioni sono facili da leggere.

Suggerimento: Per una vista da console semplificata dei registri in tempo reale con dettagli bassi, utilizzare questo comando shell:

7.7.10 Riavviare webConfigurator

Il riavvio del webConfigurator riavvia il processo di sistema che esegue la WebGUI (nginx). In casi estremamente rari il processo potrebbe essere interrotto, e il riavvio ripristinerà l'accesso alla GUI.

Se l'interfaccia grafica non risponde e questa opzione non consente di ripristinare l'accesso, selezionare l'opzione 16 del menu per **Riavviare PHP-FPM** dopo l'utilizzo di questa opzione di menu.

7.7.11 PHP Shell + Strumenti Firew4LL

La shell PHP è una potente utility che esegue il codice PHP nel contesto del sistema in esecuzione. Come con la shell normale, è anche potenzialmente pericolosa da usare. Questa è usata principalmente dagli sviluppatori e utenti esperti che sono intimamente familiari sia con PHP sia il codice di base di Firew4LL.

Gli script di ripristino

Ci sono diversi script di riproduzione per la shell PHP che automatizzano compiti semplici o consentono l'accesso alla GUI.

Questi script vengono eseguiti all'interno della shell PHP in questo modo:

```
firew4ll shell:  playback scriptname
```

Possono essere anche eseguiti da una linea di comando come:

changepassword

Questo script modifica la password di un utente, e richiede di ripristinare le proprietà dell'account se è disabilitato o scaduto.

disablecarp/enablecarp

Questi script disabilitano e abilitano le funzioni di alta disponibilità CARP, e disattiverà gli indirizzi virtuali IP di tipo CARP. Questa azione non persiste dopo il riavvio.

disablecarpmaint/enablecarpmaint

Questi script attivano e disattivano la modalità di manutenzione CARP, che lascia attivo il CARP ma degrada questa unità così l'altro nodo può assumere il controllo. Questa modalità di manutenzione persisterà dopo il riavvio.

disabledhcpd

Questo script rimuove tutte le configurazioni DHCP dal firewall, disabilitando il servizio DHCP e rimuovendo completamente tutte le relative impostazioni.

disablerefercheck

Questo script disattiva il controllo di HTTP_REFERER menzionato in *Applicazione HTTP_REFERER del browser*. Questo può aiutare per ottenere l'accesso alla GUI se una sessione del browser innesca questa protezione.

enableallowallwan

Questo script aggiunge il consenso a tutte le regole per IPv4 e IPv6 per l'interfaccia WAN.

Avvertimento: Essere estremamente attenti con questa opzione, è destinata ad essere una misura temporanea per ottenere l'accesso ai servizi sull'interfaccia WAN del firewall in situazioni in cui la rete LAN non è utilizzabile. Una volta che le regole di accesso corrette sono messe in atto, rimuovere le regole aggiunte da questo script.

enablesshd

Questo script abilita il daemon SSH, come l'opzione di menu della console o l'opzione GUI.

externalconfiglocator

Questo script cercherà un file config.xml su un dispositivo esterno, come ad esempio una chiavetta USB, e lo sposterà in posizione per l'uso da parte del firewall.

gatewaystatus

Questo script stampa lo stato del gateway corrente e le statistiche. Accetta anche un parametro opzionale breve che stampa solo il nome di gateway e lo stato, omettendo gli indirizzi e dati statistici.

generateguicert

Questo script crea un nuovo certificato auto-firmato per il firewall e lo attiva per l'impiego nella GUI. Questo è utile nei casi in cui il certificato precedente è valido o altrimenti non utilizzabile. Si riempie anche nei dettagli del certificato utilizzando l'hostname del firewall e altre informazioni personalizzate, per meglio identificare l'host.

gitsync

Questo script complesso sincronizza il PHP e altre fonti di script con i file dal repository github di Firew4LL. E' più utile sullo snapshot di sviluppo per raccogliere le modifiche dall'impegno più recente.

Avvertimento: Questo script può essere pericoloso da utilizzare in altre circostanze. utilizzare questo solo sotto la direzione di un rappresentante dello sviluppatore o un supporto tecnico.

Se lo script viene eseguito senza alcun parametro stampa un messaggio di aiuto che illustra il suo utilizzo. Maggiori informazioni possono essere trovate sul Firew4LL Doc Wiki.

installpkg / listpkg / uninstallpkg

Questi script si interfacciano con il sistema dei pacchetti Firew4LL in un modo simile alla GUI. Questi sono utilizzati principalmente per il debug dei problemi del pacchetto, confrontando le informazioni in config.xml rispetto al database dei pacchetti.

pfanchordrill

Questo script ricorsivamente ricerca attraverso gli ancoraggi di pf e stampa qualsiasi NAT o regole del firewall che trova. Questo può aiutare a rintracciare un comportamento imprevisto in settori come il bilanciamento del carico relayd che si basano sulle regole di ancoraggio che altrimenti non sarebbero visibili nella GUI.

pftabledrill

Questo script stampa il contenuto di tutte le tabelle pf, che contengono indirizzi utilizzati nelle alias del firewall così come tabelle di sistema integrato per funzioni come il blocco della rete bogon, snort, e blocco GUI/SSH. Questo script è utile per controllare se un indirizzo IP specifico si trova in qualsiasi tabella, piuttosto che la ricerca individuale.

removepkgconfig

Questo script rimuove tutte le tracce di dati di configurazione del pacchetto dalla esecuzione di config.xml. Questo può essere utile se un pacchetto ha impostazioni danneggiate o altrimenti ha lasciato i pacchetti in uno stato incoerente.

removeshaper

Questo script rimuove le impostazioni shaper del traffico ALTQ, che può essere utile se la configurazione shaper impedisce regole di carico o è altrimenti scorretta e previene il corretto funzionamento del firewall.

resetwebgui

Questo script ripristina le impostazioni della GUI per i widget, colonne cdella dashboard, il tema e altre impostazioni relative alla GUI. Può restituire la GUI, in particolare la dashboard, ad uno stato stabile se non funziona correttamente.

restartdhcpd

Questo script arresta e riavvia il daemon DHCP.

restartipsec

Questo script riscrive e ricarica la configurazione IPsec per strongSwan.

svc

Questo script permette di controllare i servizi in esecuzione sul firewall, come interagire con i servizi a **Stato> Servizi**.

La forma generale del comando è:

```
playback svc <action> <service name> [service-specific options]
```

L'azione può essere fermata, iniziata, o riavviata.

Il **nome del servizio** è il nome dei servizi come si trova in **Stato> Servizi**. Se il nome include uno spazio, racchiudere il nome tra virgolette.

Le opzioni delle specifiche di servizio variano a seconda del servizio, sono utilizzate per identificare in modo univoco i servizi con più istanze, come ad esempio le voci OpenVPN o Captive Portal.

Esempi:

- **Fermare miniupnpd:** `pfSsh.php playback svc stop miniupnpd`
- **Riavviare il client OpenVPN con ID 2:** `pfSsh.php playback svc restart openvpn client 2`
- **Avviare il processo del Captive Portal per la zona "MiaZona":** `pfSsh.php playback svc start captiveportal MyZone`

7.7.12 Aggiornamento dalla console

Questa opzione del menu esegue lo script Firew4LL-aggiornamento per aggiornare il firewall per l'ultima versione disponibile. Questa è operativamente identica a eseguire un aggiornamento dalla GUI e richiede una connessione di rete per raggiungere il server di aggiornamento.

Questo metodo di aggiornamento è coperto con maggiori dettagli in *Aggiornamento utilizzando la Console*.

7.7.13 Attivare/Disattivare SSHD

Questa opzione attiva o disattiva lo stato del daemon della Shell,sicura SSHD. Questa opzione funziona come l'opzione nella WebGUI per abilitare o disabilitare SSH, ma è accessibile dalla console.

7.7.14 Ripristino della configurazione recente

Questa opzione di menu avvia uno script che elenca e ripristina i backup dalla cronologia della configurazione. Questo è simile a l'accesso alla cronologia della configurazione dalla GUI in **Diagnostica> Backup/Ripristino** nella scheda **Cronologia di configurazione**.

Questo script è in grado di visualizzare gli ultimi file di configurazione, con un timestamp e la descrizione della modifica apportata nella configurazione, l'utente e l'indirizzo IP che ha effettuato la modifica, e la revisione di configurazione. Ciò è particolarmente utile se un errore di configurazione recente accidentalmente ha rimosso l'accesso alla GUI.

7.7.15 Riavviare PHP-FPM

Questa opzione del menu arresta e riavvia il deaemon che gestisce i processi di PHP per nginx. Se il processo del server web della GUI è in esecuzione, ma in grado di eseguire lo script PHP, richiamare questa opzione. Eseguire questa opzione in combinazione con **Riavviare il configuratore web** per il miglior risultato.

7.8 Sincronizzazione dell'orario

Il tempo e le questioni dell'orologio sono relativamente comuni sull" hardware, ma sui firewall sono critiche, soprattutto se il firewall sta eseguendo attività che coinvolgono i certificati di convalida come parte di un'infrastruttura PKI.

La sincronizzazione dell'orario di sistema è una necessità primaria sui sistemi integrati, alcuni dei quali non hanno una batteria a bordo per preservara la date e l'ora quando la corrente elettrica viene tolta.

Non solo questo aiuterà a mantenere tutto in linea con i compiti critici del sistema, ma assicura anche che i file di log sul firewall siano adeguatamente cronometrati, il che aiuterà la risoluzione dei problemi, la tenuta dei registri e la gestione generale del sistema.

7.8.1 Problemi per mantenere l'orario

L'hardware può avere problemi significativi nel mantenere l'orario, anche se tali problemi sono generalmente isolati dall'hardware vecchio e di bassa qualità. Tutti gli orologi del PC andranno alla deriva in una certa misura, ma alcuni hardware può andare alla deriva fino a un minuto ogni paio di minuti che passano e rapidamente sfuggono alla sincronia. NTP è progettato per aggiornare periodicamente il tempo del sistema per tenere conto della deriva normale. Non può ragionevolmente correggere gli orologi che vanno alla deriva in modo significativo. Questo è molto raro, ma ci sono alcuni metodi che possono potenzialmente aggirare questi problemi.

Il modo migliore per evitare problemi di tempo è quello di utilizzare un hardware di qualità che è stato testato e non fa verificare questi problemi, come l'hardware trovato nel negozio Firew4LL.

Ci sono quattro elementi per controllare se l'hardware presenta significativi problemi di mantenimento dell'orario.

NTP (Network Time Protocol)

Per impostazione predefinita, i tentativi Firew4LL per sincronizzare l'ora utilizzando il pool di server del protocollo dell'orario di rete (NTP) ntp.org. Questo assicura una data precisa e l'ora sul firewall, e ospiterà il normale scostamento d'orario. Se la data e l'ora del firewall non sono corrette, garantire la sincronizzazione NTP è in funzione. Il problema più comune che impedisce la sincronizzazione è la mancanza di un'adeguata configurazione DNS sul firewall. Se il firewall non può risolvere i nomi degli host, la sincronizzazione NTP fallirà. I risultati di sincronizzazione vengono visualizzati in fase di avvio nel registro di sistema, e lo stato della sincronizzazione dell'orologio NTP può essere visualizzato in **Stato> NTP**. Il widget **stato di NTP** per la Dashboard offre anche informazioni di base relative al server NTP selezionato per l'uso da parte del firewall.

Aggiornamenti BIOS

Abbiamo visto vecchi hardware che funzionavano bene per anni su Windows incontrare grossi problemi nel mantenere l'orario una volta ridistribuito su FreeBSD (e di conseguenza, Firew4LL). I sistemi stavano eseguendo una versione del BIOS con diverse revisioni obsolete. Una delle revisioni ha affrontato un problema di mantenimento dell'orario che apparentemente non ha mai interessato Windows. L'applicazione del BIOS aggiornamento ha risolto il problema. La prima cosa da controllare è assicurarsi che l'hardware in questione abbia l'ultimo BIOS disponibile.

Impostazioni PNP del sistema operativo nel BIOS

Un altro hardware potrebbe avere difficoltà a mantenere l'orario in FreeBSD e Firew4LL a meno che il sistema operativo con PNP nel BIOS non sia stato impostato su *No*. Se il BIOS non ha un'opzione di configurazione PNP del sistema operativo, cercare un'impostazione del OS e impostare su *altri*.

Disabilitare ACPI

Alcuni fornitori di BIOS hanno prodotto le implementazioni ACPI (Advanced Configuration and Power Interface) che sono buggy nella migliore delle ipotesi e pericolose nella peggiore delle ipotesi. In più di un'occasione abbiamo incontrato hardware che non si avvierebbero o funzionerebbero correttamente quando il supporto ACPI è attivo.

Mentre il supporto ACPI può essere disattivato nel BIOS e nel sistema operativo, si consiglia di non utilizzare hardware che richieda tali cambiamenti.

Regolare impostazioni Timecounter

Sui sistemi rari, il valore sysctl del `kern.timecounter.hardware` può avere bisogno di essere cambiato per correggere un'imprecisione dell'orologio. Questo è noto per essere un problema con le versioni precedenti di VMware, come ESX 5.0 in combinazione con un'immagine Firew4LL o FreeBSD basata su amd64. Questo caso particolare è stato un bug nel hypervisor che è stato risolto nel ESX 5.1 e nei successivi.

In questi sistemi il contatore del tempo predefinito finirà per fermare l'orologio dal ticchettio, causando problemi la crittografia, con le VPN e i servizi in generale. Su altri sistemi, l'orologio potrebbe provocare distorsioni di grandi quantità con il contatore del tempo sbagliato.

Per cambiare il contatore del tempo, accedere a **Sistema> Avanzate**, nella scheda **Parametri sintonizzabili del sistema** e aggiungere una voce da impostare `kern.timecounter.hardware` a `i8254`

Ciò fa in modo che il sistema utilizzi il chip i8254 come contatore del tempo, che tipicamente mantiene bene ma non può essere veloce come altri metodi. Le altre scelte di contatore del tempo verranno spiegate più avanti in questa sezione.

Se il sistema tiene il tempo corretto dopo aver fatto questo cambiamento, lasciare la voce sintonizzabile in atto per rendere questo cambiamento permanente. Se la modifica non ha aiutato, rimuovere il sintonizzabile o provare un altro valore.

A seconda della piattaforma e dell'hardware, ci possono essere anche altri contatori di tempo da provare. Per una lista di quelli disponibili su un firewall, eseguire il seguente comando:

```
# sysctl kern.timecounter.choice
```

Il firewall stamperà un elenco dei contatori di tempo disponibili e la loro «qualità» come riportato da FreeBSD:

```
kern.timecounter.choice:  TSC-low(1000) ACPI-safe(850) i8254(0)
dummy(-1000000)
```

Provare una di questi quattro valori per l'impostazione sysctl di `kern.timecounter.hardware`. In termini di "qualità" in questo elenco, il più grande è il numero migliore, ma la fruibilità effettiva varia da sistema a sistema.

> **TSC** Un contatore della CPU, ma è legato alla frequenza di clock e non è leggibile da altre CPU. Può essere utilizzato in sistemi bare metal SMP ma richiede che i TSC su tutte le CPU siano sincronizzati. Non può essere utilizzato in modo affidabile su sistemi con CPU a velocità variabile o sistemi virtualizzati con più CPU.
>
> **i8254** Un chip del clock che si trova nella maggior parte degli hardware, che tende ad essere sicuro, ma può avere problemi prestazionali.
>
> **ACPI-sicuro** Se opportunamente supportata dall'hardware, questa è una buona scelta perché non soffre delle limitazioni delle prestazioni di i8254, ma in pratica la sua precisione e velocità variano ampiamente a seconda dell'implementazione.
>
> **ACPI-veloce** Una più rapida attuazione del contatore ACPI disponibile su hardware che non soffre di problemi ACPI noti.
>
> **HPET** Timer degli eventi ad alta precisione, disponibile in alcuni hardware. Se disponibile, è generalmente considerato una buona fonte per un conteggio del tempo accurato.

Questo ed altro informazioni sui contatori del tempo di FreeBSD si possono trovare nel documento Contatori del tempo: efficiente e preciso mantenimento del tempo nel kernel SMP di Poul-Henning Kamp del progetto FreeBSD, e nel codice sorgente di FreeBSD.

Regolare la frequenza del timer del Kernel

In rari casi, regolando la frequenza del timer del kernel, o il sintonizzabile del kernel kern.hz, si possono aiutare le prestazioni o la stabilità. Questo è particolarmente vero in ambienti virtualizzati. Il valore predefinito è 1000, ma in

alcuni casi 100, 50, o 10 sarà un valore migliore a seconda del sistema. Quando Firew4LL è installato in VMware, viene rilevato e impostato automaticamente questo parametro sintonizzabile a 100, che dovrebbe funzionare bene in quasi tutti i casi con prodotti VMware.

Per modificare questa impostazione, aggiungere una riga al /boot/loader.conf.local con il nuovo valore:

7.8.2 Sincronizzazione ora GPS

Come aiuto nel mantenere un orologio preciso, la sincronizzazione dell'ora GPS è fornita anche da Firew4LL su un hardware supportato. Sono supportati alcuni dispositivi seriali o GPS con USB, e in combinazione con server per l'orario, che possono aiutare a mantenere l'orologio preciso. Per ulteriori dettagli, vedere *nTPD*.

7.9 Risoluzione dei problemi

L'**installazione guidata** e le attività di configurazione relative funzionano per la maggior parte delle situazioni, ma ci possono essere problemi nel far sì che le connessioni fluiscano normalmente nelle direzioni previste. Alcuni di questi problemi possono essere specifici di un particolare ambiente o di configurazione, ma possono essere affrontati con la risoluzione dei problemi di base.

7.9.1 Non riesco ad accedere WebGUI dalla LAN

Se la WebGUI non è accessibile dalla LAN, la prima cosa da controllare è il cablaggio. Se il cavo è un cavo fatto a mano o più breve di 3 piedi (un metro), provare un cavo diverso. Se il PC client è collegato direttamente a un'interfaccia di rete sul firewall, può essere necessario un cavo di crossover per un vecchio hardware che non ha il supporto Auto-MDIX sulle sue schede di rete. Questo non è un problema di gigabit o hardware più veloce.

Una volta che c'è una luce di collegamento sia sulla scheda di rete client e sia sull'interfaccia LAN del firewall, controllare la configurazione TCP/IP sul PC client. Se il server DHCP è abilitato sul firewall, come impostazione predefinita, assicurarsi che il client sia impostato anche per DHCP. Se DHCP è disabilitato sul firewall, il codice rigido su un indirizzo IP del client che risiede nella stessa sottorete come indirizzo IP della LAN del firewall, con la stessa maschera di sottorete, e utilizzare l'indirizzo IP della LAN del firewall come gateway e server DNS.

Se il cablaggio e le impostazioni di rete sono corrette, il client sarà in grado di rintracciare l'indirizzo IP della LAN del firewall. Se il PC client può rintracciare ma non accedere alla WebGUI, ci sono ancora un paio di cose da provare. In primo luogo, se l'errore sul PC client è un ripristino della connessione o un guasto, allora o il daemon del server che esegue la WebGUI non è in esecuzione o il client sta tentando di utilizzare la porta sbagliata. Se l'errore è invece un timeout di connessione, ciò punta più verso una regola firewall.

Se il client riceve un timeout di connessione, fare riferimento a *Cosa fare quando si viene bloccati fuori dalla WebGUI*. Con una connessione di rete configurata correttamente, questo non dovrebbe accadere, e quella sezione offre modi per aggirare i problemi con le regole del firewall.

Controllare due volte che la WAN e la LAN non siano sulla stessa sottorete. Se la WAN è impostato per il DHCP ed è collegato dietro un altro router NAT, può anche usare 192.168.1.1. Se la stessa sottorete è presente sulla WAN e sulla LAN, possono verificarsi risultati imprevedibili, tra cui l'impossibilità di instradare il traffico o accedere alla WebGUI. In caso di dubbio, scollegare il cavo WAN, riavviare il firewall Firew4LL e riprovare.

Se il client riceve un ripristino della connessione, prima provare a riavviare il processo server WebGUI dalla console di sistema, tipicamente l'opzione 11, seguita dall'opzione 16 per riavviare PHP-FPM. Se questo non aiuta, avviare una shell dalla console (opzione 8) e digitare:

```
# sockstat | grep nginx
```

Il firewall restituirà una lista di tutti i processi Nginx in esecuzione, e la porta su cui sono in ascolto, come questa:

root	nginx	41948	5	tcp4	*:443	*:*
root	nginx	41948	6	tcp6	*:443	*:*
root	nginx	41948	7	tcp4	*:80	*:*
root	nginx	41948	8	tcp6	*:80	*:*

In quell'output, si mostra che il processo è in ascolto sulla porta 443 di ogni interfaccia sia IPv4 sia IPv6, così come la porta 80 per il reindirizzamento, ma che può variare in base alla configurazione del firewall.

Provare a connettersi all'indirizzo IP della LAN del firewall usando direttamente quella porta, sia HTTP sia HTTPS. Per esempio, se l'indirizzo IP della LAN era 192.168.1.1, e stava ascoltando sulla porta 82, provare http://192.168.1.1:82 e https:///192.168.1.1:82.

7.9.2 Non si naviga in internet dalla LAN

Se il PC client è in grado di raggiungere la WebGUI ma non Internet, ci sono diverse cose da considerare. L'interfaccia WAN può non essere configurata correttamente, la risoluzione DNS potrebbe non funzionare, ci potrebbe essere un problema con le regole del firewall, con regole del NAT, o anche qualcosa di semplice come un problema di gateway locale.

Problemi con l'interfaccia WAN

In primo luogo, controllare l'interfaccia WAN per essere sicuri che sia operativa. Andare alla sezione **Stato> Interfacce** e guardare lo stato dell'interfaccia WAN. Se l'interfaccia funziona correttamente lo stato mostrerà "up". Se mostra "nessun vettore" o "down", effettuare un doppio controllo del cablaggio e delle impostazioni WAN in **Interfacce> WAN**.

Se l'interfaccia utilizza PPPoE o PPTP per il tipo di WAN, v'è una linea di stato supplementare che indica se la connessione PPP è attiva. Se è down, provare a premere il pulsante  **Connettere**. Se questo non funziona, effettuare un doppio controllo di tutte le impostazioni di interfaccia su **interfacce> WAN**, controllare o riavviare il provider CPE (modem via cavo/DSL, ecc), e, forse, consultare il provider di servizi Internet per un aiuto per quanto riguarda le impostazioni e lo stato del circuito.

Problemi relativi alla risoluzione DNS

All'interno della WebGUI, navigare fino a **Diagnostica > Ping** e inserire l'indirizzo del gateway ISP. L'indirizzo del gateway è elencato in **Stato > Interfacce** per l'interfaccia WAN e sotto **Stato> Gateway**.

Se il gateway è sconosciuto, provare un altro indirizzo valido come 8.8.8.8. Se il firewall è in grado di tracciare l'indirizzo e ricevere una risposta, ripetere lo stesso ping test dal PC client. Aprire una riga di comando o una finestra del terminale, e rintracciare lo stesso indirizzo IP.

Se il client può rintracciare l'indirizzo IP, quindi provare a ritrovare un sito web per nome come www.google.com. Provare dal firewall GUI e dal PC client. Se il ping test dell'IP funziona, ma il test del nome non riesce, allora c'è un problema con la risoluzione DNS. Vedere *Provare la connettività per gli aggiornamenti bogon*.

Se la risoluzione DNS non funziona sul firewall, controllare prima quale servizio DNS è abilitato sul firewall e come è configurato. Per impostazione predefinita, un firewall Firew4LL è configurato per utilizzare il risolutore DNS in una modalità che non richiede server DNS specifici. Interrogare direttamente i server root e altri server autorevoli. Installazioni precedenti e installazioni aggiornate predefinite del DNS Forwarder, che richiede ai server DNS Server di essere inseriti in **Sistema > Impostazioni generali** o da acquisire da un WAN dinamico come DHCP o PPPoE. Il risolutore DNS può operare anche in questa modalità se **Abilitare la modalità d'inoltro** è attivata nelle sue impostazioni.

Se il risolutore del DNS è attivo ma il firewall non è in grado di risolvere i nomi dell'host, il problema è di solito una mancanza di connettività della WAN. A parte questo, una possibilità è che la WAN o la marcia della rete upstream non passa correttamente il traffico DNS in un modo che è compatibile con DNSSEC. Disabilitare DNSSEC nelle opzioni del risolutore per vedere se questo permette alla risoluzione di funzionare. È anche possibile che l'ISP filtri le richieste DNS e richieda l'uso di server DNS specifici. In tal caso, configurare i server DNS e quindi attivare la modalità di inoltro o passare al DNS Forwarder.

Le impostazioni del server DNS del firewall sono sotto **Sistema>Impostazioni generali**, e sono visibili anche su **Stato>Interfacce**. Verificare con ping per essere sicuri che questi server DNS siano raggiungibili. Se il firewall può raggiungere l'indirizzo del gateway presso l'ISP, ma non i server DNS, contattare l'ISP e ricontrollare tali valori. Se i server DNS sono ottenuti tramite DHCP o PPPoE e il firewall non può raggiungerli, contattare l'ISP. Se tutto il resto non riesce, prendere in considerazione l'utilizzo della i nome server della pubblica DNS di Google (8.8.8, 8.8.4.4) sul firewall invece di quelli forniti dall'ISP.

Se DNS funziona dal firewall Firew4LL ma non da un PC client, potrebbe essere la configurazione del risolutore DNS o il DNS Forwarder sul firewall, la configurazione del client, o le regole del firewall. Fuori dalla casella, il risolutore del DNS gestisce le query DNS per i client dietro il firewall. Se i PC client sono configurati con DHCP, riceveranno l'indirizzo IP dell'interfaccia firewall a cui sono collegati come server DNS, a meno che questo non venga modificato manualmente. Per esempio, se un PC è sull'interfaccia LAN, e l'indirizzo IP della LAN del firewall è 192.168.1.1, allora il server DNS del client dovrebbe essere anche 192.168.1.1. Se il risolutore DNS e il DNS Forwarder sono disattivati, regolare i server DNS che vengono assegnati ai client DHCP sotto **Servizi>Server DHCP Server**. quando i risolutori DNS e i DNS Forwarder sono disabilitati, i server DNS di sistema vengono assegnati direttamente ai client, ma se questo non è il caso in oggetto per questa impostazione, definirli nelle impostazioni DHCP. Se il PC client non è configurato per DHCP, accertati che abbia il server DNS corretto: o l'indirizzo IP della LAN del firewall Firew4LL o un gruppo alternativo di server DNS interni o esterni.

Un'altra possibilità per il DNS di lavorare dal firewall Firew4LL ma non da un client locale è una regola firewall troppo rigida sulla LAN. Controllare **Stato>Registri di sistema**, nella scheda **Firewall**. Se le connessioni bloccate appaiono nel registro dal client locale che cerchi di raggiungere un server DNS, allora aggiungere una regola firewall nella parte superiore delle regole LAN per tale interfaccia che consentirà le connessioni ai server DNS sulla **porta TCP e UDP 53**.

Problemi con il gateway del client

Affinché un firewall Firew4LL instradi correttamente il traffico Internet per i PC client, esso deve avere il proprio gateway. Se i PC client sono configurati utilizzando il server DHCP integrato nei firewall Firew4LL, questo verrà impostato automaticamente. Tuttavia, se i client ricevono informazioni DHCP da un server DHCP alternativo, o se i loro indirizzi IP sono stati inseriti manualmente, controllare due volte che il loro gateway sia impostato per l'indirizzo IP dell'interfaccia a cui si collegano sul firewall Firew4LL. Ad esempio, se i client sono sull'interfaccia LAN Firew4LL e l'indirizzo IP per l'interfaccia LAN è 192.168.1.1, l'indirizzo del gateway sui PC client deve essere impostato su 192.168.1.1.

Problemi Regole Firewall

Se la regola di default «LAN verso tutti» è stata modificata o rimossa dall'interfaccia LAN, il traffico che tenta di raggiungere Internet dai PC client tramite il firewall Firew4LL può essere bloccato. Questo è facilmente confermato raggiungendo **Stato>Registro di sistema** e guardando la scheda del **Firewall**. Se ci sono voci che mostrano connessioni bloccate dai PC della LAN che tentano di raggiungere gli host di Internet, rivisitare il gruppo di regole della LAN in **Firewall > Regole**, sulla scheda **LAN** per effettuare le modifiche necessarie per consentire tale traffico. Consultare *Firewall* per informazioni più dettagliate sulla modifica o la creazione di regole aggiuntive.

Se funziona dal lato LAN ma non da un'interfaccia OPT, assicurati che il firewall abbia delle regole per permettere al traffico di passare. Le regole non vengono create come predefinite sulle interfacce OPT.

Problemi Regole NAT

Se le norme NAT in uscita sono state modificate rispetto alle loro impostazioni predefinite, il traffico che tenta di raggiungere Internet potrebbe non avere un NAT correttamente applicato. Passare alla scheda **Firewall>NAT, in uscita**. Nella maggior parte dei casi l'impostazione dovrebbe essere sulla **Generazione automatica delle regole NAT in uscita**. Se non c'è, cambiare tale impostazione, Fare clic su **Salvare** e **Applicare modifiche,** e quindi cercare di raggiungere di nuovo Internet da un PC client. Se questo non ha aiutato ad un uscire un PC sulla LAN, allora il problema è probabilmente altrove.

Se il NAT in uscita è impostato su **Generazione di una regola NAT in uscita manuale** e l'accesso a Internet funziona da LAN ma non da un'interfaccia OPT, aggiungere manualmente le regole che corrispondono al traffico proveniente dall'interfaccia OPT. Consultare le norme esistenti per la LAN e adattarle di conseguenza, o fare riferimento al *NAT in uscita* per ulteriori informazioni sulla creazione di regole NAT in uscita.

Lo stesso vale per il traffico proveniente da utenti VPN: OpenVPN, IPsec, ecc. Se questi utenti hanno bisogno di raggiungere Internet tramite questo firewall Firew4LL, avranno bisogno di regole NAT in uscita per le loro sottoreti. Vedere *NAT in uscita* per maggiori informazioni.

7.10 File di configurazione XML di Firew4LL

I firewall di Firew4LL memorizzano tutte le loro impostazioni in un file di configurazione in formato XML. Tutte le impostazioni di configurazione, comprese le impostazioni per i pacchetti, sono contenute in questo file. Tutti gli altri file di configurazione per i servizi e il comportamento del sistema vengono generati dinamicamente al momento dell'esecuzione in base alle impostazioni contenute nel file di configurazione XML.

Coloro che hanno familiarità con FreeBSD e i sistemi operativi correlati l'hanno scoperto nel modo più duro, quando le loro modifiche ai file di configurazione di sistema sono state ripetutamente sovrascritte dal firewall prima di arrivare a capire che Firew4LL gestisce tutto automaticamente.

La maggior parte delle persone non avrà mai bisogno di sapere dove risiede il file di configurazione, ma per riferimento è in /cf/conf/ config.xml. Tipicamente, /conf/ è un collegamento simbolico a /cf/conf, quindi può anche essere accessibile direttamente da /conf/ config.xml, ma questo varia in base al layout della piattaforma e del filesystem.

7.10.1 Modifica manuale della configurazione

Alcune opzioni di configurazione sono disponibili solo modificando manualmente il file di configurazione, anche se questo non è richiesto nella stragrande maggioranza delle distribuzioni. Alcune di queste opzioni sono coperte in altre parti di questa guida.

> **Avvertimento:** Attenzione: Anche per gli amministratori esperti è facile modificare erroneamente il file di configurazione. Tenere sempre i backup ed essere consapevoli che la rottura della configurazione si tradurrà in conseguenze indesiderate.

Il metodo più semplice e sicuro per modificare il file di configurazione è quello di fare un backup da **Diagnostica>Backup/ Ripristino**, salvare il file su un PC, modificare il file e apportare le modifiche necessarie, quindi ripristinare il file di configurazione modificato nel firewall. Utilizzare un editor che comprenda correttamente le terminazioni di linea UNIX, e preferibilmente un editor che abbia una gestione speciale per XML come l'evidenziazione della sintassi. Non usare notepad.exe su Windows.

Per gli amministratori che hanno familiarità con l'editor vi, il comando viconfig modificherà la configurazione in esecuzione dal vivo, e dopo aver salvato e lasciato l'editor, il firewall rimuoverà la configurazione cache da /tmp/config.cache e le modifiche saranno visibili nella GUI. Le modifiche non saranno attive fino al prossimo riavvio/ricarica del servizio relativo alla parte modificata della configurazione.

7.11 Cosa fare quando si è bloccati fuori dalla WebGUI

In alcune circostanze un amministratore può essere bloccato fuori dalla WebGUI. Non abbiate paura se questo accade; ci sono un certo numero di modi per riprendere il controllo. Alcuni metodi sono un po" complicati, ma è quasi sempre possibile recuperare l'accesso. Gli scenari peggiori richiedono l'accesso fisico, come chiunque con accesso fisico può bypassare misure di sicurezza.

Avvertimento: Attenzione: Che le tattiche di questa sezione siano una lezione. La sicurezza fisica di un firewall è fondamentale, soprattutto in ambienti in cui il firewall è fisicamente situato in un'area comune e accessibile a persone diverse dagli amministratori autorizzati.

Prima di intraprendere qualsiasi di questi passaggi, provare le credenziali predefinite:

Nome utente: admin

Parola d'ordine: firew4ll

7.11.1 Password dimenticata

La password dell'amministratore del firewall può essere facilmente reimpostata usando la console del firewall se è stata persa. Accedere alla console fisica (Seriale o Tastiera/Monitor) e utilizzare l'opzione 3 per ripristinare la password WebGUI. Questa opzione può anche ripristinare l'account admin se è stato disabilitato o scaduto.

Dopo aver reimpostato la password, l'utente amministratore può effettuare il login con la password predefinita Firew4LL.

7.11.2 Password dimenticata con console bloccata

Se la console è protetta da password, non tutto è perduto. Ci vogliono due riavvii da realizzare, ma la password può essere resettata con un accesso fisico alla console:

- Riavviare il firewall Firew4LL
- Scegliere l'opzione di avvio singolo utente (2) dal menu loader (quello con il logo ASCII Firew4LL)
- Premere Invio quando richiesto per avviare /bin/sh
- Rimozione di tutte le partizioni come riscrivibili

```
# /sbin/mount -a -t ufs
```

- Eseguire il comando integrato di reimpostazione della password:

```
# /etc/rc.initial.password
```

- Seguire le istruzioni per reimpostare la password
- Riavviare

Al riavvio del firewall, l'utente amministratore può effettuare il login con la password predefinita Firew4LL.

7.11.3 Confusione HTTP contro HTTPS

Assicurarsi che il client si connette con il protocollo corretto, HTTP o HTTPS. Se uno non funziona, provare l'altra. Se l'interfaccia grafica non è stato configurato correttamente, il firewall può essere in esecuzione l'interfaccia grafica su una combinazione di porta e protocollo di inaspettato, come ad esempio:

- http://firew4llhostname:443
- https://firew4llhostname:80

Per reimpostarlo dalla console, reimpostare l'indirizzo IP dell'interfaccia LAN, inserire lo stesso indirizzo IP, e lo script chiederà di ripristinare la WebGUI su HTTP.

7.11.4 Accesso bloccato con regole firewall

Se un amministratore remoto perde l'accesso alla WebGUI a causa di una modifica delle regole del firewall, allora l'accesso può ancora essere ottenuto dal lato LAN. Le regole LAN non possono impedire l'accesso alla GUI a meno che la regola anti-blocco non sia disabilitata. La regola anti-blocco assicura che gli host sulla LAN siano in grado di accedere alla WebGUI in ogni momento, indipendentemente dalle altre regole del blocco dell'interfaccia LAN.

Dover portare a spasso qualcuno sul posto attraverso la correzione della regola dalla LAN è meglio che perdere tutto o dover fare un viaggio nella posizione del firewall!

7.11.5 Aggirare da remoto il blocco Firewall con le regole

Ci sono alcuni modi per manipolare il comportamento del firewall nella shell per riguadagnare l'accesso alla GUI del firewall. Le seguenti tattiche sono elencate in ordine di facilità e di quanto impatto abbiano sul sistema in esecuzione.

Aggiungere una regola con EasyRule

Il modo più semplice, assumendo che l'amministratore conosca l'indirizzo IP di un PC client remoto che ha bisogno di accesso, è quello di utilizzare lo script shell easyrule per aggiungere una nuova regola firewall. Nell'esempio seguente, lo script easyrule permetterà l'accesso all'interfaccia WAN, da x.x.x.x (l'indirizzo IP del client) a y.y.y.y (presumibilmente l'indirizzo IP WAN) sulla porta TCP 443:

```
# easyrule pass wan tcp x.x.x.x y.y.y.y 443
```

Una volta che lo script easyrule aggiunge la regola, il client sarà in grado di accedere alla GUI dall'indirizzo di origine specificato.

Aggiungere una regola "consentire a tutti" sulla WAN dalla shell

Un'altra tattica consiste nell'attivare temporaneamente una regola "consentire a tutti" sulla WAN per lasciare dentro un client.

Avvertimento: Attenzione: Un regola tipo "consentire a tutti" è pericolosa da avere su un'interfaccia WAN collegata a Internet. Non dimenticare di rimuovere la regola una volta aggiunta da questo script

Per aggiungere una regola "consentire a tutti" all'interfaccia WAN, eseguire il seguente comando al prompt della shell:

```
# pfSsh.php playback enableallowallwan
```

Una volta che l'amministratore riprende l'accesso e risolve il problema originale impedendo loro di raggiungere la GUI, rimuovere la «regola consentire tutti» sulla WAN.

Disattivare il firewall

Un amministratore può (solo temporaneamente) disattivare le regole del firewall disattivare la console fisica o SSH.

> **Avvertimento:** Attenzione: Questo disabilita completamente pf che disabilita le regole del firewall e del NAT. Se la rete gestita da questo firewall si basa sul NAT per funzionare, cosa che la maggior parte fanno, allora l'esecuzione di questo comando interromperà la connettività dalla LAN a Internet.

Per disabilitare il firewall, collegarsi alla console fisica o SSH ed utilizzare l'opzione 8 per avviare una shell e digitare:

```
# pfctl -d
```

Questo comando disabiliterà il firewall, comprese tutte le funzioni NAT. L'accesso alla WebGUI è ora possibile da qualsiasi luogo, almeno per pochi minuti o fino a quando un processo sul firewall conceda allo schema di regole ia ricaricarsi (che è quasi ogni pagina da salvare o l'azione **Applicare le modifiche**). Una volta che l'amministratore ha regolato le regole e recuperato l'accesso necessario, riattivare il firewall digitando:

```
# pfctl -e
```

Modifica manuale dello schema delle regole

L'insieme di regole caricato viene mantenuto in /tmp/rules.debug. Se l'amministratore ha familiarità con la sintassi PF, può modificare il file per risolvere il problema della connettività e ricaricare le regole:

```
# Pfctl -f /tmp/rules.debug
```

Dopo essere rientrato nella WebGUI con quella correzione temporanea, l'amministratore deve eseguire qualsiasi lavoro è necessario nella WebGUI per rendere la correzione permanente. Quando le regole vengono salvate nella WebGUI, la modifica temporanea in /tmp/ rules.debug verrà sovrascritta.

7.11.6 Per aggirare da remoto il blocco Firewall con Tunneling SSH

Se l'accesso remoto alla WebGUI è bloccato dal firewall, ma l'accesso SSH è permesso, allora c'è un modo relativamente facile per entrare: il Tunneling SSH.

Se la WebGUI è sulla porta 80, impostare il client SSH per inoltrare la porta locale 443 (o 4443, o un'altra porta) alla porta remota localhost:443. Se la WebGUI del firewall è su un'altra porta, usare quella come destinazione. Poi puntare il browser su https://localhost. Aggiungere la porta alla fine dell'URL se differisce dal predefinito 443, per esempio https://localhost:4443. Se la GUI sta usando HTTP, cambiare il protocollo sull'URL in http://.

Compilare le opzioni come mostrato in Figura *Impostazione del Tunnel SSH con porta 80 in PuTTY*, quindi fare clic su Aggiungere.

Una volta che il client si connette e si autentica, la WebGUI è accessibile dalla porta locale reindirizzata.

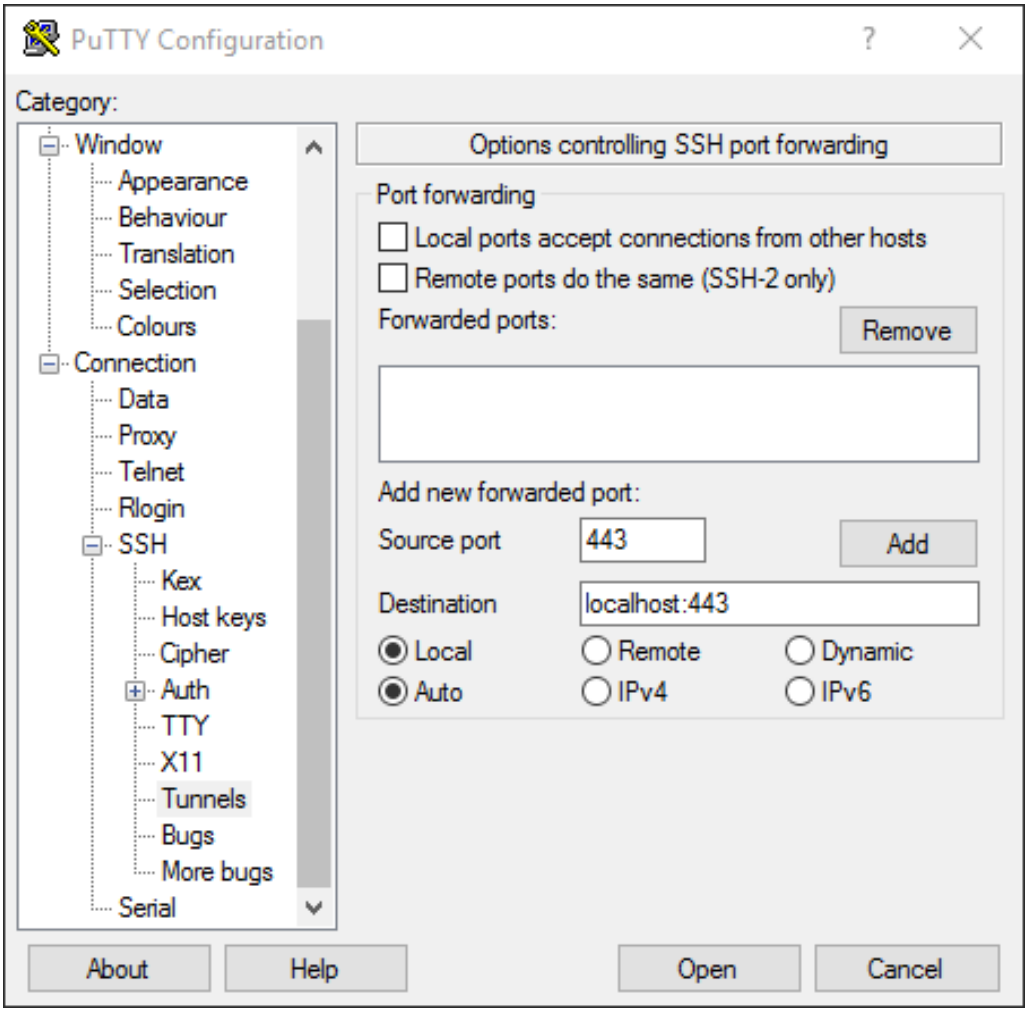


Fig. 16: Impostazione del Tunnel SSH con porta 80 in PuTTY

7.11.7 Bloccato fuori a causa di un errore della configurazione Squid

Se un amministratore del firewall configura accidentalmente lo Squid per usare la stessa porta della WebGUI, può causare una condizione di gara per il controllo della porta, a seconda di quale servizio (ri)iniziare in un momento particolare. Se Squid riesce ad ottenere il controllo della porta desiderata dalla WebGUI, allora la WebGUI non sarà accessibile per correggere la configurazione.

La seguente procedura può aiutare a riprenderne il controllo.

- Connettersi alla console del firewall di Firew4LL con SSH o accesso fisico
- Avviare una shell, opzione 8 dalla console.
- Terminae il processo di squid:

```
# /usr/local/etc/rc.d/squid.sh stop
```

Se questo non funziona, provare questo comando:

```
# killall -9 squid
```

o:

```
# squid -k shutdown
```

Una volta che il processo squid è completamente terminato, utilizzare l'opzione del menu della console 11 per riavviare il processo WebGUI, e quindi tentare di accedere nuovamente alla WebGUI.

Nota: Lavorare rapidamente o ripetere il comando di spegnimento, perché lo squid può essere riavviato automaticamente dai suoi script di monitoraggio interni a seconda del metodo utilizzato per fermare il processo

---

La maggior parte della configurazione di Firew4LL viene eseguita usando il configuratore GUI basato sul web (configuratore we), o WebGUI in breve. Ci sono alcuni compiti che possono essere eseguiti anche dalla console, sia che si tratti di un monitor e una tastiera, una porta seriale, o tramite SSH.

7.12 Collegamento al WebGUI

Per raggiungere la WebGUI, connettersi con un browser web da un computer collegato alla LAN. Questo computer può essere collegato direttamente con un cavo di rete o allo stesso interruttore dell'interfaccia LAN del firewall. Per default, l'indirizzo IP della LAN di un nuovo sistema Firew4LL è 192.168.1.1 con una maschera /24 (255.255.255.0), e c'è anche un server DHCP in esecuzione. Se il computer è impostato per utilizzare DHCP, dovrebbe ottenere un indirizzo nella sottorete LAN automaticamente. Quindi aprire un browser e raggiungere https://192.168.1.1

Avvertimento: Avvertimento: Se la sottorete LAN predefinita entra in conflitto con la sottorete WAN, la sottorete LAN deve essere modificata prima di collegarla al resto della rete.

L'indirizzo IP della LAN può essere cambiato e DHCP può essere disabilitato utilizzando la console:

- Aprire la console (VGA, seriale o usando SSH da un'altra interfaccia)
- Scegliere l'opzione 2 dal menu della console
- Inserire il nuovo indirizzo indirizzo IP sulla LAN, la maschera di sottorete, e specificare se attivare o meno il DHCP.
- Inserire l'indirizzo iniziale e finale del pool DHCP se DHCP è attivato. Questo può essere qualsiasi intervallo all'interno del data sottorete.

Nota: Quando si assegna un nuovo indirizzo IP per la LAN, non può essere nella stessa sottorete del WAN o qualsiasi altra interfaccia attiva. Se ci sono altri dispositivi già presenti sulla sottorete LAN, può anche non essere impostato per lo stesso indirizzo IP di un host esistente.

Se il server DHCP è disabilitato, i computer client su LAN deve avere un indirizzo IP nella sottorete Firew4LL della LAN configurato in modo statico, come ad esempio 192.168.1.5, con una maschera di sottorete che corrisponda a quello dato a Firew4LL, come ad esempio 255.255. 255.0.

Una volta che il computer è connesso alla stessa LAN di Firew4LL, individuare l'indirizzo IP della LAN del firewall. La GUI è in ascolto su HTTPS per impostazione predefinita, ma se il browser tenta di connettersi tramite HTTP, sarà reindirizzato invece dal firewall alla porta HTTPS. Per accedere alla GUI direttamente senza il reindirizzamento, usare: https://192.168.1.1

Quando si carica la WebGUI, i firewall presenta prima una pagina di login. In questa pagina, inserire le credenziali di default:

nome utente: admin

parola d'ordine: firew4ll

CAPITOLO 8

Interfacce e configurazione

8.1 Gruppo di interfacce

A differenza delle altre interfacce di questo capitolo, un gruppo di interfacce non è un tipo di interfaccia che può essere assegnato. I gruppi di interfacce sono utilizzati per applicare regole di firewall o NAT per un insieme di interfacce su una scheda comune. Se questo concetto è poco familiare, bisogna considerare come le regole del firewall per OpenVPN, il server PPPoE, o L2TP lavorano sul server. Ci sono più interfacce del sistema operativo sottostante, ma le regole per tutte loro sono gestite su una singola scheda per ogni tipo. Se molte interfacce di una funzione analoga sono presenti sul firewall e necessitano di regole praticamente identiche, un gruppo di interfacce può essere creato per aggiungere regole per tutte le interfacce allo stesso tempo. Le interfacce possono ancora avere le proprie regole individuali, che vengono elaborate dopo le regole del gruppo.

Per creare un gruppo di interfacce:

- raggiungere a **Interfacce>(Assegnare)**, scheda **Gruppi di interfaccia**
- Fare clic su  **Aggiungere** per creare un nuovo gruppo
- Inserire un **Nome del gruppo**. Questo nome può contenere solo lettere maiuscole e minuscole, numeri, spazi o caratteri speciali
- Inserire una **Descrizione del gruppo** (opzionale)
- Aggiungere interfacce come **Membri del gruppo** con Ctrl-clic per selezionare le voci dalla lista di interfacce
- Fare clic su **Salvare**

I gruppi di interfacce hanno ciascuno una singola scheda sotto **Firewall>Regole** per gestire le loro regole. La figura *Scheda di tutte le regole del firewall per il gruppo di interfacce* mostra la scheda delle regole del firewall per il gruppo definito nella figura *Aggiungere un gruppo di interfacce*

Vedi anche:

Configurazione delle regole del firewall* , per informazioni sulla gestione delle regole del firewall.

8.1.1 Ordine di elaborazione del gruppo di regole

L'ordine di elaborazione delle regole per un utente è:

- regole galleggianti
- regole del gruppo di interfacce
- regole riferite alla singola interfaccia

Ad esempio, se una regola nella scheda gruppo corrisponde a un collegamento, non verranno consultate le regole della scheda di interfaccia. Allo stesso modo, se una regola galleggiante con Quick Set è abbinata una connessione, non verranno consultate le regole del gruppo di interfaccia.

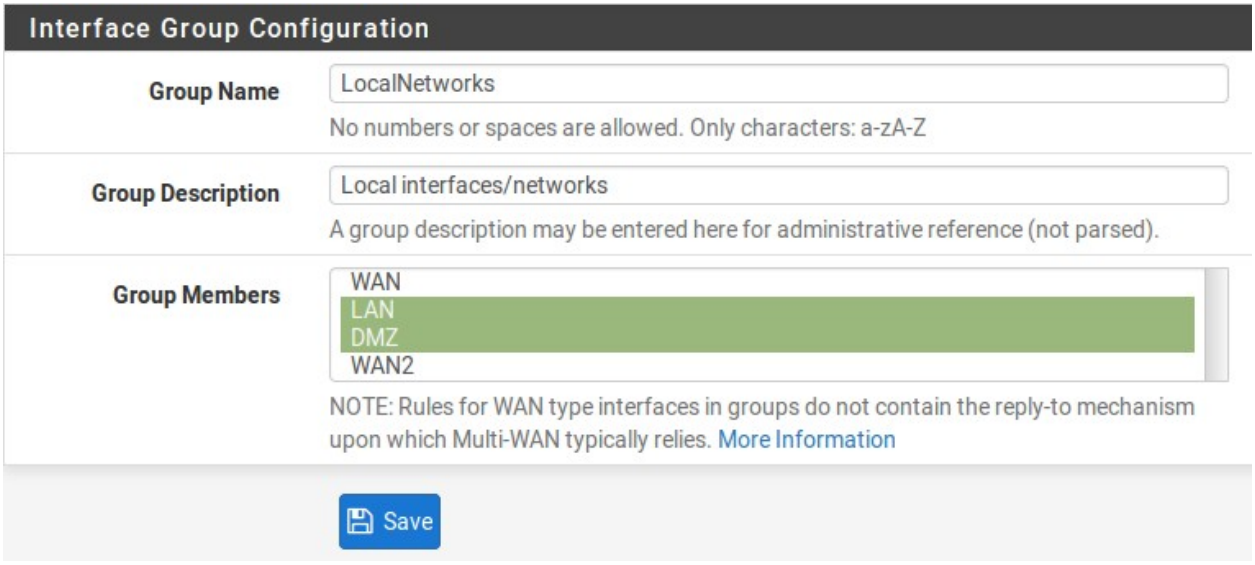


Fig. 1: Aggiungere un gruppo di interfacce

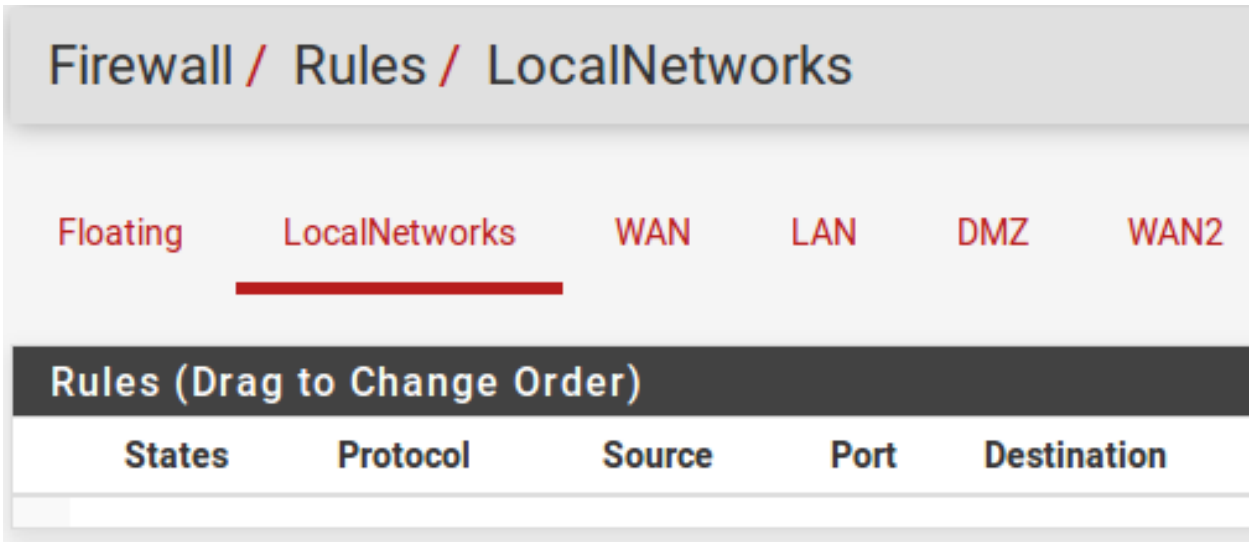


Fig. 2: Scheda di tutte le regole del firewall per il gruppo di interfacce

L'ordine di elaborazione impedisce una combinazione di regole che altrimenti potrebbe essere una buona misura. Ad esempio, se una regola generale di blocco è presente sul gruppo, può non essere sovrascritta da una regola su un'interfaccia specifica. Stessa cosa con una regola di passaggio, una norma specifica per l'interfaccia non può bloccare il traffico trasmesso da una regola della scheda di gruppo.

8.1.2 Uso con interfacce WAN

È sconsigliato l'utilizzo di gruppi di interfacce con più reti WAN. Ciò potrebbe sembrare conveniente, ma le regole del gruppo non ricevono lo stesso trattamento delle regole della scheda WAN. Ad esempio, le regole su una scheda per l'interfaccia di tipo WAN (Gateway selezionato sulla configurazione dell'interfaccia) riceveranno un reply-to che permette a pf rimandare il traffico di ritorno attraverso l'interfaccia da cui è entrato. Le regole della scheda di gruppo non ricevono una reply-to che di fatto significa che le regole del gruppo solo funzionano come previsto sulla WAN con il gateway predefinito.

8.2 Wireless

La scheda Wireless sotto **Interfacce>(assegnare)** è per la creazione e la gestione di interfacce aggiuntive virtuali del punto di accesso virtuale (VAP). Utilizzando VAP si consente a più reti con wireless SSID unici di essere eseguite fuori una singola scheda, se questa funzione è supportata dal driver e l'hardware in uso. Un VAP viene creato sulla scheda Wireless, quindi assegnato sulla scheda delle interfacce. Informazioni approfondite su questa funzione possono essere trovate in *wireless*.

8.3 VLAN

Le interfacce contrassegnate con VLAN, o 802.1Q, si trovano nella scheda **VLAN** sotto **Interfacce>(assignare).** Le istanze VLAN permettono al sistema di gestire il traffico contrassegnato da un interruttore 802.1Q compatibile separatamente come se ogni tag fosse una interfaccia distinta. Su questa scheda viene creata una VLAN, poi assegnata nella scheda **Assegnazioni interfaccia**. Informazioni approfondite su questa funzionalità si possono trovare nelle *LAN virtuali (VLANs).*

8.4 QinQ

La scheda QinQ sotto **Interfacce>(assignare)** permette di creare un'interfaccia compatibile 802.1ad, nota anche come *VLAN fornite*. Questa funzione consente di contenere più tag VLAN in un unico pacchetto. Questo può aiutare a trasportare il traffico contrassegnato con VLAN per altre reti attraverso una rete intermedia utilizzando un tag diverso o sovrapponendolo. Informazioni approfondite su questa funzionalità possono essere trovate in *Configurazione di QinQ di \firew4ll*.

8.5 Bridge

Bridge di interfaccia, o più interfacce legate insieme in un dominio di broadcast con livello condiviso 2, vengono creati e gestiti sulla scheda **Bridge** in **Interfacce>(assegnare).** Maggiori informazioni sui bridge, compreso come crearli e gestirli, è in *Bridging*.

8.6 OpenVPN

Dopo la creazione di un'istanza OpenVPN, può essere assegnata in Interfacce>(assegnare). Assegnare un'interfaccia OpenVPN

Vedi anche:

Assegnazione delle interfacce OpenVPN per maggiori informazioni.

8.7 PPP

Ci sono quattro tipi di interfacce PPP:

- **PPP** semplice per 3G/4G e dispositivi modem
- **PPPoE** per le connessioni DSL o simili
- **PPTP** e **L2TP** per gli ISP che li richiedono per l'autenticazione.

Nella maggior parte di questi casi sono gestiti direttamente dalle impostazioni di interfaccia, ma possono anche essere modificati sotto **Interfacce>(assegnare)** nella scheda **PPP**.

8.7.1 PPP con Multi-Link (MLPPP)

La modifica di un'istanza PPP consente che PPP con Multi-Link (MLPPP) siano configurati per i fornitori supportati. MLPPP uniscono collegamenti PPP multipli in un singolo canale aggregato più grande. A differenza di altre tecniche di multi-WAN, con MLPPP è possibile utilizzare l'intera banda di tutti i collegamenti per una singola connessione, e non si causano le solite preoccupazioni sul bilanciamento del carico e sul failover. Il collegamento MLPPP è presentato come un'interfaccia con un indirizzo IP, e se un collegamento non riesce, la connessione funziona lo stesso ma con capacità ridotta.

Suggerimento: Per maggiori informazioni su MLPPP, vedere *Collegamenti di multiple WAN*.

8.7.2 Tipi di interfaccia PPP (Protocollo Point-to-Point)

Aggiungere o modificare una voce PPP come segue:

- Individuare **Interfacce>(assegnare)** nella scheda **PPP**
- Fare clic su  per modificare una voce esistente o su  per aggiungere una nuova voce
- Impostare il tipo di collegamento, che cambia le opzioni rimanenti sulla pagina. I tipi di collegamento sono spiegati in tutto il resto di questa sezione.

PPP (3G/4G, Modem)

Il tipo di collegamento **PPP** viene utilizzato per parlare con un modem su un dispositivo seriale. Questo può essere qualsiasi cosa da un dongle USB 3G/4G per accedere a una rete cellulare a un vecchio modem hardware per l'accesso dial-up. Selezionando il tipo di collegamento PPP, l'elenco delle **Interfacce del Link** viene compilato con dispositivi seriali che possono essere utilizzati per comunicare con un modem. Fare clic su una voce specifica per selezionarla per l'uso. Dopo aver selezionato l'interfaccia, facoltativamente, immettere una **Descrizione** per la voce PPP.

Nota: Il dispositivo seriale per un modem non viene rilevato

automaticamente. Alcuni modem si presentano come diversi dispositivi, e il dispositivo dipendente per la linea PPP può essere una delle scelte disponibili, ma iniziare con l'ultimo dispositivo, quindi provare il primo, e poi altri in mezzo se nessuno funziona.

Quando si configura una rete 3G/4G, le opzioni per il **Provider del servizio** di riempire prima altri campi pertinenti sulla pagina.

- Scegliere un **Paese**, come ad esempio Stati Uniti, per attivare l'elenco a discesa dei **Provider** con i fornitori di cellulari noti in quel paese
- Selezionare un **provider** dalla lista, come ad esempio *T-Mobile*, per attivare l'elenco a discesa del **Piano**.
- Selezionare un **Piano** e i campi rimanenti saranno riempiti con i valori noti per il **Provider** e il **Piano**

  Le opzioni del **Provider del servizio** possono essere configurate manualmente se sono necessari altri valori, o quando si utilizza un provider che non è elencato:

  Nome utente e password Le credenziali utilizzate per l'accesso PPP.

  Numero di telefono Il numero da comporre sul provider di servizi Internet per guadagnare l'accesso. Per 3G/4G questo tende ad essere un numero, ad esempio 99# o # 777, e per la connessione dial-up questo è di solito un numero di telefono tradizionale.

  Nome per il punto d'accesso (APN) Questo campo è richiesto da alcuni ISP per identificare il servizio a cui si connette il client. Alcuni provider usano questo per distinguere tra piani consumer e business, o reti legacy.

  Numero APN Impostazione opzionale. Il valore predefinito è 1 se l'APN è impostato, é ignorato quando APN è disinserito.

  PIN della SIM Codice di sicurezza sulla SIM per impedire l'uso non autorizzato della carta. Non inserire nulla qui se la SIM non dispone di un codice PIN.

  Attesa del PIN della SIM Numero di secondi di attesa per la SIM alla scoperta della rete dopo che il PIN viene inviato nella SIM. Se il ritardo non è abbastanza lungo, la SIM non può avere il tempo di inizializzare correttamente dopo lo sblocco.

  Stringa di inizializzazione La stringa di inizializzazione del modem, se necessaria. Non includere AT all'inizio del comando. La maggior parte dei modem moderni non richiedono una stringa di inizializzazione personalizzata.

  Connessione finita Il tempo di attesa di un tentativo di connessione per avere successo, di pochi secondi. Il valore predefinito è 45 secondi.

  Registrazione in tempo Se selezionata, il tempo di disponibilità della connessione viene monitorato e visualizzato sullo **Stato> Interfacce**.

PPPoE (Protocollo Point-to-Point Protocol su Ethernet)

PPPoE è un metodo popolare di autenticazione e accesso ad una rete ISP, più comunemente riscontrato sulle reti DSL.

Per configurare un collegamento PPPoE, iniziare impostando il **Tipo di collegamento** a PPPoE e completare il resto delle impostazioni come segue:

Interfaccia (interfacce) del Link Una lista di interfacce di rete che possono essere utilizzate per PPPoE. Queste sono di solito interfacce fisiche ma può anche funzionare su alcuni altri tipi di interfaccia come le VLAN. Selezionarne una per il normale PPPoE, o multipla per MLPPP.

Descrizione Una descrizione facoltativa della voce PPP

Nome utente e password Le credenziali per questo circuito PPPoE. Questi saranno forniti dall'ISP, e il nome utente è in genere sotto forma di un indirizzo di posta elettronica, come ad esempio miaazienda@ispesempio.com.

Nome di servizio lasciato vuoto per la maggior parte dei fornitori di servizi Internet, alcuni lo richiedono impostato su un valore specifico. Contattare l'ISP per confermare il valore se la connessione non funziona quando è lasciato vuoto.

Configurare il nome di servizio NULL Alcuni ISP richiedono che NULL essere inviato al posto di un nome di servizio vuoto. Selezionare questa opzione quando l'ISP considera questo comportamento necessario.

Ripristino periodico Configura un tempo prestabilito, quando la connessione verrà interrotta e riavviata. Questo è raramente necessario, ma in certi casi può meglio gestire riconnessioni quando un ISP è costretto a riconnettersi quotidianamente o a comportamenti inusuali simili.

PPTP (Protocollo di tunneling con Point-to-Point)

Da non confondere con una VPN PPTP, questo tipo di interfaccia PPTP è destinato a connettersi a un ISP e autenticarsi, più o meno lo stesso come funziona PPPoE. Le opzioni per una WAN PPTP sono identiche alle opzioni PPPoE dello stesso nome. Fare riferimento alla sezione precedente per informazioni sulla configurazione.

(Protocollo di tunneling di livello 2)

L2TP, come è configurato qui, è usato per connettersi ad un ISP che lo richiede per l'autenticazione come tipo di WAN. L2TP funziona in modo identico a PPTP. Fare riferimento alle sezioni precedenti per informazioni sulla configurazione.

8.7.3 Opzioni avanzate PPP

Tutti i tipi di PPP hanno diverse opzioni avanzate in comune che possono essere modificate nelle loro voci qui. Nella maggior parte dei casi queste impostazioni non devono essere modificate. Per visualizzare queste opzioni, fare clic su  **Visualizzare avanzate**.

Chiamata su richiesta Il comportamento predefinito per un collegamento PPP è quello di connettersi immediatamente e si cercherà immediatamente di riconnettersi quando un collegamento viene perso. Questo comportamento è descritto come **Sempre On**. La **Chiamata su richiesta** ritarderà questo tentativo di connessione. Quando è impostato, il firewall aspetterà che un pacchetto tenti di uscire da questa interfaccia, e poi si connetterà. Una volta collegato, non si disconnetterà automaticamente.

Timeout di inattività Una connessione PPP sarà mantenuta aperta indefinitamente per impostazione predefinita. Un valore in **Timeout di inattività**, specificato in secondi, farà sì che il firewall controlli la linea per l'attività. Se non c'è traffico sul collegamento per il tempo dato, il collegamento sarà scollegato. Se è stata impostata anche la **Chiamata su richiesta**, il firewall tornerà alla modalità chiamata su richiesta.

Nota: Firew4LL eseguirà per default il monitoraggio del gateway, chegenereràgenererà due ping ICMP al secondo sull'interfaccia. Il Timeout inattivo non funzionerà in questo caso. Questo può essere risolto modificando il gateway per questo link PPP, e selezionando **Disabilitare il monitoraggio del gateway**.

Compressione (vjcomp) Questa opzione controlla se verrà utilizzata o meno la compressione dell'intestazione TCP di Van Jacobson. Per impostazione predefinita sarà negoziato con il peer durante l'accesso, quindi se entrambi i lati supportano la funzionalità, verrà utilizzato. La spunta **Disabilitare vjcomp** farà sì che la funzionalità sia sempre disabilitata. Di solito questa caratteristica è vantaggiosa perché salva diversi byte per ogni pacchetto di dati TCP. L'opzione dovrebbe quasi sempre rimanere abilitata. Questa

compressione è inefficace per le connessioni TCP con le estensioni moderne abilitate come con la stampa dell'orario o SACK, che modificano le opzioni TCP tra pacchetti sequenziali.

Fissaggio MSS dei TCP L'opzione tcpmssfix fa sì che il daemon PPP regoli i segmenti TCP SYN in entrata e in uscita in modo che la dimensione massima del segmento richiesta (MSS) non sia superiore alla quantità consentita dall'interfaccia MTU. Questo è necessario nella maggior parte dei casi per evitare problemi causati da router che rilasciano messaggi ICMP come «Dati troppo grandi». Senza questi messaggi, la macchina di origine invia dati, supera il router rouge poi colpisce una macchina che ha un MTU che non è abbastanza grande per i dati. Poiché l'opzione IP «Non frammentare» è impostata, questa macchina invia un messaggio ICMP «Dati troppo grandi» all'origine e fa cadere il pacchetto. Il router rouge rilascia il messaggio ICMP e l'origine non riesce mai a scoprire che deve ridurre la dimensione del frammento o eliminare l'opzione IP "Non frammentare" dai suoi dati in uscita. Se questo comportamento non è desiderabile, controllare **Disabilita tcpmssfix**.

Nota: I valori MTU e MSS per l'interfaccia possono essere regolati anche nella pagina di configurazione dell'interfaccia sotto il menu **Interfacce**, come le **interfacce> WAN.**

Sequenza breve (ShortSeq) Questa opzione è significativa solo se MLPPP è negoziata. Proibisce intestazioni di frammento multi-link più corte, salvando due byte su ogni fotogramma. Non è necessario disabilitarla per connessioni che non sono multi-link. Se MLPPP è attivo e questa funzionalità deve essere disabilitata, controllare **Disabilitare sequenze brevi**.

Compressione del campo di controllo dell'indirizzo (AFCComp) Questa opzione si applica solo ai tipi di link asincroni. Salva due byte per fotogramma. Per disabilitarlo, controllare **Disabilitare la compressione ACF**.

Compressione dei campi del protocollo (ProtoComp) Questa opzione salva un byte per fotogramma per la maggior parte dei fotogrammi. Per disabilitarla, controllare Disabilitare **la compressione del protocollo.**

8.8 GRE (Incapsulamento del routing generico)

L'incapsulamento del routing generico (GRE) è un metodo di tunneling del traffico tra due endpoint senza crittografia. Può essere utilizzato per instradare pacchetti tra due posizioni che non sono direttamente collegati, che non richiedono crittografia. Può anche essere combinato con un metodo di crittografia che non esegue il proprio tunneling. L'IPsec in modalità di trasporto può utilizzare GRE per il tunneling del traffico criptato in modo che consenta il routing tradizionale o l'uso di protocolli di routing. Il protocollo GRE è stato originariamente progettato da Cisco, ed è la modalità di tunneling predefinita su molti dei loro dispositivi.

Come creare o gestire un'interfaccia GRE:

- Individuare **Interfacce>(assegnare),** scheda GRE
- Fare clic su  **Aggiungere** per creare una nuova istanza GRE, oppure fare clic su  per modificare un'interfaccia esistente.
- Completare le impostazioni come segue:

  Interfaccia primaria L'interfaccia su cui il tunnel GRE terminerà. Spesso questa sarà uns WAN o una connessione di tipo WAN.

  Indirizzo remoto GRE L'indirizzo del peer remoto. Questo è l'indirizzo a cui i pacchetti GRE saranno trasmessi da questo firewall; l'indirizzo esterno instradabile all'altra estremità del tunnel.

indirizzo locale del tunnel GRE L'indirizzo interno per la fine del tunnel su questo firewall. Il firewall utilizzerà questo indirizzo per il proprio traffico nel tunnel, e traffico remoto del tunnel verrebbe inviato a questo indirizzo dal peer remoto.

indirizzo remoto del tunnel GRE L'indirizzo utilizzato dal firewall all'interno del tunnel per raggiungere l'altra estremità. Il traffico destinato per l'altra estremità del tunnel deve utilizzare questo indirizzo come gateway per il routing.

Tunnel di sottorete GRE La maschera di sottorete per l'indirizzo di interfaccia GRE.

Descrizione Una breve descrizione di questo tunnel GRE a scopo di documentazione.

- Fare clic su **Salvare**

8.9 GIF (Interfaccia di tunnel generica)

Un'interfaccia di tunnel generica (GIF) è simile al GRE; entrambi i protocolli sono un mezzo per tunnel del traffico tra due host senza crittografia. In aggiunta al tunnel IPv4 o IPv6, il GIF può essere utilizzato per il tunnel IPv6 su reti IPv4 e viceversa. I tunnel GIF sono comunemente utilizzati per ottenere la connettività IPv6 ad un broker di tunnel come Hurricane Electric in luoghi in cui la connettività IPv6 non è disponibile.

Vedi anche:

Vedere *Collegamento con un servizio di Tunnel Broker* per informazioni sulla connessione a un servizio tunnelbroker.

Le interfacce GIF trasportano più informazioni attraverso il tunnel di quelle che possono fare con GRE, ma il GIF non è così ampiamente supportato. Ad esempio, un tunnel GIF è in grado di collegare il livello 2 tra due posizioni, mentre GRE non può.

Come creare o gestire un'interfaccia GIF:

- Arrivare a Interfacce>(Assegnare), scheda GIF
-  Fare clic su Aggiungere per creare una nuova istanza GIF o fare clic su per modificare un'interfaccia esistente
- Completare le impostazioni come segue:

Interfaccia primaria L'interfaccia su cui il tunnel GIF terminerà. Spesso questa sarà una WAN o una connessione di tipo WAN.

Indirizzo remoto GIF L'indirizzo del peer remoto. Questo è l'indirizzo in cui i pacchetti GIF saranno inviati da questo firewall; L'indirizzo esterno instradabile all'altra estremità del tunnel. Ad esempio, in un tunnel IPv6-in-IPv4 a Hurricane Electric, questo sarebbe l'indirizzo IPv4 del server di tunnel, come ad esempio 209.51.181.2.

Indirizzo locale tunnel GIF L'indirizzo interno per la fine del tunnel su questo firewall. Il firewall utilizzare questo indirizzo per il proprio traffico nel tunnel, e il traffico remoto del tunnel verrebbe inviato a questo indirizzo dal peer remoto. Ad esempio, per il tunneling IPv6-in-IPv4 tramite Hurricane Electric, ci si riferisce a questo come l'"**indirizzo del client IPv6.**

Indirizzo remoto del tunnel GIF L'indirizzo utilizzato dal firewall all'interno del tunnel per raggiungere l'altra estremità. Il traffico destinato per l'altra estremità del tunnel deve utilizzare questo indirizzo come gateway per il routing. Ad esempio, per il tunneling IPv6-in-IPv4 tramite Hurricane Electric, ci si riferisce a questo come **indirizzo del server IPv6**.

Sottorete del tunnel GIF La maschera di sottorete o lunghezza del prefisso per l'indirizzo di interfaccia. In questo esempio è 64.

Caching della route Le opzione di caching della route controllano se è è memorizzato il percorso al punto di fine remoto o meno. Se il percorso del peer remoto è statico, impostando questa opzione, si può evitare un percorso di ricerca per pacchetto. Tuttavia, se il percorso verso il lato opposto dovesse cambiare, questa opzione potrebbe comportare che il traffico GIF non riusca a fluire quando la route cambia.

Comportamento amichevole dell'ECN L'opzione di comportamento amichevole ECN controlla se la pratica della notifica esplicita della congestione (ECN) di copiare il bit TOS in entrata/in uscita dal traffico del tunnel è eseguita o meno dal firewall. Per default il firewall cancella il bit TOS sui pacchetti o lo imposta a 0, a seconda della direzione del traffico. Con questa opzione impostata, il bit viene copiato come necessario tra i pacchetti interni ed esterni per essere più disponibile per i router intermedi che possono eseguire la configurazione del traffico. Questo comportamento rompe il RFC 2893 quindi deve essere utilizzato solo quando entrambi i peers accettano di abilitare l'opzione.

Descrizione Una breve descrizione di questo tunnel GIF a scopo di documentazione.

- Fare clic su **Salva**

Nota: Se l'interfaccia GIF è assegnata in **Interfacce>(assegnare),** impostare il **tipo di configurazione IPv4** e il **tipo di configurazione IPv6** su *Nessuno*. Il firewall creerà automaticamente un gateway dinamico in questa situazione.

8.10 LAGG (Aggregazione di Link)

L'aggregazione dei link è gestita da interfacce di tipo lagg(4) (LAGG) su Firew4LL. LAGG combina più interfacce fisiche come un'unica interfaccia logica. Ci sono diversi modi in cui questo può funzionare, sia per guadagnare sulla larghezza di banda supplementare, sulla ridondanza, o su qualche combinazione delle due.

Come creare o gestire interfacce LAGG:

- Individuare **Interfacce>(assegnare),** scheda LAGG
- Fare clic su  **Aggiungere** per creare un nuovo LAGG, oppure fare clic su  per modificare un'istanza esistente.
- Completare le impostazioni come segue:

Interfacce primarie Questo elenco contiene tutte le interfacce attualmente non assegnate e i membri dell'interfaccia LAGG corrente quando si modifica un'istanza esistente. Per aggiungere interfacce a questo LAGG, selezionare una o più interfacce in questo elenco.

Nota: Un'interfaccia può essere aggiunta ad un gruppo LAGG solo se non è assegnata. Se un'interfaccia non è presente nell'elenco, è probabile che sia già stata assegnata come interfaccia.

Protocollo LAGG Attualmente esistono sei diverse modalità operative per le interfacce LAGG: LACP, Failover, Bilanciamento di carico, Round Robin e Nessuno.

LACP Il protocollo LAGG più comunemente utilizzato. Questa modalità supporta il protocollo di controllo dell'aggregazione link IEEE 802.3ad (LACP) e il protocollo Marker. In modalità LACP, la negoziazione avviene con lo switch – che deve anche supportare LACP – per formare un gruppo di porte che sono tutte attive allo stesso tempo. Si tratta di un gruppo di aggregazione di collegamenti o di un GAL. La velocità e la MTU di ogni porta di un GAL devono essere identiche e le porte devono

anche funzionare a full- duplex. Se si perde il collegamento con una porta del GAL, il GAL continua a funzionare ma a capacità ridotta. In questo modo, un pacchetto LACP LAGG può ottenere sia ridondanza che una maggiore larghezza di banda.

Il traffico è bilanciato tra tutte le porte del GAL, tuttavia, per la comunicazione tra due singoli host utilizzerà una sola porta alla volta perché il client parlerà con un solo indirizzo MAC alla volta. Per connessioni multiple attraverso dispositivi multipli, questa limitazione diventa effettivamente irrilevante. La limitazione non è rilevante anche per il failover.

Oltre a configurare questa opzione su Firew4LL, lo switch deve abilitare LACP su queste porte o avere le porte raggruppate in un gruppo LAG. Entrambe le parti devono concordare la configurazione in modo che possa funzionare correttamente

failover Quando si utilizza il protocollo Failover il traffico LAGG verrà inviato solo sull'interfaccia primaria del gruppo. Se l'interfaccia primaria non fallisce, allora il traffico utilizzerà la prossima interfaccia disponibile. L'interfaccia primaria è la prima interfaccia selezionata nell'elenco, e continuerà in ordine fino a raggiungere la fine delle interfacce selezionate.

Nota:

Per impostazione predefinita, il traffico può essere ricevuto solo sull'interfaccia attiva. Creare un sistema adattabile per `net.link.lagg.failover_rx_all` con il valore di 1 per consentire al traffico di essere ricevuto su ogni interfaccia del gruppo.

Bilanciamento del carico La modalità di bilanciamento del carico accetta il traffico in entrata su qualsiasi porta del gruppo LAGG e bilancia il traffico in uscita su qualsiasi porta attiva del gruppo LAGG. Si tratta di un'impostazione statica che non controlla lo stato di collegamento né negozia con lo switch. Il traffico in uscita è bilanciato dal carico in base a tutte le porte attive del LAGG utilizzando un hash calcolato utilizzando diversi fattori, come l'indirizzo IP di origine e di destinazione, l'indirizzo MAC e il tag VLAN.

Round Robin Questa modalità accetta il traffico in entrata su qualsiasi porta del gruppo LAGG e invia il traffico in uscita utilizzando un algoritmo di pianificazione round robin. questo significa che il traffico sarà inviato in sequenza, utilizzando ogni interfaccia del gruppo a turno.

Nessuna Questa modalità disabilita il traffico sull'interfaccia LAGG senza disabilitare l'interfaccia stessa. Il sistema operativo farà ancora credere che l'interfaccia sia attiva e utilizzabile, ma nessun traffico verrà inviato o ricevuto sul gruppo

Descrizione Una breve nota sullo scopo di questa istanza LAGG.

- Fare clic su **Salvare**

  Dopo aver creato un'interfaccia LAGG, questa funziona come qualsiasi altra interfaccia fisica. Assegnare l'interfaccia lagg in **Interfacce>(assegnare)** e dargli un indirizzo IP, o costruire altre cose su di esso come una VLAN.

8.10.1 LAGG e regolazione del traffico

A causa di limitazioni in FreeBSD, lagg(4) non supporta altq(4), quindi non è possibile usare direttamente il regolatore del traffico sulle interfacce LAGG. Le interfacce vlan(4) supportano altq(4) e le VLAN possono essere usate in aggiunta alle interfacce LAGG, quindi usando le VLAN si può risolvere il problema. Come soluzione alternativa, i limitatori possono controllare l'utilizzo della larghezza di banda sulle interfacce LAGG.

8.10.2 Portata della LAGG

L'utilizzo di un LAGG non garantisce necessariamente un flusso completo pari alla somma di tutte le interfacce. In particolare, un singolo flusso non supererà la portata di un'interfaccia membro della LAGG. Il traffico su un LAGG viene gestito in modo tale che i flussi tra due host, come Firew4LL e un gateway upstream, utilizzino solo un singolo link poiché il flusso avviene tra un singolo indirizzo MAC su ciascun lato.

Nelle reti dove ci sono molti host che comunicano con diversi indirizzi MAC, l'uso può avvicinarsi alla somma di tutte le interfacce nel LAGG.

8.11 Configurazione dell'interfaccia

Per assegnare una nuova interfaccia:

- Individuare **Interfacce>(assegnare)**
- Scegliere la nuova interfaccia dalla lista delle **porte disponibile di rete**
- Cliccare su  **Inserire**

La nuova interfaccia assegnata verrà visualizzata nell'elenco. La nuova interfaccia avrà un nome predefinito assegnato dal firewall come OPT1 o OPT2, con il numero crescente in base al suo ordine di assegnazione. Le prime due interfacce predefinite per i nomi WAN e LAN, ma possono essere rinominati. Questi nomi OPTx appaiono nel menu delle **interfacce**, come **Interfacce>OPT1**. Selezionando l'opzione del menu per l'interfaccia si aprirà la pagina di configurazione per l'interfaccia.

Sono disponibili le seguenti opzioni per tutti i tipi di interfaccia.

8.11.1 Descrizione

Il nome della interfaccia. Questo cambierà il nome dell'interfaccia nel menu **Interfacce**, nelle schede sotto **Firewall>Regole**, in **Servizi>DHCP**, e altrove in tutta la GUI. I nomi delle interfacce possono contenere solo lettere, numeri e lìunico carattere speciale che è permesso è un underscore («_»). L'uso di un nome personalizzato rende più facile ricordare lo scopo di un'interfaccia e identificare un'interfaccia per l'aggiunta di regole del firewall o la scelta di altre funzionalità per interfaccia.

8.11.2 Tipo di configurazione IPv4

Consente di configurare le impostazioni IPv4 per l'interfaccia. Dettagli per questa opzione sono nella sezione successiva,*Tipi di WAN con Ipv4*.

8.11.3 IPv6 Tipo di configurazione

Consente di configurare le impostazioni IPv6 per l'interfaccia. Dettagli per questa opzione sono in*Tipi di WAN con IPv6*.

8.11.4 Indirizzo MAC

L'indirizzo MAC di un'interfaccia può essere modificato ("mascherato") per simulare un pezzo di apparecchiatura precedente.

Avvertimento: Avvertimento: Si consiglia di evitare questa pratica. Il vecchio MAC sarebbe generalmente eliminato resettando l'apparecchiatura a cui questo firewall si connette, o cancellando la tabella ARP, o in attesa che le vecchie voci ARP scadano. È una soluzione a lungo termine a un problema temporaneo.

Lo spoofing dell'indirizzo MAC del firewall precedente può consentire una transizione agevole da un vecchio router a un nuovo router, in modo che le cache ARP sui dispositivi e sui router upstream non siano un problema. Può anche essere usato per ingannare un pezzo di apparecchiatura facendogli credere che stia parlando con lo stesso dispositivo con cui stava parlando prima, come nei casi in cui un certo router di rete utilizza un ARP statico o altrimenti filtri basati sull'indirizzo MAC. Questo è comune sui modem via cavo, dove possono richiedere l'indirizzo MAC per essere registrati se questo cambia.

Un aspetto negativo dello spoofing dell'indirizzo MAC è che a meno che il vecchio pezzo di apparecchiatura sia andato permanentemente in pensione, vi è il rischio di avere in seguito un conflitto xon l'indirizzo MAC sulla rete, che può portare a problemi di connettività. I problemi della cache ARP tendono ad essere molto temporanei, risolvendosi automaticamente in pochi minuti o con il ciclo di alimentazione di altre apparecchiature.

Se il vecchio indirizzo MAC deve essere ripristinato, questa opzione deve essere svuotata e quindi il firewall deve essere riavviato. In alternativa, inserire l'indirizzo MAC originale della scheda di rete e salvare/applicare, quindi svuotare nuovamente il valore.

8.11.5 MTU (Unità di trasmissione massima)

Il campo dimensione di **massima unità di trasmissione (MTU)** può essere lasciato vuoto, ma può essere modificato quando richiesto. Alcune situazioni possono richiedere un MTU inferiore per garantire che i pacchetti siano dimensionati in modo appropriato per una connessione Internet. Nella maggior parte dei casi, i valori predefiniti assunti per il tipo di connessione WAN funzioneranno correttamente. Può essere aumentato per coloro che utilizzano cornici jumbo sulla loro rete.

In una tipica rete in stile Ethernet, il valore predefinito è 1500, ma il valore effettivo può variare a seconda della configurazione dell'interfaccia.

8.11.6 MSS (Dimensione massima del segmento)

Simile al campo MTU, il campo MSS adegua la dimensione massima del segmento (MSS) di connessioni TCP alla dimensione specificata, al fine di lavorare intorno ai problemi con il percorso MTU Discovery

8.11.7 Velocità e duplex

Il valore predefinito per la velocità di collegamento e duplex è quello di lasciare che il firewall decida cosa è meglio. L' opzione predefinita tipica è *Autoselect*, che negozia le migliori impostazioni di velocità e duplex con il peer, di solito uno switch.

Le impostazioni di velocità e duplex su un'interfaccia devono corrispondere al dispositivo a cui è collegata. Ad esempio, quando il firewall è impostato su *Autoselect*, lo switch deve essere configurato anche per *Autoselect*. Se l'interruttore o un altro dispositivo ha una velocità specifica e duplex forzato, deve essere corrisposto dal firewall.

8.11.8 Blocco delle reti private

Quando il **blocco delle reti private** è attivo Firew4LL inserisce automaticamente una regola che impedisce a qualsiasi rete RFC 1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) e loopback (127.0.0.0/8) di comunicare su tale interfaccia.

Questa opzione è di solito desiderabile solo su interfacce di tipo WAN per impedire la possibilità di traffico privato numerato in arrivo su un'interfaccia pubblica.

8.11.9 Blocco delle reti bogon

Quando il **blocco delle reti bogon** è attivo, Firew4LL bloccherà il traffico da un elenco di reti riservate e non assegnate. Questo elenco viene aggiornato periodicamente dal firewall, automaticamente.

Ora che lo spazio IPv4 è stato assegnato, questa lista è abbastanza piccola, contenente per lo più reti che sono state riservate in qualche modo da IANA. Queste sottoreti non dovrebbero mai essere in uso attivo su una rete, specialmente una rivolta a Internet, quindi è una buona prassi abilitare questa opzione sulle interfacce tipo WAN. Per IPv6, l'elenco è abbastanza grande, contenente parti considerevoli del possibile spazio IPv6 che deve ancora essere allocato. Sui sistemi con basse quantità di RAM, questa lista potrebbe essere troppo grande, o il valore predefinito di **Voci massime della tabella del firewall** potrebbe essere troppo piccolo. Tale valore può essere regolato in **Sistema>Avanzate** nella scheda **Firewall & NAT**.

8.12 Tipi di WAN con IPv4

Una volta che un'interfaccia è stata assegnata, nella maggior parte dei casi richiederà un indirizzo IP. Per le connessioni IPv4 sono disponibili le seguenti opzioni: IPv4 statico, DHCP, PPP, PPPoE, PPTP e L2TP. Queste opzioni sono selezionate utilizzando il selettore del tipo di **configurazione IPv4** su una pagina di interfaccia (ad es. **Interfacce>WAN**).

8.12.1 Nessuno

Quando il **tipo di configurazione IPv4** è impostato su *Nessuno*, IPv4 è disabilitato sull'interfaccia. Questo è utile se l'interfaccia non ha connettività IPv4 o se l'indirizzo IP dell'interfaccia è gestito in altro modo, come per un'interfaccia OpenVPN o GIF.

8.12.2 IPv4 statico

Con IPv4 statico, l'interfaccia contiene un indirizzo IP configurato manualmente. Una volta scelto, sono disponibili tre campi aggiuntivi nella schermata di configurazione dell'interfaccia: indirizzo IPv4, un selettore di sottorete CIDR e il campo del **gateway di upstrem IPv4**.

Configurare l'interfaccia per l'IPv4 statico su un'interfaccia interna (ad es. LAN, DMZ):

- Selezionare *IPv4 statico* sotto **Tipo di configurazione IPv4**
- Inserire l'indirizzo IPv4 per l'interfaccia nella casella di **indirizzo IPv4**
- Scegliere la maschera di sottorete appropriata dal menù a discesa CIDR dopo la casella dell'indirizzo
- Non selezionare un **gateway di upstream IPv4**

Per configurare l'interfaccia per IPv4 statico su un tipo di interfaccia WAN:

- Selezionare *IPv4 statico* sotto **Tipo di configurazione IPv4**
- Inserire l'indirizzo IPv4 per l'interfaccia nella casella di **indirizzo IPv4**
- Scegliere la maschera di sottorete appropriata dal menù a discesa CIDR dopo la casella dell'indirizzo
- Eseguire una delle seguenti azioni per usare un gateway sull'interfaccia:
  - Selezionare un **gateway di upstream IPv4** dall'elenco, o

- Cliccare su  **Aggiungere un nuovo gateway** per creare un nuovo gateway se non esiste già. Cliccando sul link, viene visualizzato un form modale per aggiungere la porta d'ingresso senza lasciare la pagina. Compilare i dati richiesti sul nuovo modulo:

  Gateway predefinito Se questa è l'unica WAN o sarà una nuova WAN predefinita, selezionare questa casella. I gateway IPv4 e IPv6 predefiniti funzionano indipendentemente l'uno dall'altro. I due non devono necessariamente essere sullo stesso circuito. Cambiare il gateway IPv4 predefinito non ha alcun effetto sul gateway IPv6, e viceversa.

  Nome del gateway Il nome utilizzato per riferirsi al gateway all'interno, così come in luoghi come i gruppi gateway, i grafici di qualità, e altrove.

  IPv4 del gateway L'indirizzo IP del gateway. Questo indirizzo deve essere all'interno della stessa sottorete dell'indirizzo IPv4 statico quando si usa questo modulo.

  Descrizione Breve testo che indica lo scopo del gateway.

- Cliccare su **Inserire**

Nota: Selezionando un gateway IPv4 dall'elenco a discesa o aggiungendo e selezionando un nuovo gateway, Firew4LL tratterà questa interfaccia come un'interfaccia di tipo WAN per il NAT e le funzioni correlate. Questo non è auspicabile per interfacce interne come LAN o DMZ. I gateway possono ancora essere utilizzati su interfacce interne per percorsi statici senza selezionare un gateway IPv4 upstream qui sullo schermo delle interfacce.

8.12.3 DHCP

Quando un'interfaccia è impostata su DHCP, Firew4LL tenterà la configurazione IPv4 automatica di questa interfaccia tramite DHCP. Questa opzione attiva anche diversi campi aggiuntivi nella pagina. Nella maggior parte dei casi questi campi aggiuntivi possono essere lasciati in bianco.

Hostname Alcuni ISP richiedono l'hostname per l'identificazione del client. Il valore nel campo **Nome dell'host** viene inviato come identificativo del client DHCP e hostname quando si richiede un contratto di locazione DHCP.

Indirizzo IPv4 dell'Alias Questo valore è usato come indirizzo di alias IPv4 fisso dal client DHCP poiché un tipico VIP dell'IP Alias non può essere usato con DHCP. Questo può essere utile per accedere a un pezzo di ingranaggio su una rete separata, numerata staticamente al di fuori dello scopo DHCP. Un esempio potrebbe essere quello di raggiungere un indirizzo IP di gestione del modem via cavo.

Rifiutare le locazioni da Un indirizzo IPv4 per un server DHCP che dovrebbe essere ignorato. Ad esempio, un modem via cavo che distribuisce indirizzi IP privati quando la sincronizzazione via cavo è stata persa. Inserisre qui l'indirizzo IP privato del modem, ad es. 192.168.100.1 e il firewall non rileverà né tenterà di usare un indirizzo IP fornito dal server specificato.

Configurazione avanzata Abilita le opzioni per controllare i tempi del protocollo. Nella stragrande maggioranza dei casi questo deve essere lasciato deselezionato e le opzioni all'interno invariate.

Tempistiche del protocollo I campi di questa area forniscono un controllo a grana fine sui tempi utilizzati da dhclient quando si gestisce un indirizzo su questa interfaccia. Queste opzioni sono quasi sempre lasciate ai loro valori predefiniti. Per maggiori dettagli su cosa controlla ogni campo, vedere la pagina principale di dhclient

Predefiniti Ha diverse opzioni per i valori di tempo del protocollo preimpostati. Questi sono utili come punto di partenza per le regolazioni personalizzate o per l'uso quando i valori devono essere reimpostati ai valori predefiniti

Override di configurazione Abilita un campo per usare un file di configurazione dhclient personalizzato. Il percorso completo deve essere dato. L'utilizzo di un file personalizzato è raramente necessario, ma alcuni ISP richiedono campi DHCP o opzioni che non sono supportate nella GUI Firew4LL.

8.12.4 Tipi di PPP

I vari tipi di connessione basati su PPP, come PPP, PPPoE, PPTP e L2TP, sono tutti trattati in dettaglio in precedenza in questo capitolo (PPP). Quando uno di questi tipi è selezionato qui sullo schermo delle interfacce, le loro opzioni di base possono essere cambiate come descritto. Per accedere alle opzioni avanzate, seguire il link di questa pagina o passare a **Interfacce>(assegnare)** sulla schede **PPP**, trovare la voce, e modificarla.

8.13 Tipi di WAN con IPv6

Analogamente a IPv4, il **tipo di configurazione IPv6** controlla se e come un indirizzo IPv6 è assegnato ad un'interfaccia. Ci sono diversi modi per configurare IPv6 e il metodo esatto dipende dalla rete a cui questo firewall è collegato e come l'ISP ha distribuito IPv6.

Vedere anche:

Per ulteriori informazioni sull'IPv6, inclusa un'introduzione di base, vedere *IPv6*.

8.13.1 Nessuno

Quando il **tipo di configurazione IPv6** è impostato su *Nessuno*, IPv6 è disabilitato sull'interfaccia. Questo è utile se l'interfaccia non ha connettività IPv6 o se l'indirizzo IP dell'interfaccia è gestito in altro modo, come per un'interfaccia OpenVPN o GIF.

8.13.2 IPv6 statico

I controlli degli IPv6 statici funzionano in modo identico alle impostazioni degli IPv4 statici. Vedere *IPv4 statico* per i dettagli.

Con **IPv6 statico**, l'interfaccia contiene un indirizzo IPv6 configurato manualmente. Una volta scelto, sono disponibili tre campi aggiuntivi nella schermata di configurazione dell'interfaccia: **Indirzzo IPv6**, un selettore della lunghezza del prefisso e il campo **gateway Upstream IPv6**.

I gateway IPv4 e IPv6 di default funzionano indipendentemente l'uno dall'altro. I due non devono necessariamente essere sullo stesso circuito. Cambiare il gateway IPv4 predefinito non ha effetto sul gateway IPv6 e viceversa.

8.13.3 DHCP6

DHCP6 configura Firew4LL per tentare la configurazione IPv6 automatica di questa interfaccia tramite DHCPv6. DHCPv6 configura l'interfaccia con un indirizzo IP, lunghezza del preisso, server DNS, ecc. ma non un gateway. Il gateway è ottenuto tramite annunci del router, quindi questa interfaccia sarà impostata per accettare annunci del router. Si tratta di una scelta progettuale nell'ambito della specifica IPv6, non di una limitazione di Firew4LL. Per maggiori informazioni sulla pubblicità del router, vedere *Annunci del Router*.

Sono disponibili diversi campi aggiuntivi per DHCP con IPv4 che non esistono per DHCP con IPv4:

Utilizzare la connettività IPv4 come interfaccia primaria Quando è impostata, la richiesta DHCP con IPv6 viene inviata utilizzando IPv4 su questa interfaccia, piuttosto che utilizzando l'IPv6 originario. Questo è richiesto solo in casi speciali quando l'ISP richiede questo tipo di configurazione.

Richiedere solo un prefisso IPv6 Quando è impostato, il client DHCPv6 non richiede un indirizzo per l'interfaccia stessa, richiede solo un prefisso delegato.

Dimensione della delega del prefisso DHCPv6 Se l'ISP fornisce una rete IPv6 instradata tramite la delega del prefisso, pubblicheranno la dimensione della delega, che può essere selezionata qui. È un valore tra 48 e 64. Per maggiori informazioni su come funziona la delega del prefisso DHCPv6, vedere *Delega del Prefisso DHCP6*. Per utilizzare questa delega, un'altra interfaccia interna deve essere impostata su **tipo di configurazione IPv6** della *traccia di interfaccia* (*Tracciare interfaccia*) in modo che possa utilizzare gli indirizzi delegati dal server DHCPv6 upstream.

Inviare suggerimento per il prefisso IPv6 Quando impostata, la dimensione della delega del prefisso DHCPv6 viene inviata con la richiesta di informare il server upstream riguardo la grandezza desiderata per una delega da questo firewall. Se un ISP permette la scelta, e la dimensione scelta è all'interno della gamma consentita, la dimensione richiesta sarà data al posto della dimensione predefinita.

Debug Quando è impostato, il client DHCPv6 viene avviato in modalità debug.

Configurazioni avanzate Consente una vasta gamma di parametri di regolazione avanzati per il client DHCPv6. Queste opzioni sono usate raramente, e quando sono richieste, i valori sono dettati dall'ISP o dall'amministratore di rete. Vedere la pagina principale di dhcp6c.conf per i dettagli.

Override di configurazione Abilita un campo per usare un file di configurazione personalizzato. Il percorso completo deve essere dato. L'utilizzo di un file personalizzato è raramente necessario, ma alcuni ISP richiedono campi DHCP o opzioni che non sono supportati nella GUI Firew4LL.

8.13.4 SLAAC

L'autoconfigurazione senza indirizzo (SLAAC) come il tipo IPv6 fa in modo che Firew4LL configuri l'indirizzo IPv6 per l'interfaccia degli annunci router (RA) che pubblicizzano il prefisso e le relative informazioni. Si noti che il DNS non è tipicamente fornito tramite RA, quindi Firew4LL tenterà comunque di ottenere i server DNS tramite DHCPv6 quando si utilizza SLAAC. In futuro, le estensioni RDNSS per il processo RA possono consentire che i DNS server siano ottenuti da RA. Per maggiori informazioni sugli annunci del router, vedere *Annunci del Router*.

8.13.5 Tunnel di 6RD

6RD è una tecnologia di tunneling IPv6 impiegata da alcuni ISP per attivare rapidamente il supporto IPv6 per le loro reti, passando il traffico IPv6 all'interno di pacchetti IPv4 appositamente predisposti tra e router utente finale e il relay ISP. Si riferisce a 6to4 ma è destinato ad essere utilizzato all'interno della rete ISP, utilizzando gli indirizzi IPv6 dall'ISP per il traffico client. Per utilizzare 6RD, l'ISP deve fornire tre informazioni: il prefisso 6RD, il relay di confine 6RD e la lunghezza del prefisso IPv4 di 6RD.

Prefisso 6RD Il prefisso IPv6 6RD assegnato dall'ISP, come 2001:db8::/32.

Relay di confine 6RD L'indirizzo IPv4 del relay 6RD dell'ISP.

Lunghezza del prefisso IPv4 6RD Controlla quanto dell'indirizzo IPv4 dell'utente finale utente è codificato all'interno del prefisso 6RD. Questo è normalmente fornito dal ISP. Un valore pari a 0 significa che l'intero indirizzo IPv4 sarà incorporato all'interno del prefisso 6RD. Questo valore consente agli ISP di indirizzare efficacemente più indirizzi IPv6 ai client rimuovendo le informazioni ridondanti IPv4 se una assegnazione ISP è interamente all'interno della stessa sottorete più grande.

8.13.6 Tunnel 6to4

Simile a 6RD, *6to4* è un altro metodo di tunneling del traffico IPv6 all'interno IPv4. A differenza di 6RD, tuttavia, 6to4 utilizza prefissi e relay costanti. Come tale non ci sono impostazioni regolabili dall'utente per utilizzare l'opzione *6to4*. Il prefisso 6to4 è sempre 2002::/16. Qualsiasi indirizzo all'interno del prefisso 2002::/16 è considerato un indirizzo 6to4 piuttosto che un indirizzo IPv6 originario. Anche a differenza di 6RD, un tunnel 6to4 può essere terminato ovunque su Internet, non solo presso l'utente finale ISP, quindi la qualità della connessione tra l'utente e il relay 6to4 può variare notevolmente.

I tunnel 6to4 sono sempre terminati all'indirizzo IPv4 di 192.88.99.1. Questo indirizzo IPv4 è anycasted, il che significa che anche se l'indirizzo IPv4 è lo stesso ovunque, può essere indirizzato regionalmente verso un nodo vicino all'utente.

Un'altra carenza di 6to4 è che si basa su altri router per trasmettere il traffico tra la rete 6to4 e il resto della rete IPv6. C'è la possibilità che alcuni peer IPv6 non abbiano la connettività alla rete 6to4, e quindi questi sarebbero irraggiungibili per i client che si connettono ai relay 6to4, e questo potrebbe anche variare a seconda del nodo 6to4 a cui l'utente è effettivamente collegato.

8.13.7 Track Interface

La scelta di *Track Interface* funziona in concerto con un'altra interfaccia IPv6 utilizzando la delega del prefisso DHCPv6. Quando una delega è ricevuta dall'ISP, questa opzione indica quale interfaccia verrà assegnata agli indirizzi IPv6 delegati dall'ISP e nei casi in cui si ottiene una delega più ampia, quale prefisso all'interno della delega viene utilizzato.

> **Interfaccia IPv6** Un elenco di tutte le interfacce del sistema attualmente impostate per i tipi dinamici di WAN IPv6 che offrono la delega di prefissi (DHCPv6, PPPoE, 6rd, ecc.). Selezionare l'interfaccia dall'elenco che riceverà le informazioni sulla sottorete delegata dall'ISP.
>
> **ID del prefisso IPv6** Se l'ISP ha delegato più di un prefisso tramite DHCPv6, lId del prefisso "IPv6 controlla quale delle sottoreti delegate /64 sarà utilizzata su questa interfaccia. Questo valore è specificato in esadecimale.

Ad esempio, Se una delega è fornita dall'ISP significa che le reti 16 /64 sono disponibili, così i prefissi ID da 0 a f può essere utilizzato.

Per maggiori informazioni su come funziona il prefisso di delega, vedere *Delega del prefisso DHCP6 prefisso*.

Firew4LL supporta numerosi tipi di interfacce di rete, sia da utilizzare direttamente interfacce fisiche oppure impiegando altri protocolli come PPP o VLAN.

Le assegnazioni di interfaccia e la creazione di nuove interfacce virtuali sono tutte gestite in **Interfacce>(assegnare).**

8.14 Interfacce fisiche e virtuali

La maggior parte delle interfacce discusse in questo capitolo possono essere assegnate come WAN, LAN o come interfaccia OPT sotto **Interfacce>(assegnare).** Tutte le interfacce attualmente definite e rilevate sono elencate direttamente su **Interfacce>(assegnare)** o nell'elenco delle interfacce disponibili per l'assegnazione. Per impostazione predefinita, questo elenco include solo le interfacce fisiche, ma le altre schede in **Interfacce>(assegnare)** possono creare interfacce virtuali che possono poi essere assegnate.

Le interfacce su Firew4LL supportano varie combinazioni di opzioni sulle interfacce stesse. Possono anche supportare più reti e protocolli su una singola interfaccia, o più interfacce possono essere unite in una maggiore capacità o interfaccia virtuale ridondante.

Tutte le interfacce sono trattate allo stesso modo; ogni interfaccia può essere configurata per qualsiasi tipo di connettività o ruolo. Le interfacce WAN e LAN di default possono essere rinominate e utilizzate in altri modi.

Le interfacce fisiche e virtuali vengono trattate una volta assegnate, e hanno le stesse capacità. Ad esempio, un'interfaccia VLAN può avere lo stesso tipo di configurazione che può avere un'interfaccia fisica. Alcuni tipi di interfaccia ricevono un trattamento speciale una volta assegnate, che sono coperti nelle rispettive sezioni di questo capitolo.

Questa sezione illustra i vari tipi di interfacce che possono essere creati, non assegnati, e gestiti.

CAPITOLO 9

Gestione Utenti e Autenticazione

9.1 Gestione utenti

La **gestione utenti** si trova su **Sistema>Gestione utenti**. Da lì utenti, gruppi, server possono essere gestiti, e le impostazioni che regolano il comportamento della gestione dell'utente possono essere modificate.

9.1.1 Privilegi

Gestire i privilegi per gli utenti e i gruppi è simile, quindi entrambi saranno coperti qui piuttosto che duplicare lo sforzo. Se un utente o un gruppo è gestito, la voce deve essere creata e salvata prima che i privilegi possano essere aggiunti all'account o al gruppo. Per aggiungere privilegi, quando si modifica l'utente o il gruppo esistente, fare clic su  **Aggiungere** nella sezione **Privilegi assegnati** o **Privilegi effettivi**.

Viene presentato un elenco di tutti i privilegi disponibili. I privilegi possono essere aggiunti uno alla volta selezionando una singola voce, o selezionando più voci usando ctrl-click. Se altri privilegi sono già presenti sull'utente o sul gruppo, essi sono nascosti da questa lista quindi non possono essere aggiunti due volte. Per cercare uno specifico privilegio per nome, inserire il termine di ricerca nella casella **Filtro** e fare clic su  **Filtro**.

La selezione di un privilegio mostrerà una breve descrizione del suo scopo nell'area del blocco informazioni sotto i pulsanti di autorizzazione e di azione. La maggior parte dei privilegi sono auto-esplicativi sulla base dei loro nomi, ma alcuni permessi notevoli sono:

WebCFG - Tutte le pagine Consente l'accesso degli utenti a qualsiasi pagina nella GUI

WebCfg - Dashboard (tutti) Consente all'utente di accedere alla pagina della dashboard e a tutte le sue funzioni associate (widget, grafici, etc.)

WebCfg - Sistema Pagina di gestione della password utente: Se l'utente ha accesso solo a questa pagina, può accedere alla GUI per impostare la propria password, ma non per fare altro.

Utente - VPN - IPsec xauth Dialin Consente all'utente di collegarsi e autenticarsi per IPsec xauth

Utente - Config – Diniego della scrittura della configurazione Non consente all'utente di effettuare modifiche alla configurazione del firewall (*con- fig.xml*). Notare che questo non impedisce all'utente di compiere altre azioni che non comportano l'atto di scrivere per la configurazione.

Utente - Sistema - accesso all'account Shell Dà all'utente la possibilità di effettuare il login su ssh, anche se l'utente non avrà accesso a livello root quindi la funzionalità è limitata. Un pacchetto per *sudo* è disponibile per migliorare questa funzionalità.

Dopo il login, il firewall tenterà di visualizzare la dashboard. Se l'utente non vi ha accesso, essi saranno inoltrati alla prima pagina nella loro lista di privilegi a cui hanno il permesso di accedere.

I menu sul firewall contengono solo voci per le quali esistono privilegi su un account utente. Ad esempio, se l'unica pagina di diagnostica a cui un utente ha accesso è **Diagnostica>Ping**, allora nessun altro elemento verrà visualizzato nel menu **Diagnostica**.

9.1.2 Aggiunta/Modifica degli utenti

La scheda **Utenti** in **Sistema>Gestione utenti** è dove i singoli utenti sono gestiti. Per aggiungere un nuovo utente, fare clic su **Aggiungere**, per modificare un utente esistente, fare clic su .

Prima che i permessi possano essere aggiunti ad un utente, deve prima essere creato, quindi il primo passo è sempre quello di aggiungere l'utente e salvare. Se più utenti hanno bisogno delle stesse autorizzazioni, è più facile aggiungere un gruppo e quindi aggiungere utenti al gruppo.

Per aggiungere un utente, fare clic su **Aggiungere** e apparirà la nuova schermata utente.

Disabilitato Questa casella controlla se questo utente sarà attivo. Se questo account deve essere disattivato, spunta questa casella.

Nome utente Imposta il nome di login per l'utente. Questo campo è richiesto, deve essere inferiore a 16 caratteri e può contenere solo lettere, numeri, e un periodo, trattino, o sottolineatura.

Password e conferma sono necessarie. Le password sono memorizzate nella configurazione Firew4LL come hash. Assicurarsi che i due campi corrispondano per confermare la password.

Nome completo Campo opzionale che può essere utilizzato per inserire un nome più lungo o una descrizione per un account utente.

Data di scadenza Può anche essere definito se si desidera disattivare automaticamente l'utente quando tale data è stata raggiunta. La data deve essere indicata nel formato MM/GG/AAAA.

Gruppi Se i gruppi sono già stati definiti, questo controllo può essere utilizzato per aggiungere l'utente come membro. Per aggiungere un gruppo per questo utente, trovarlo nella colonna **Non membro di**, selezionarlo, e fare clic su per spostarlo nella colonna **Membro di**. Per rimuovere un utente dal gruppo, selezionarlo dalla colonna **Membro di** e fare clic su per spostarlo nella colonna **Non membro di**.

Privilegi effettivi appaiono quando si modifica un utente esistente, non quando si aggiunge un utente. Vedere **Privilegi** per informazioni sulla gestione dei privilegi. Se l'utente fa parte di un gruppo, i permessi del gruppo sono mostrati in questa lista, ma tali permessi non possono essere modificati, tuttavia possono essere aggiunti permessi ulteriori.

Certificato il comportamento di questa sezione cambia a seconda che un utente venga aggiunto o modificato. Quando si aggiunge un utente, per creare un certificato fare clic su **Cliccare per creare un certificato utente** per vedere il modulo per creare un certificato. Inserire il **nome descrittivo**, scegliere **un'autorità di certificazione**, selezionare una **lunghezza di chiave** e inserire una **durata di vita**. Per ulteriori informazioni su questi parametri, vedere Creare un certificato interno. Se si modifica un utente,

questa sezione della pagina diventa invece un elenco di certificati utente. Da qui, fare clic su  **Aggiungere** per aggiungere un certificato all'utente. Le impostazioni di quella pagina sono identiche a *Creare un certificato interno* tranne che un numero ancora maggiore di dati è pre-riempito con il nome utente. Se il certificato esiste già, selezionare *Scegliere un certificato esistente* e quindi scegliere un **certificato esistente** dall'elenco.

Chiavi autorizzate le chiavi pubbliche SSH possono essere inserite per l'accesso alla shell o ad altri SSH. Per aggiungere una chiave, incollare o inserire i dati chiave.

Chiave pre-condivisa IPsec Usata per una configurazione IPsec mobile con chiave pre-condivisa senza autenticazione. Se una **Chiave pre-condivisa per IPsec** viene inserita qui, il nome utente viene utilizzato come identificatore. La PSK viene visualizzata anche sotto **VPN>IPsec** nella scheda **Chiavi pre-condivisa**. Se IPsec mobile viene utilizzato solo con autenticazione, questo campo può essere lasciato vuoto.

Dopo aver salvato l'utente, fare clic sulla riga dell'utente per modificare la voce, se necessario.

9.1.3 Aggiunta/Modifica dei gruppi

I gruppi sono un ottimo modo per gestire le serie di autorizzazioni da dare agli utenti in modo che non abbiano bisogno di essere mantenuti individualmente su ogni account utente. Ad esempio, un gruppo potrebbe essere usato per gli utenti di IPsec xauth, o per un gruppo che può accedere alla dashboard del firewall, a un gruppo di amministratori del firewall, o a molti altri possibili scenari utilizzando qualsiasi combinazione di privilegi.

Come per gli utenti, un gruppo deve prima essere creato prima di aggiungere i privilegi. Dopo aver salvato il gruppo, modificare il gruppo per aggiungere i privilegi.

I gruppi sono gestiti in **Sistema>Gestione utente** nella scheda **Gruppi**. Per aggiungere un nuovo gruppo da questa schermata, fare clic su  **Aggiungere**. Per modificare un gruppo esistente, fare clic su  **Avanti** sulla sua voce nell'elenco.

Nota: Quando si lavora con LDAP e RADIUS, i gruppi locali devono esistere per corrispondere ai** gruppi di cui gli utenti sono membri sul server. Ad esempio, se esiste un gruppo LDAP chiamato «firewall_admins», Firew4LL deve anche contenere un gruppo chiamato identicamente, «firewall_admins», con i privilegi desiderati. I gruppi remoti con nomi lunghi o nomi contenenti spazi o altri caratteri speciali devono essere configurati per un campo di **applicazione** *remoto*.

Avviare il processo di aggiunta di un gruppo facendo clic su  **Aggiungere** e la schermata per aggiungere un nuovo gruppo apparirà.

Nome del gruppo Questa impostazione ha le stesse restrizioni di un nome utente: deve essere di 16 caratteri o meno e può contenere solo lettere, numeri, e un periodo, trattino, o sottolineatura. Questo può sembrare un po" limitato quando si lavora con gruppi di LDAP, per esempio, ma di solito è più facile creare o rinominare un gruppo con nome appropriato sul server di autenticazione invece di tentare di rendere il gruppo firewall compatibile.

Scopo Può essere impostato *Locale* per i gruppi sul firewall stesso (come quelli per l'uso nella shell), o *Remoto* per allentare le restrizioni del nome del gruppo e per evitare che il nome del gruppo sia esposto al sistema operativo di base. Ad esempio, i nomi dei gruppi di scopi remoti possono essere più lunghi e contenere spazi.

Descrizione Testo facoltativo in forma libera per riferimento e per meglio identificare lo scopo del gruppo nel caso in cui il nome del gruppo non sia sufficiente.

Gruppi Questa serie di controlli definisce quali utenti esistenti saranno membri del nuovo gruppo. Gli utenti Firewall sono elencati nella colonna **Non Membri** per impostazione predefinita. Per aggiungere un utente a questo gruppo, trovarlo nella colonna **Non Membri**, selezionarlo, e fare clic su  per spostarlo nella colonna **Membri**. Per rimuovere un utente dal gruppo, selezionarlo dalla colonna **Membri** e fare clic su  per spostarlo nella colonna **Non Membri**.

Privilegi assegnati appare solo quando si modifica un gruppo esistente. Questa sezione permette di aggiungere privilegi al gruppo. Vedere *Privilegi* in precedenza in questa guida per informazioni sulla gestione dei privilegi.

Impostazioni

La scheda **Impostazioni** in Gestione Utenti controlla due cose: quanto è valida una sessione di login e dove l'accesso alla GUI preferirà essere autenticato.

Tempo di sessione Questo campo specifica quanto durerà una sessione di login alla GUI quando inattiva. Questo valore è specificato in **minuti**, e il valore predefinito è di quattro ore (240 minuti). Un valore di 0 può essere inserito per disabilitare la scadenza della sessione, rendendo le sessioni di login valide per sempre. Un timeout più breve è meglio, anche se rendono sufficiente che un amministratore attivo non sarebbe disconnesso involontariamente durante l'esecuzione di modifiche.

Avvertimento:

Attenzione: Permettere a una sessione di rimanere valida quando inattiva per lunghi periodi di tempo non è sicuro. Se un amministratore lascia un terminale incustodito con una finestra del browser aperta e collegata, qualcuno o qualcos'altro potrebbe approfittare della sessione aperta.

Server di autenticazione Questo selettore sceglie la fonte di autenticazione primaria per gli utenti che accedono alla GUI. Questo può essere un server RADIUS o LDAP, o il database locale predefinito. Se il server RADIUS o LDAP è irraggiungibile per qualche motivo, l'autenticazione tornerà alla banca dati locale anche se viene scelto un altro metodo.

Quando si utilizza un server RADIUS o LDAP, gli utenti e/o appartenenti ai gruppi devono ancora essere definiti nel firewall al fine di allocare correttamente le autorizzazioni, in quanto non v'è ancora un metodo per ottenere i permessi dinamicamente da un server di autenticazione.

Affinché l'appartenenza al gruppo funzioni correttamente, Firew4LL deve essere in grado di riconoscere i gruppi presentati dal server di autenticazione. Ciò richiede due cose:

1. I gruppi locali devono esistere con nomi identici.
2. Firew4LL deve essere in grado di individuare o ricevere un elenco di gruppi dal server di autenticazione.

   Vedere i *server di autenticazione* per dettagli specifici per ogni tipo di server di autenticazione.

9.2 Server di autenticazione

Utilizzare la scheda **Server di autenticazione** in **Sistema>Gestione utenti**, i server RADIUS e LDAP può essere definita come fonti di autenticazione. Vedere *Supporto per tutta \firew4ll* per informazioni su dove possono essere utilizzati questi server in Firew4LL attualmente. Per aggiungere un nuovo server da questa schermata, fare clic su  **Inserire**. Per modificare un server esistente, fare clic su  **Aventi** al suo ingresso.

Vedi anche:

Per ulteriori informazioni, è possibile accedere al *Archivio di Hangout* per visualizzare l'Hangout di agosto 2015 su RADIUS e LDAP.

9.2.1 RADIUS

Per aggiungere un nuovo server RADIUS:

- Assicurarsi che il server RADIUS abbia il firewall definito come client prima di procedere.
- Passare a **Sistema>Gestione utente**, scheda **Server di autenticazione**.
- Fare clic su  Aggiungere.
- Impostare il selettore del **tipo** su *RADIUS*. Verranno visualizzate le impostazioni del server RADIUS.
- Compilare i campi come descritto di seguito:

  Nome descrittivo Il nome di questo server RADIUS. Questo nome sarà usato per identificare il server in tutta la GUI Firew4LL.

  Hostname o indirizzo IP L'indirizzo del server RADIUS. Questo può essere un nome di dominio completamente qualificato, o un indirizzo IP IPv4.

  Segreto condiviso La password stabilita per questo firewall sul software del server RADIUS.

  Servizi offerti Questo selettore imposta quali servizi sono offerti da questo server RADIUS. *Autenticazione e Contabilizzazione* , *Solo autenticazione* o *Solo contabilizzazione*. L"*autenticazione* utilizzerà questo server RADIUS per autenticare gli utenti. La *contabilizzazione* invia i dati di avvio/arresto dei pacchetti contabili RADIUS per le sessioni di login se supportato nell'area in cui viene utilizzato.

  Porta di autenticazione appare solo se è stata scelta una modalità di autenticazione. Impostare la porta UDP dove avverrà l'autenticazione RADIUS. La porta di default per l'autenticazione RADIUS è *1812*.

  Porta di contabilizzazione appare solo se viene scelta una modalità di ccontabilizzazione. Impostare la porta UDP dove avverrà la contabilizzazione RADIUS. La porta di contabilizzazione RADIUS di default è *1813*.

  Timeout di autenticazione Controlla quanto tempo, in secondi, il server RADIUS può impiegare per rispondere a una richiesta di autenticazione. Se lasciato vuoto, il valore predefinito è 5 secondi. Se un sistema interattivo di autenticazione a due fattori è in uso, aumentare questo tempo per tenere conto di quanto tempo impiegherà l'utente per ricevere e inserire un token, che può essere 60-120 secondi o più se deve attendere un'azione esterna come una telefonata, SMS, ecc.

- Fare clic su **Salvare** per creare il server.
- Visitare **Diagnostica>Autenticazione** per testare il server RADIUS utilizzando un account valido.

Per i gruppi RADIUS, il server RADIUS deve restituire una lista di gruppi nell'attributo di risposta del RADIUS Class come stringa. I gruppi multipli devono essere separati da un punto e virgola.

Ad esempio, in FreeRADIUS, per restituire i gruppi «admin» e «Utente VPN», si utilizzerebbe il seguente Attributo di risposta RADIUS:

```
Class := "admins;VPNUsers"
```

Se il server RADIUS restituisce correttamente l'elenco di gruppo per un utente e i gruppi esistono localmente, i gruppi saranno elencati sui risultati quando si utilizza la pagina **Diagnostica>Autenticazione** per testare un account. Se i

gruppi non si presentano, assicurati che esistano su Firew4LL con nomi corrispondenti e che il server stia restituendo l'attributo Class come stringa, non come binario.

9.2.2 LDAP

Per aggiungere un nuovo server LDAP:

- Assicurarsi che il server LDAP possa essere raggiunto dal firewall.
- Se viene utilizzato SSL, prima di procedere importare l'autorità di certificazione utilizzata dal server LDAP in Firew4LL. Vedere *Gestione dell'autorità di certificazione* per maggiori informazioni sulla creazione o l'importazione di CA.
- Passare a **Sistema>Gestione utenti**, scheda **Server**.
- Fare clic su  **Aggiungere**.
- Impostare il selettore del **tipo** a *LDAP*. Verranno visualizzate le impostazioni del server LDAP.
- Compilare i campi come descritto di seguito:

  Hostname o **indirizzo IP** L'indirizzo del server LDAP. Può essere un nome di dominio completamente qualificato, un indirizzo IP IPv4 o un indirizzo IP IPv6.

Nota: Se viene utilizzato SSL, qui deve essere specificato un hostname e deve corrispondere al **nome comune** del certificato del server presentato dal server LDAP e tale hostname deve essere risolto nell'indirizzo IP del server LDAP, ad es. *CN=ldap.esempio.com*, e *ldap.esempio.com è 192.168.1.5*. L'unica eccezione è che l'indirizzo IP del server è anche la CN del certificato server stesso. Questo può essere aggirato in alcuni casi, creando un override dell'host del Forwader DNS per fare in modo che il certificato del server CN risolva l'indirizzo IP corretto se non corrispondono in questa infrastruttura di

---

rete e non possono essere facilmente corretti.

Valore della porta Questa impostazione specifica la porta su cui il server LDAP sta ascoltando le query LDAP. La porta TCP di default è *389* e *636* per SSL. Questo campo viene aggiornato automaticamente con il valore predefinito basato sul **Trasporto** selezionato.

Nota: Quando si utilizza la porta *636* per SSL, Firew4LL utilizza un *ldaps://* URL, non supporta STARTTLS. Assicurarsi che il server LDAP sia in ascolto sulla porta corretta con la modalità corretta

Trasporto Questa impostazione controlla quale metodo di trasporto verrà utilizzato per comunicare con il server LDAP. La prima, e di default, selezione è *TCP - Standard* che utilizza connessioni TCP semplice sulla porta 389. Una scelta più sicura, se il server LDAP la supporta, è *SSL - Criptato* sulla porta 636. La scelta SSL crittograferà le query LDAP fatte al server, questo è particolarmente importante se il server LDAP non è su un segmento di rete locale.

Nota: Si raccomanda sempre di usare sempre SSL dove possibile, anche se il TCP semplice è più facile da configurare e diagnosticare dal momento che la cattura di un pacchetto mostrerebbe il contenuto delle query e le risposte.

Autorità di certificazione peer Se *SSL - Criptato* è stato scelto per il **Trasporto**, allora il valore di questo selettore viene utilizzato per convalidare il certificato del server LDAP. La CA selezionata deve corrispondere alla CA configurata sul server LDAP, altrimenti sorgeranno problemi. Per ulteriori informazioni sulla creazione o sul l'importazione di CA, consultare la *gestione dell'autorità di certificazione*.

Versione del protocollo Sceglie quale versione del protocollo LDAP è utilizzata dal server LDAP, sia *2* o *3*, di solito *3*.

Scopo della ricerca Determina dove, e quanto in profondità, una ricerca opererà per trovare una corrispondenza.

Livello Scegli tra il *livello 1* o *intero inferiore a tre* per controllare quanto in profondità andrà la ricerca. L'*intero inferiore a tre* è la scelta migliore quando la decisione non è certa ed è quasi sempre necessaria per le configurazioni di Active Directory.

DN di base Controlla dove la ricerca inizierà. Tipicamente impostato su «Root» della struttura LDAP, ad esempio DC=esempio,DC=com.

Contenitori di autenticazione Un elenco separato da un punto e virgola di potenziali conti o contenitori. Questi contenitori saranno preimpostati alla ricerca DN di base di sopra o specificare un percorso contenitore completo qui e lasciare la DN di base in bianco. Se il server LDAP lo supporta, e le impostazioni di bind sono corrette, fare clic sul pulsante **Selezionare** per sfogliare i contenitori del server LDAP e selezionarli lì. Alcuni esempi di questi contenitori sono:

- – `CN=Utenti;DC=esempio;DC=com` Questo cercherebbe gli utenti

  all'interno del dominio il componente *esempio.com*, una sintassi comune da vedere per la Active Directory

- – `CN=Utenti,DC=esempio,DC=com;OU=AltriUtenti,DC=esempio,DC=com`

  Questo cercherebbe in due luoghi diversi, il secondo dei quali è limitato all'unità organizzativa di altri utenti

  Query estesa Specifica una restrizione aggiuntiva alla ricerca del nome utente, che permette di usare il membro del gruppo come filtro. Per impostare una query estesa, selezionare la casella e riempire il valore con un filtro come:

  ```
  memberOf=CN=VPNUsers,CN=Users,DC=example,DC=com
  ```

  Credenziali Bind Controlla come questo client LDAP tenterà di collegarsi al server. Per impostazione predefinita la casella **Usare vincoli anonimi per risolvere nomi distinti** è selezionata per eseguire un bind anonimo. Se il server richiede l'autenticazione per effettuare una query, deselezionare quella casella e quindi specificare una **DN utente** e una **password** da usare per la bind.

Nota:

La Active Directory richiede tipicamente l'uso di credenziali di bind e può essere necessario un account di servizio o un amministratore equivalente a seconda della configurazione del server. Consultare la documentazione di Windows per determinare ciò è necessario in un ambiente specifico.

Modello iniziale pre-riempie le opzioni rimanenti nella pagina con i valori predefiniti comuni per un dato tipo di server LDAP. Le scelte includono *OpenLDAP* , *Microsoft AD* , e *Novell eDirectory*.

Attributo di denominazione utente L'attributo utilizzato per identificare il nome di un utente, più comunemente *cn* o *samAccount- Nome*.

Attributo di denominazione di gruppo L'attributo utilizzato per identificare un gruppo, come *cn*.

Attributo di un membro del gruppo L'attributo di un utente che significa che è il membro di un gruppo, come *membro*, *membroUid*, *membroDi* o *membroUnico*.

Gruppi RFC2307 Specifica come l'appartenenza al gruppo è organizzata sul server LDAP. Quando non è selezionata, l'appartenenza al gruppo in stile Active Directory viene usata quando i gruppi sono elencati come attributo dell'oggetto utente. Se selezionata, l'appartenenza al gruppo in stile RFC 2307 viene usata dove gli utenti sono elencati come membri dell'oggetto gruppo.

Nota:

Quando questo viene utilizzato, l'attributo membro del gruppo può anche bisogno cambiato, tipicamente sarebbe impostato su `memberUid` in questo caso, ma può variare per schema LDAP

Classe dell'oggetto del gruppo Usato con i gruppi di stile RFC 2307, specifica la classe di oggetti del gruppo, tipicamente posixGruppo ma può variare in base allo schema LDAP. Non è necessario per gruppi di stile Active Directory.

Codifica UTF8 Se selezionata, le query al server LDAP saranno codificate UTF8 e le risposte saranno decodificate UTF8. Il supporto varia a seconda del server LDAP. Generalmente necessario solo se nomi utente, gruppi, password e altri attributi contengono caratteri non tradizionali.

Alterazioni del nome utente Quando non è selezionata, un nome utente dato come utente@nomehost rimuoverà la porzione @nomehost in modo che solo il nome utente venga inviato nella richiesta di bind LDAP. Se selezionata, il nome utente viene inviato per intero.

- Fare clic su **Salvare** per creare il server.
- Visitare **Diagnostica>Autenticazione** per testare il server LDAP utilizzando un account valido.

Se la query LDAP restituisce correttamente l'elenco di gruppo per un utente, e i gruppi esistono localmente, i gruppi saranno elencati sui risultati quando si utilizza la pagina **Diagnostica>Autenticazione** per testare un account. Se i gruppi non si presentano, assicurarsi che esistano su Firew4LL con i nomi corrispondenti e che sia selezionata la struttura del gruppo (ad es. i gruppi RFC 2703 devono essere selezionati)

9.3 Esempi di autenticazione esterna

Ci sono innumerevoli modi per configurare il gestore utente per connettersi a un server esterno RADIUS o LDAP, ma ci sono alcuni metodi comuni che possono essere utili da usare come guida. Di seguito sono riportati tutti gli esempi testati/funzionanti, ma la configurazione del server probabilmente varia dall'esempio

9.3.1 Esempio di server RADIUS

Questo esempio è stato fatto contro FreeRADIUS, ma fare lo stesso per Windows Server sarebbe identico. Vedere *Autenticazione RADIUS con Windows Server* per informazioni sulla configurazione di un server Windows per RADIUS.

Questo presuppone che il server RADIUS sia già stato configurato per accettare query da questo firewall come client con un segreto condiviso.

Nome descrittivo ExCoRADIUS

Genere *Raggio*

Hostname o indirizzo IP 192.2.0.5

Segreto condiviso segretosegreto

Servizi offerti *Autenticazione e contabilitazione*

Porta di autenticazione 1812

Porta di contabilitazione 1813

Timeout di autenticazione 10

9.3.2 Esempio OpenLDAP

In questo esempio, Firew4LL è impostato per connettersi a un server OpenLDAP aziendale.

Nome descrittivo ExCoLDAP

Genere *LDAP*

Hostname o indirizzo IP ldap.esempio.com

Porta 636

Trasporto *SSL - Encrypted*

Autorità del certificate peer *ExCo CA*

Versione protocollo *3*

Ambito della ricerca `*Intero subtree*, dc=firew4ll, dc=org`

Contenitori dell'autenticazione `CN=pfsgruppo; ou=people, dc=firew4ll, dc=org`

Credenziali bind Bind anonimo *Selezionato*

Modello iniziale *OpenLDAP*

Attributo di denominazione utente cn

Attributo di denominazione di gruppo cn

Attributo del membro del gruppo memberUid

Gruppi RFC2307 Selezionato

Classe dell'oggetto del gruppo posixGroup

Codifica UTF8 *Selezionato*

Alterazioni del nome utente *Non selezionato*

9.3.3 Esempio della LDAO della Active Directory

In questo esempio, Firew4LL è impostato per connettersi ad una struttura di Active Directory al fine di autenticare gli utenti per una VPN. I risultati sono limitati al gruppo **Utenti VPN**. Omettere la query estesa per accettare qualsiasi utente.

Nome descrittivo ExCoADVPN

genere *LDAP*

Hostname o indirizzo IP 192.0.2.230

Porta 389

Trasporto *TCP - standard*

Protocol Version *3*

Ambito di ricerca *Intero subtree*, DC=dominio, DC=locale

Contenitori di autenticazione `CN=Utenti, DC=dominio, DC=locale`

Query estese `memberof=CN=UtentiVPN,CN=UtentiDC=esempio,DC=com`

Credenziali bind bind anonimp *Selezionata*

Utente DN CN=binduser,CN=Users,DC=domain,DC=local

Password segretosegreto

Modello iniziale *Microsoft AD*

Attributo della denominazione utente samAccountNome

Attributo della denominazione del gruppo *cn*

Attributo del membro del gruppo *memberOf*

Questo esempio utilizza TCP semplice, ma se l'autorità di certificazione per la struttura AD viene importato sotto il gestore del certificato in Firew4LL, SSL può essere utilizzato anche selezionando tale opzione e scegliendo il CA appropriato dall'elenco a discesa delle autorità di certificazione peer, e impostare l'hostname al nome comune del certificato server.

9.4 Risoluzione dei problemi

È possibile testare i server di autenticazione utilizzando lo strumento di **Diagnostica>Autenticazione**. Da quella pagina, testare un utente è semplice:

- Passare alla **Diagnostica>Autenticazione**
- Selezionare un **Server di autenticazione**
- Inserire un **nome utente**
- Inserire una **password**
- Fare clic sul pulsante **Provare**.

Il firewall tenterà di autenticare l'utente dato rispetto al server specificato e restituirà il risultato. Di solito è meglio provare questo almeno una volta prima di tentare di utilizzare il server.

Se il server restituisce un set di gruppi per l'utente, e i gruppi esistono localmente coActive Directoryn lo stesso nome, i gruppi vengono stampati nei risultati del test.

Se si riceve un errore durante il test di autenticazione, controllare le credenziali e le impostazioni del server, quindi effettuare le modifiche necessarie e riprovare.

9.4.1 Errori di LDAP in Active Directory

L'errore più comune con l'accesso LDAP all'Active Directory è non specificare un utente bind corretto nel formato corretto. Se il solo nome utente non funziona, digitare il Nome distinti completo (DN) per l'utente bind, come CN=utentebind,CN=Utenti,DC=dominio,DC=locale.

Se il DN completo dell'utente è sconosciuto, può essere trovato navigando fino all'utente in **Modificare ADSI** trovato sotto **Strumenti amministrativi** sul server Windows.

Un altro errore comune con l'appartenenza al gruppo è non specificare l'*intero inferiore-3* per il livello di ricerca.

9.4.2 Appartenenza a un Gruppo in Active Directory

A seconda di come sono stati creati i gruppi in Active Directory, il modo in cui sono specificati può essere diverso per cose come i Contenitori di autenticazione e/o le Query estese. Ad esempio, un gruppo di utenti tradizionale in AD è esposto in modo diverso alla LDAP rispetto a un'unità organizzativa separata. Modificare ADSI trovato sotto Strumenti amministrativi sul server Windows può essere utilizzato per determinare ciò che serà il DN per un dato gruppo.

9.4.3 Query estesa

L'errore più comune di una Query estesa è che la direttiva in questione non include né l'oggetto della ricerca né il modo in cui ricercare, come: `memberOf=CN=VPNUsers,CN=Users,DC=example,DC=com`

Si noti che nell'esempio sopra il DN del gruppo è dato insieme con la restrizione (memberOf=)

9.4.4 Risoluzione dei problemi tramite i registri log

I guasti di autenticazione sono tipicamente registrati dal server di destinazione (freeRADIUS, Windows Event Viewer, ecc.), assumendo che la richiesta stia facendo tutta la strada per l'host di autenticazione. Controllare i registri del server per una spiegazione dettagliata perché una richiesta non è riuscita. Il registro di sistema su Firew4LL (**Stato>Registri di sistema**) può anche contenere alcuni dettagli che accennano ad una risoluzione.

9.4.5 Risoluzione dei problemi tramite la cattura dei pacchetti

La cattura dei pacchetti può essere inestimabile per diagnosticare pure gli errori. Se un metodo non crittografato (RADIUS, LDAP senza SSL) è in uso, la password effettiva in uso potrebbe non essere visibile, ma abbastanza del protocollo di scambio può essere visto per determinare perché una richiesta non si riesce a completare.

Questo è particolarmente vero quando una cattura viene caricata in wireshark, che si possono interpretare le risposte, come si vede in Figura *Esempio della cattura fallita LDAP* Per ulteriori informazioni sulle catture di pacchetti, vedere Cattura di pacchetti.

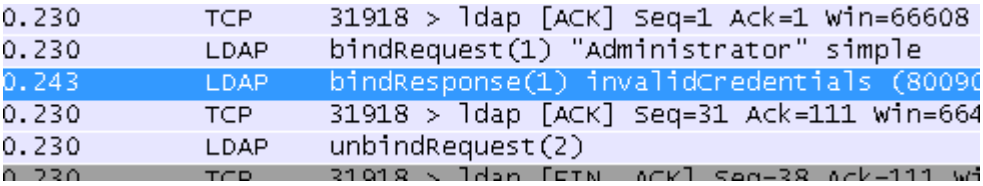


Fig. 1: Esempio della cattura fallita LDAP

Il gestore utente in Firew4LL fornisce la possibilità di creare e gestire più account utente. Questi account possono essere utilizzati per accedere alla GUI, utilizzare i servizi VPN come OpenVPN e IPsec, e utilizzare il Captive Portal.

Il Gestore Utente può essere utilizzato anche per definire fonti di autenticazione esterne come RADIUS e LDAP.

Vedi anche:

Per ulteriori informazioni, è possibile accedere all'archivio Hangouts per visualizzare l'Hangout di febbraio 2015 sulla gestione utenti e Privilegi, e l'Hangout di agosto 2015 su RADIUS e LDAP.

9.4.6 Supporto per tutto Firew4LL

A partire da questa documentazione, non tutte le aree di Firew4LL si collegano nuovamente alla Gestione utenti.

GUI di |firew4ll| Sostiene gli utenti nela Gestione utenti, e via RADIUS o LDAP. I gruppi o gli utenti di RADIUS o LDAP richiedono definizioni nel gestore utente locale per gestire i loro permessi di accesso.

OpenVPN Supporta gli utenti della Gestione utenti, RADIUS o LDAP tramite la gestione utenti.

IPsec Supporta gli utenti nella Gestione utenti, RADIUS o LDAP tramite la gestione utenti per xauth, e RADIUS per IKEv2 con EAP-RADIUS.

Captive portal Supporta gli utenti locali in Gestione utenti, e gli utenti RADIUS tramite le impostazioni nella pagina Portale captive.

L2TP Supporta gli utenti nelle impostazioni L2TP, e via RADIUS nelle impostazioni L2TP.

Server PPPoE Supporta gli utenti nelle impostazioni PPPoE.

CAPITOLO 10

Gestione Certificati

10.1 Gestione dell'autorità dei certificati

Le autorità di certificazione (CA) sono gestite da **Sistema>Gestione certificati**, nella scheda **CA**. Da questa schermata i CA possono essere aggiunti, modificati, esportati o cancellati.

10.1.1 Creare una nuova autorità di certificazione

Per creare una nuova CA, avviare il processo come segue:

- Passare a **Sistema>Gestione certificazioni** nella scheda **CA**.
- Fare clic su **Aggiungere** per creare una nuova CA.
- Inserire un **nome descrittivo** per la CA. Questo è usato come etichetta per questa CA in tutta la GUI.
- Selezionare il metodo che meglio si adatti a come verrà generata la CA. Queste opzioni e ulteriori istruzioni sono nelle sezioni corrispondenti qui sotto:
  - Creare un'autorità di certificazione interna
  - Importare un'autorità di certificazione esistente
  - Creare un'autorità di certificazione intermedia

Creare un'autorità di certificazione interna

Il metodo più comune utilizzato da qui è quello di creare un'autorità di certificazione interna. Questo farà una nuova CA di root basata sulle informazioni inserite in questa pagina.

- Selezionare la **lunghezza della chiave** per scegliere come «forte» la CA è in termini di crittografia. Più lunga è la chiave, più sicura è. Tuttavia, i tasti più lunghi possono richiedere più tempo alla CPU per essere processati, quindi non è sempre saggio usare il valore massimo. Il valore predefinito di *2048* è un buon equilibrio.

- Selezionare un **algoritmo Digest** dall'elenco fornito. La migliore pratica attuale è usare un algoritmo più forte di SHA1, dove possibile. *SHA256* è una buona scelta.

  -.. note:: Alcune apparecchiature più vecchie o meno sofisticate, come ad esempio telefoni VoIP abilitati-VPN possono supportare solo SHA1 per l'algoritmo Digest. Consultare la documentazione del dispositivo per le specifiche.

- Digitare un valore di durata di vita per specificare il numero di giorni per i quali la CA sarà valida. La durata dipende dalle preferenze personali e le politiche del sito. Cambiare la CA spesso è più sicuro, ma è anche un problema di gestione in quanto richiederebbe la riedizione di nuovi certificati alla scadenza della CA. Per impostazione predefinita la GUI suggerisce di utilizzare 3650 giorni, che è di circa 10 anni.
- Digitare i valori per la sezione **Nome distinto** per i parametri personalizzati nella CA. Questi sono tipicamente riempiti con le informazioni di un'organizzazione, o nel caso di un individuo, le informazioni personali. Queste informazioni sono per lo più cosmetiche, utilizzate per verificare l'esattezza della CA e per distinguere l'CA dall'altra. Non devono essere utilizzati segni di punteggiatura e caratteri speciali.
  - Selezionare il **codice del paese** dall'elenco. Questo è il codice del paese riconosciuto-ISO, non un dominio di primo livello con hostname.
  - Indicare lo **Stato** o la **provincia** in modo completo, non abbreviato.
  - Inserire la **città**.
  - Indicare il nome dell'**organizzazione**, in genere il nome della società.
  - Inserire un **indirizzo email** valido.
  - Inserire il **nome comune** (CN). Questo campo è il nome interno che identifica la CA. A differenza di un certificato, il CN per una CA non ha bisogno di essere l'hostname, o qualcosa di specifico. Ad esempio, potrebbe essere chiamato *VPNCA* o *MiaCA*.

Nota: Anche se è tecnicamente valido, evitare l'uso di spazi nel CN.

- Fare clic su **Salvare**

Se vengono segnalati errori, ad esempio caratteri non validi o altri problemi di input, saranno descritti sullo schermo. Correggere gli errori, e tentare di salvare di nuovo.

Importa un'autorità di certificazione esistente

Se una CA esistente proveniente da una fonte esterna deve essere importata, è possibile farlo selezionando il **metodo** di *importazione di un'autorità di certificazione esistente*. Questo può essere utile in due modi: uno, per le CA realizzate utilizzando un altro sistema, e due, per le CA fatte da altri che devono essere affidabili.

- Inserire i **dati del certificato** per la CA. Per avere fiducia in una CA proveniente da un'altra fonte, sono richiesti solo i dati del certificato per la CA. È tipicamente contenuto in un file che termina con . *crt* o *.pem*. Sarebbe testo semplice, e racchiuso in un blocco come:

- Inserire la chiave di certificazione privata se si importa una CA esterna personalizzata, o una CA che è in grado di generare i propri certificati e liste di revoca dei certificati. Questo è tipicamente in un file che termina in *.key*. Sarebbero dati di testo semplice racchiusi in un blocco come

- Inserire il **Seriale** per il prossimo certificato se la chiave privata è stata inserita. Questo è essenziale. Una CA creerà certificati ciascuno con un numero di serie unico in sequenza. Questo valore controlla la seriale del prossimo certificato generato da questa CA. È essenziale che ogni certificato abbia una serie unica, o ci

saranno problemi in seguito con la revoca del certificato. Se il prossimo seriale è sconosciuto, cercare di stimare quanti certificati sono stati fatti dalla CA, e poi impostare il numero abbastanza alto perché una collisione sia improbabile.

- Fare clic su **Salvare**

Se vengono segnalati errori, ad esempio caratteri non validi o altri problemi di input, saranno descritti sullo schermo. Correggere gli errori, e tentare di salvare di nuovo.

Importazione di un'autorità di certificazione a catena o a nidificazione

Se la CA è stata firmata da un intermediario e non direttamente da un CA di root, può essere necessario importare insieme la CA di root e quella intermedia in un'unica voce, come:

Creare un'autorità di certificazione intermedia

Una CA intermedia creerà una nuova CA in grado di generare certificati, ma dipende da un'altra CA superiore ad essa. Per crearne uno, selezionare *Creare un'autorità di certificazione intermedia* dal menu a discesa **Metodo**.

Nota: Il CA di livello superiore deve essere già presente su Firew4LL (Creato o importato)

- Scegliere l'CA di livello superiore per firmare questa CA utilizzando l'elenco a discesa **Firmare l'autorità di certificazione**. Verranno mostrate solo le CA con chiavi private presenti, in quanto ciò è necessario per firmare correttamente questa nuova CA.
- Inserire i parametri rimanenti identici a quelli per la *creazione di un'autorità di certificazione interna*.

10.1.2 Modifica di un'autorità di certificazione

Dopo l'aggiunta di una CA, può essere modificata dall'elenco delle CA presenti nella **scheda Sistema>Gestione certificazioni** sulla scheda **CA**. Per modificare una CA, fare clic sull'icona  alla fine della riga. Lo schermo presentato permette di modificare i campi come se la CA fosse stata importata.

Per informazioni sui campi in questa schermata, vedere *Importare un'autorità di certificazione esistente*. Nella maggior parte dei casi lo scopo di questa schermata sarebbe quello di correggere il **Seriale** della CA, se necessario, o di aggiungere una chiave ad una CA importata in modo che possa essere utilizzata per creare e firmare certificati e CRL.

10.1.3 Esportare un'autorità di certificato

Dall'elenco delle CA di **Sistema>Gestione certificati** nella scheda **CA**, è possibile esportare il certificato e/o la chiave privata di una CA. Nella maggior parte dei casi la chiave privata di una CA non verrebbe esportata, a meno che non si stia trasferendo in una nuova sede o si stia effettuando un backup. Quando si utilizza la CA per una VPN o per altri scopi, esportare solo il certificato per la CA.

Avvertimento: Se la chiave privata di una CA entra nelle mani sbagliate, l'altra parte potrebbe generare nuovi certificati che sarebbero considerati validi contro la CA.

Per esportare il certificato per una CA, fare clic sull'icona  a sinistra. Per esportare la chiave privata per la CA, fare clic sull'icona  a destra. Spostare il puntatore del mouse sull'icona e un suggerimento mostrerà l'azione da eseguire per una facile conferma. I file verranno scaricati con il nome descrittivo della CA come nome del file, con l'estensione *.crt* per il certificato, e *.key* per la chiave privata.

10.1.4 Rimuovere un'autorità di certificazione

Per rimuovere una CA, prima deve essere rimossa dal servizio attivo.

- Controllare le aree che possono utilizzare una CA, come OpenVPN, IPsec, e pacchetti.
- Rimuovere le voci che utilizzano la CA o selezionare una diversa CA.
- Passare a **Sistema>Gestione certificati** nella scheda **CA**.
- Trovare la **CA** per eliminarla nell'elenco.
- Cliccare su  alla fine della riga per la CA.
- Cliccare OK nella finestra di conferma.

Se viene visualizzato un errore, seguire le istruzioni sullo schermo per correggere il problema e quindi riprovare.

10.2 Gestione certificati

I certificati sono gestiti dal **Sistema>Gestione certificati**, nella scheda **Certificati**. Da questa schermata i certificati possono essere aggiunti, modificati, esportati o cancellati.

10.2.1 Creare un nuovo certificato

Per creare un nuovo certificato, avviare il processo nel modo seguente:

- Passare a **Sistema>Gestione certificati** nella scheda **Certificati**.
- Fare clic su **Aggiungere** per creare un nuovo certificato.
- Immettere un **nome descrittivo** per il certificato. Questo è usato come etichetta per questo certificato per tutta la GUI.
- Selezionare il **metodo** che meglio si adatta a come verrà generato il certificato. Queste opzioni e ulteriori istruzioni sono nelle relative sezioni di seguito:
  - Importazione di un certificato esistente
  - Creare un certificato interno
  - Creare un Richiesta di firma del certificato

Importazione di un certificato esistente

Se un certificato esistente proveniente da una fonte esterna deve essere importato, può essere fatto selezionando il metodo di importazione di un certificato esistente. Questo può essere utile per i certificati che sono stati effettuati utilizzando un altro sistema o per i certificati che sono stati forniti da un terzo.

- Inserire i dati del certificato, questo è richiesto. È tipicamente contenuto in un file che termina con *.crt*. Sarebbe un testo semplice, e racchiuso in un blocco come: .. code-block:: none

  ——BEGIN CERTIFICATE—— [A bunch of random-looking base64-encoded data] ——END CERTIFICATE——

- Inserire i dati della **chiave privata** è anche necessario. Questo è in genere in un file con estensione *.key* .. code-block:: none

  ——BEGIN RSA PRIVATE KEY—— [A bunch of random-looking base64-encoded data] ——END RSA PRIVATE KEY——

- Cliccare su Salvare per completare il processo di importazione.

Se si verificano errori, seguire le istruzioni sullo schermo per risolverli. L'errore più comune è non incollare nella giusta parte del certificato o della chiave privata. Assicurasi di includere l'intero blocco, tra cui l'intestazione e il piè di pagina intorno i dati codificati.

10.2.2 Creare un certificato interno

Il **metodo** più comune è creare un certificato interno. Questo creerà un nuovo certificato utilizzando una delle autorità di certificazione esistente.

- Selezionare l'**autorità di certificazione** con cui verrà firmato il presente certificato. Solo una CA che ha una chiave privata presente può essere in questo elenco, in quanto la chiave privata è necessaria per la CA per firmare un certificato..
- Selezionare la **lunghezza della chiave** per scegliere come «forte» il certificato è in termini di crittografia. Più lunga è la chiave, più sicura è. Tuttavia, i tasti più lunghi possono richiedere più tempo alla CPU per essere processati, quindi non è sempre saggio usare il valore massimo. Il valore predefinito di *2048* è un buon equilibrio..
- Selezionare un **algoritmo Digest** dall'elenco fornito. La migliore pratica attuale è usare un algoritmo più forte di SHA1, dove possibile. *SHA256* è una buona scelta.

Nota: Alcune apparecchiature più vecchie o meno sofisticate, come ad esempio telefoni VoIP VPN abilitati possono supportare solo SHA1 per l'algoritmo Digest. Consultare la documentazione del dispositivo per le specifiche.

- Selezionare un **tipo di certificato** che corrisponda allo scopo del presente certificato.
  - Scegliere un **Certificato del server** se il certificato verrà utilizzato in un server VPN o server HTTPS. Questo indica ciò che all'interno del certificato può essere utilizzato in un ruolo di server, e nessun altro.

Nota: I certificati tipo server includono attributi dell'uso della chiave estesa che indicano che possono essere utilizzati per l'autenticazione del server così come l'OID 1.3.6.1.5.5.8.2.2 che viene utilizzato da Microsoft per significare che un certificato può essere utilizzato come intermediario IKE. Questi sono necessari per Windows 7 e successivamente per fidarsi del certificato del server per l'uso con alcuni tipi di VPN. Essi sono anche contrassegnati con un vincolo che indica che non sono una CA, e hanno impostato nsCertType su «server».

- Scegliere **Certificato utente** se il certificato può essere utilizzato in una capacità dell'utente finale, come un client VPN, ma non può essere utilizzato come server. Questo impedisce all'utente di usare il proprio certificato per impersonare un server.

Nota: I certificati di tipo utente includono attributi dell'uso della chiave estesa che indicano che possono essere utilizzati per l'autenticazione del client. Essi sono inoltre contrassegnati da un vincolo che indica che non si tratta di una CA.

- Scegliere l'**autorità di certificazione** per creare una CA intermedia. Un certificato generato in questo modo sarà subordinato alla CA scelta. Può creare i propri certificati, ma la CA della root deve anche essere inclusa quando viene usata. Questo è noto anche come «incatenamento»
- Digitare un valore di **durata di vita** per specificare il numero di giorni per i quali il certificato sarà valido. La durata dipende dalle preferenze personali e le politiche del sito. Cambiare il certificato spesso è più sicuro, ma è anche un problema di gestione in quanto richiede la riedizione di nuovi certificati quando scadono. Per impostazione predefinita la GUI suggerisce di utilizzare 3650 giorni, che sono circa 10 anni.
- Digitare i valori per la sezione **Nome distinto** per i parametri personalizzati nel certificato. La maggior parte di questi campi saranno pre-popolati con i dati della CA. Tali informazioni sono generalmente fornite con le informazioni di un'organizzazione, o nel caso di un individuo, informazioni personali. Queste informazioni sono per lo più cosmetiche, utilizzate per verificare l'esattezza del certificato e per distinguere un certificato da un altro. Non devono essere utilizzati segni di punteggiatura e caratteri speciali.
  - Selezionare il **codice paese** dalla lista. Questo è il codice ISO del paese riconosciuto, non un dominio di livello superiore con hostname.
  - Inserire lo **Stato** o **Provincia** scritto per intero, non abbreviato.
  - Inserire la **città**.
  - Inserire il nome dell'**organizzazione**, in genere il nome della società.
  - Inserire un **indirizzo email** valido.
  - Inserire il **nome comune** (CN). Questo campo è il nome interno che identifica il certificato. A differenza di una CA, il CN per un certificato dovrebbe essere un nome utente o nome dell'host. Ad esempio, potrebbe essere chiamato *certificatoVPN*, *utente01*, o *vpnrouter.esempio.com*.

Nota: Anche se è tecnicamente valido, evitare l'uso di spazi nel CN.

- Fare clic su  **Aggiungere** per **Aggiungere nomi alternativi** se necessari. I nomi alternativi consentono al certificato di specificare più nomi che sono tutti validi per il NC, come due nomi host diversi, un indirizzo IP aggiuntivo, un URL, o un indirizzo e-mail. Questo campo può essere lasciato vuoto se non è richiesto o se il suo scopo non è chiaro.
  - Inserire un **Tipo** per il nome alternativo. Questo deve contenere uno dei *DNS* (FQDN o hostname), *IP* (indirizzo IP), *URI*, o *e-mail*.
  - Immettere un **Valore** per il Nome alternativo. Questo campo deve contenere un valore opportunamente formattato in base al tipo immesso.
  - Cliccare  **Eliminare** alla fine della riga per un Nome alternativo non necessario.
  - Ripetere questa procedura per ogni ulteriore **Nome alternativo**.
- Fare clic su **Salvare**

Se vengono segnalati errori, come caratteri non validi o altri problemi di input, essi saranno descritti sullo schermo. Correggere gli errori e tentare di salvare di nuovo.

Crea una richiesta di firma del certificato

La scelta di un **metodo** di *richiesta di firma di certificato* crea un nuovo file di richiesta che può essere inviato a una CA di terze parti da firmare. Questo dovrebbe essere utilizzato per ottenere un certificato da un'autorità di certificazione root di fiducia. Una volta scelto questo metodo, i parametri rimanenti per la creazione di questo certificato sono identici a quelli per la *creazione di un certificato interno*.

10.2.3 Esportare un certificato

Dall'elenco dei certificati di **Sistema>Gestione certificati** nella scheda **Certificati**, un certificato e/o la sua chiave privata possono essere esportati.

Per esportare il certificato, fare clic sull'icona  . Per esportare la chiave privata del certificato, fare clic sull'icona  . Per esportare il certificato della CA, il certificato e la chiave privata per il certificato insieme in un file PKCS#12, fare clic sull'icona  . Per confermare l'esportazione del file corretto, posizionare il puntatore del mouse sull'icona e un suggerimento mostrerà l'azione da eseguire.

I file verranno scaricati con il nome descrittivo del certificato come nome del file, e l'estensione *.crt* per il certificato e *.key* per la chiave privata, o . *P12* per un file PKCS#12.

10.2.4 Rimuovere un certificato

Per rimuovere un certificato, prima deve essere rimosso dall'uso attivo.

- **Selezionare** le aree che possono utilizzare un certificato, come ad esempio le opzioni di WebGUI, OpenVPN, IPsec, e pacchetti.
- Rimuovere le voci utilizzando il certificato, oppure scegliendo un altro certificato.
- Passare a **Sistema>Gestione certificati** nella scheda **Certificati**.
- Individuare il certificato da eliminare nella lista
- Cliccare su  alla fine della riga per il certificato.
- Fare clic su OK nella finestra di conferma.

Se viene visualizzato un errore, seguire le istruzioni sullo schermo per correggere il problema e quindi riprovare.

10.2.5 Certificati dell'utente

Se viene utilizzata una VPN che richiede certificati utente, essi possono essere creati in uno dei diversi modi. Il metodo esatto dipende da dove viene eseguita l'autenticazione per la VPN e se il certificato esiste già o meno.

Nessuna autenticazione o autenticazione esterna

Se non c'è un'autenticazione utente, o se l'autenticazione utente viene eseguita su un server esterno (RADIUS, LDAP, ecc) allora fare un certificato utente come qualsiasi altro certificato descritto in precedenza. Assicurarsi che il certificato utente sia selezionato per il tipo di certificato e che il nome comune sia il nome utente dell'utente.

Autenticazione locale/Creare certificato quando si crea un utente

Se l'autenticazione utente viene eseguita su Firew4LL, il certificato utente può essere fatto all'interno della gestione degli utenti.

- Passare a **Sistema>Gestione utenti**
- Creare un utente. Vedere *Gestione utenti e autenticazione* per dettagli.
- Compilare il **nome utente** e la **password**
- Selezionare **Fare clic per creare un certificato utente** nella sezione certificati utente, che mostrerà una forma semplice per la creazione di un certificato utente.
  - Inserire una breve **Nome descrittivo**, che può essere il nome utente o qualcosa come *accesso remoto al certificato della VPN di Bob*.
  - Scegliere l'**autorità di certificazione** adeguata per la VPN.
  - Regolare la **lunghezza della chiave** e **la durata di vita** se lo si desidera.
- Finire gli altri dettagli utente necessari.
- Fare clic su **Salvare**

Autenticazione locale/aggiungere un certificato a un utente esistente

Per aggiungere un certificato a un utente esistente:

- Passare a **Sistema> Gestione utenti**
- Cliccare su  per modificare l'utente
- Cliccare su  **Aggiungere** sotto i certificati utente.
- Scegliere le opzioni disponibili in base alle esigenze del processo di creazione del certificato descritto in *Creare un nuovo certificato*, o selezionare *Scegliere un certificato esistente* e quindi selezionare uno dei **certificati esistenti**

Per ulteriori informazioni su come aggiungere e gestire utenti, vedere *Gestione utenti e autenticazione*.

10.3 Gestione degli elenchi di revoca dei certificati

Le liste di revoca dei certificati (CRL) fanno parte del sistema X.509 che pubblica elenchi di certificati che non dovrebbero più essere attendibili. Tali certificati possono essere stati compromessi o essere altrimenti invalidati. Un'applicazione che utilizza una CA, come OpenVPN, può opzionalmente utilizzare una CRL in modo da poter verificare i certificati dei client di connessione. Una CRL è generata e firmata contro una CA utilizzando la sua chiave privata, quindi per creare o aggiungere certificati a una CRL nella GUI, la chiave privata della CA deve essere presente. Se la CA è gestita esternamente e la chiave privata per la CA non è sul firewall, una CRL può ancora essere generata al di fuori del firewall e importata.

Il modo tradizionale di utilizzare una CRL è quello di avere solo una CRL per CA e solo aggiungere certificati non validi a tale CRL. In Firew4LL, tuttavia, possono essere create più CRL per una singola CA. In OpenVPN, possono essere scelte diverse CRL per istanze VPN separate. Ciò potrebbe essere utilizzato, ad esempio, per impedire ad un certificato specifico di connettersi ad un'istanza mentre gli consente di collegarsi ad un'altra. Per IPsec, tutte le CRL sono consultate e non c'è nessuna selezione come attualmente esiste con OpenVPN.

Le liste di revoca dei certificati sono gestite da **Sistema>Gestione certificati**, nella scheda **Revoca dei certificati**. Da questa schermata le voci della CRL possono essere aggiunte, modificate, esportate o cancellate. L'elenco mostrerà tutte le autorità di certificazione e un'opzione per aggiungere una CRL. Lo schermo indica anche se la CRL è interna o esterna (importata) e mostra il numero di certificati revocati su ciascuna CRL.

Nota: Le CRL generate con Firew4LL 2.2.4-RELEASE e versioni

successive includono l'attributo identificativo della chiave amministrativa per consentire la corretta funzionalità con strongSwan per l'uso con IPsec.

10.3.1 Creare una nuova lista di revoca dei certificati

Per creare una nuova CRL:

- Passare a Sistema>Gestione certificati, nella scheda revoca dei certificati.
- Trovare la riga con la CA per cui la LCR verrà creata.
- Cliccare **Aggiungere** o **Importare la CRL** alla fine della riga per creare una nuova CRL.
- Scegli **Creare una lista di revoche di certificato interna** per il **metodo**.
- Inserire un **nome descrittivo** per la CRL, che viene utilizzato per identificare questa CRL nelle liste in tutta la GUI. Di solito è meglio includere un riferimento al nome della CA e/o lo scopo della CRL.
- Selezionare la CA appropriata dal menu a discesa delle **Autorità di certificazione**.
- Inserire il numero di giorni per i quali la CRL dovrebbe essere valida nella casella della **durata di vita**. Il valore di default è *9999*
- giorni, o anni quasi 27 e mezzo.
  - Fare clic su **Salvare**

Il browser farà ritorno alla lista CRL, e la nuova voce verrà mostrata lì.

10.3.2 Importare una lista di revoca dei certificati esistenti

Per importare una CRL da una fonte esterna:

- Passare a **Sistema>Gestione certificati**, nella scheda di **revoche di certificati**
- Trovare la riga con la CA per cui la LCR sarà importata.
- Cliccare su **Aggiungere** o **Importare la CRL** alla fine della riga per creare una nuova CRL.
- Selezionare **Importare una lista della revoca dei certificati esistente** per il **metodo**.
- Inserire un **nome descrittivo** per la CRL, che viene utilizzata per identificare questa CRL nelle liste in tutta la GUI. Di solito è meglio includere un riferimento al nome della CA e/o lo scopo della CRL.
- Selezionare la CA appropriata dal menu a discesa **Autorità di certificazione**.
- Inserire i **dati della CRL**. Questo è di solito in un file che termina in *.crl*. Sarebbero dati di testo semplice racchiusi in un blocco come:
- Fare clic su **Salvare** per completare il processo di importazione.

Se appare un errore, seguire le istruzioni sullo schermo per correggere il problema e quindi riprovare. L'errore più comune è non incollare nella parte giusta dei dati della CRL. Accertarsi di inserire l'intero blocco, compresi l'intestazione iniziale e il piè di pagina finale dei dati codificati.

10.3.3 Esportare una lista di revoche di certificati

Dall'elenco della CRL di **Sistema>Gestione certificazioni** nella scheda **Revoca del certificato** può essere esportata anche una CRL. Per esportare la CRL, fare clic sull'icona  . Il file verrà scaricato con il nome descrittivo della CRL come il nome del file, e l'estensione *.crl*.

10.3.4 Eliminare un elenco di revoche di certificati

- Controllare le aree che possono utilizzare la CRL, come OpenVPN.
- Rimuovere le voci utilizzando la CRL, o scegliere un'altra CRL.
- Passare a **Sistema>Gestione certificazione** nella scheda **revoca dei certificati**.
- Individuare la CRL per eliminare nell'elenco
- Cliccare sull'icone  alla fine della riga della CRL.
- Fare clic su OK nella finestra di conferma.

Se viene visualizzato un errore, seguire le istruzioni sullo schermo per correggere il problema e quindi riprovare.

10.3.5 Revocare un certificato

Una CRL non è molto utile se non contiene certificati revocati. Un certificato viene revocato aggiungendolo in una CRL:

- Passare a **Sistema>Gestione certificati** nella scheda **revoca dei certificati**.
- Individuare la CRL da modificare nella lista
- Cliccare l'icona  alla fine della riga della CRL. Verrà presentata una schermata che elenca tutti i certificati attualmente revocati, e un controllo per aggiungerne di nuovi.
- Selezionare il certificato dalla lista **Scegliere un certificato da revocare**.
- Selezionare un **motivo** dall'elenco a discesa per indicare il motivo per cui il certificato è stato revocato. Queste informazioni non pregiudicano la validità del certificato, sono semplicemente di natura informativa. Questa opzione può essere lasciata al valore di default.
- Fare clic su **Aggiungere** e il certificato verrà aggiunto alla CRL.

  I certificati possono essere rimossi dalla CRL utilizzando pure questa schermata:

- Passare a **Sistema>Gestione certificati** nella scheda **revoca dei certificati**.
- Individuare la CRL da modificare nella lista
- Cliccare l'icona  alla fine della riga della CRL.
- Trovare il certificato nell'elenco e fare clic sull'icona  per rimuoverlo dalla CRL.

- Fare clic su **OK** nella finestra di conferma.

Dopo l'aggiunta o la rimozione di un certificato, la CRL sarà ri-scritta se è attualmente in uso da parte di tutte le istanze della VPN in modo che i cambiamenti della CRL saranno immediatamente attive.

10.3.6 Aggiornamento di una lista di revoche di certificati importata

Per aggiornare una CRL importata:

- Passare a **Sistema>Gestione certificati** nella scheda **revoca dei certificati**.
- Individuare la CRL da modificare nella lista
- Cliccare sull'icona  alla fine della riga della CRL.
- Cancellare il contenuto incollato nella casella dei **dati della CRL** e sostituirlo con il contenuto della nuova CRL
- Fare clic su **Salvare**.

Dopo l'aggiornamento della CRL importata, sarà ri-scritta se è attualmente in uso da parte di tutte le istanze della VPN in modo che i cambiamenti della CRL saranno immediatamente attive.

10.4 Introduzione di base all'infrastruttura a chiave pubblica X.509

Un'opzione di autenticazione per le VPN è quella di usare le chiavi X.509. Una discussione approfondita sulle infrastrutture X.509 e le chiavi pubblicje (PKI) esula dall'ambito di questo libro ed è l'argomento di un certo numero di libri interi per gli interessati ai dettagli. Questo capitolo fornisce la comprensione di base necessaria per la creazione e la gestione dei certificati in Firew4LL.

Con le PKI, viene creata prima un'autorità di certificazione (CA). Questa CA firma poi tutti i singoli certificati nella PKI. Il certificato della CA viene utilizzato sui server e sui client VPN per verificare l'autenticità dei certificati server e dei client utilizzati. Il certificato per la CA può essere utilizzato per verificare la firma dei certificati, ma non per firmare i certificati. La firma dei certificati richiede la chiave privata per la CA. La segretezza della chiave privata della CA è ciò che garantisce la sicurezza di una PKI. Chiunque abbia accesso alla chiave privata della CA può generare certificati da utilizzare su una PKI, quindi deve essere mantenuta sicura. Questa chiave non è mai distribuita a client o server.

Avvertimento: Non copiare mai più file sui client di quelli necessari, in quanto questo potrebbe compromettere la sicurezza della PKI.

Un certificato è considerato valido se è attendibile per una data CA. Nel caso delle VPN, ciò significa che un certificato rilasciato da una CA specifica sarebbe considerato valido per qualsiasi VPN che utilizza tale CA. Per questo motivo la migliore pratica è quella di creare una CA unica per ogni VPN che ha un diverso livello di sicurezza. Per esempio, se ci sono due VPN di accesso mobile con lo stesso accesso di sicurezza, usare la stessa CA per quelle VPN è OK. Tuttavia se una VPN è per gli utenti e un'altra VPN è per la gestione remota, ognuna con restrizioni diverse, allora dovrebbe essere usata una CA unica per ogni VPN.

Le liste di revoca dei certificati (CRL) sono elenchi di certificati che sono stati compromessi o che altrimenti devono essere invalidati. La revoca di un certificato può essere considerata non attendibile a condizione che l'applicazione che utilizza la CA utilizzi anche una CRL. Le CRL sono generate e firmate contro una CA utilizzando la sua chiave privata, quindi per creare o aggiungere certificati a una CRL nella GUI la chiave privata per una CA deve essere presente.

CAPITOLO 11

Backup e ripristino

11.1 Effettuare il backup dalla WebGUI

Fare un backup dalla WebGUI è semplice.

- Accedere a **Diagnostica>Backup e ripristino**
- Impostare l'**area di backup** su *TUTTI* (la scelta di default)
- Impostare le opzioni desiderate, come ad esempio **Ignorare RRD** e **Crittografia**
- Fare clic su **Scaricare la configurazione in formato XML** (Figura *WebGUI di riserva*).

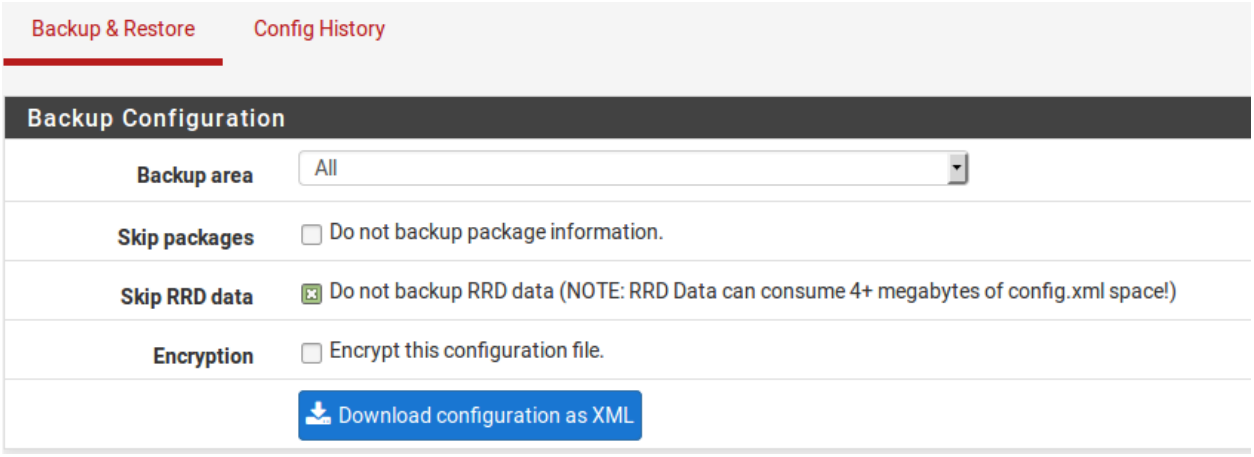


Fig. 1: Backup dalla WebGUI

Il browser web chiederà quindi di salvare il file da qualche parte sul PC utilizzato per visualizzare la WebGUI. Sarà chiamato config-hostname>-timestamp>.xml, ma che può essere cambiato prima di salvare il file.

11.2 Usare il pacchetto per il Backup di configurazione automatica (AutoConfigBackup)

La informazioni più aggiornate su AutoConfigBackup si possono trovare sulla pagina di documentazione di Firew4LL sul pacchetto AutoConfigBackup

11.2.1 Funzionalità e vantaggi

Quando un cambiamento nella configurazione del firewall è fatto, viene crittografato automaticamente con la passphrase immesso nella configurazione del pacchetto e caricato su HTTPS ai server AutoConfigBackup. Solo configurazioni criptate vengono conservate sui server AutoConfigBackup. Questo dà un istantaneo, sicuro backup off-site dei file di configurazione del firewall senza alcun intervento da parte dell'utente una volta che il pacchetto è configurato.

11.2.2 Compatibilità con la versione di Firew4LL

Il pacchetto AutoConfigBackup funziona con tutte le versioni supportate di Firew4LL

11.2.3 Installazione e configurazione

Per installare il pacchetto:

- Passare a **Sistema>Gestione pacchetto**, scheda **Pacchetti disponibili**
- Individuare **AutoConfigBackup** nella lista
- Fare clic su **Installare** alla fine della voce AutoConfigBackup
- Cliccare **Confermare** per confermare l'installazione

Il firewall quindi scarica e installa il pacchetto. Una volta installato, il pacchetto può essere trovato nel menu sotto Diagnostica> AutoConfigBackup

Impostare hostname

Assicurarsi di configurare un hostname unico e un dominio su**Sistema>Impostazioni generali**. Le voci di configurazione in AutoConfigBackup sono memorizzate da FQDN (Nome di dominio pienamente qualificato + dominio, ad esempio hostname + dominio), quindi ogni firewall sottoposto a backup deve avere un FQDN unico, altrimenti il sistema non può distinguere tra più installazioni.

Configurare AutoConfigBackup

Il pacchetto è configurato in **Diagnostica> AutoConfigBackup**. Nella scheda **Impostazioni**, compilare le impostazioni come segue:

Nome utente dell'abbonamento Il nome utente per l'account dell'abbonamento di Firew4LL

Password/Conferma dell'abbonamento La password per l'account dell'abbonamento di Firew4LL

Password/Conferma con crittografia Una passphrase arbitraria usata per crittografare la configurazione prima del caricamento. Questa dovrebbe essere una password lunga e complessa per garantire la sicurezza della configurazione. I server AutoConfigBackup contengono solo copie criptate, che sono inutili senza questa p**assword di crittografia**

> **Avvertimento:** E' importante che la password di crittografia sia ricordata o salvata in modo sicuro al di fuori del firewall. Senza la password di crittografia, il file di configurazione non può essere recuperato e la password di crittografia non viene memorizzata sul server al di fuori del file di configurazione.

Testare le funzionalità di backup

Effettuare una modifica per forzare un backup di configurazione, come modificare e salvare un firewall o una regola NAT, quindi fare clic su **Applicare modifiche**. Visitare **Diagnostica>AutoConfigBackup**, scheda **Ripristinare**, che elencherà i backup disponibili con la pagina che ha fatto la modifica (se disponibile)..

Effettuare il backup manuale

I backup manuali dovrebbero essere effettuati prima di un aggiornamento o di una serie di modifiche significative, in quanto memorizza un backup specificamente, mostrando il motivo, che rende quindi facile da ripristinare, se necessario. Dal momento che ogni modifica di configurazione innesca un nuovo backup, quando una serie di modifiche è fatto, può essere difficile sapere dove il processo è iniziato.

Per forzare un backup manuale della configurazione:

- Accedere a **Diagnostica> AutoConfigBackup**
- Fare clic sulla scheda **Effettuare il backup ora** nella parte superiore
- Inserire un **Motivo del backup**
- Fare clic su **Backup**

Ripristino di una configurazione

Per ripristinare una configurazione:

- Accedere a **Diagnostica> AutoConfigBackup**
- Fare clic sulla scheda **Ripristinare** in alto
- Individuare il backup desiderato nella lista
- Cliccare su  a destra della riga di configurazione

Il firewall scaricherà la configurazione specificata dal server AutoConfigBackup, la decripterà con la **password di criptazione** e la ripristinerà.

Per default, il pacchetto **non** avvierà un riavvio. A seconda degli elementi di configurazione ripristinati, un riavvio potrebbe non essere necessario. Ad esempio, il firewall e le regole NAT vengono ricaricati automaticamente dopo il ripristino di una configurazione. Dopo il ripristino, all'utente viene chiesto se desidera riavviare. Se la configurazione ripristinata cambia qualcosa delle regole NAT e firewall, scegliere **Sì** e permettere al firewall di riavviare.

11.2.4 Ripristino Bare Metal

Se il disco nel firewall fallisce, da subito la seguente procedura è necessaria per il recupero in una nuova installazione.

- Sostituire il disco guasto
- Installare Firew4LL sul nuovo disco

- Configurazione della LAN e della WAN, e assegnare l'hostname e il dominio esattamente come precedentemente configurato
- Installare il pacchetto **AutoConfigBackup**
- Configurare il pacchetto AutoConfigBackup come descritto sopra, utilizzando lo stesso account del portale e la stessa **password di crittografia** precedentemente utilizzata.
- Visitare la scheda **Ripristino**
- Scegliere la configurazione da ripristinare
- Quando viene richiesto di riavviare il sistema dopo il ripristino, farlo

Una volta che il firewall è stato riavviato, si sarà in esecuzione con la configurazione di backup prima del fallimento.

11.2.5 Controllo dello stato di AutoConfigBackup

Lo stato di un AutoConfigBackup eseguito può essere controllato rivedendo l'elenco dei backup mostrati nella scheda **Ripristino**. Questa lista è estratta dai server AutoConfigBackup. Se il backup è elencato lì, è stato creato con successo.

Se un backup non riesce, un avviso viene registrato, e sarà visibile nella WebGUI.

11.3 Tecniche alternative di backup remoto

Le seguenti tecniche possono anche essere utilizzate per eseguire backup a distanza, ma ogni metodo ha le sue caratteristiche di sicurezza che possono escludere il loro uso in molti luoghi. Per cominciare, queste tecniche non crittografano la configurazione, che può contenere informazioni sensibili. Ciò può comportare la trasmissione della configurazione su un collegamento non cifrato e non attendibile. Se si deve usare una di queste tecniche, è meglio farlo da un collegamento non WAN (LAN, DMZ, ecc.) o attraverso una VPN. L'accesso al supporto di memoria che contiene il backup deve essere controllato, se non criptato. Il pacchetto AutoConfigBackup è un mezzo molto più semplice e sicuro per automatizzare i backup remoti.

11.3.1 Recupero con wget

La configurazione può essere recuperata da un sistema remoto utilizzando wget , e questo processo può essere script con cron o con altri mezzi. Anche quando si utilizza HTTPS, questo non è un trasporto veramente sicuro in quanto il controllo del certificato è disabilitato per ospitare certificati auto-firmati, consentendo attacchi man-in-the-middle. Quando si eseguono backup con wget attraverso reti non affidabili, utilizzare HTTPS con un certificato che può essere verificato da wget.

Su Firew4LL il comando wget deve essere suddiviso in più passaggi per gestire la procedura di login e il download del backup, tenendo conto anche della verifica CSRF.

Per un firewall con HTTPS con certificato auto-firmato, il comando sarebbe il seguente:

- Inviare il modulo di login insieme al primo CSRF token e Salva il secondo CSRF token:

```
$ wget -qO- --keep-session-cookies --save-cookies cookies.txt \
--no-check-certificate https://192.168.1.1/diag_backup.php \
| grep "name=' csrf_magic'" | sed 's/.*value="\(.*\)".*/\1/' > csrf.txt
```

- Inviare il modulo di accesso con il primo token CSRF e salvare il secondo token CSRF:

```
$ wget -qO- --keep-session-cookies --load-cookies cookies.txt \
--save-cookies cookies.txt --no-check-certificate \
--post-data "login=Login&usernamefld=admin&passwordfld=firew4ll& csrf_magic=$(cat␣
↪csrf.txt)" \
https://192.168.1.1/diag_backup.php     | grep "name=' csrf_magic'" \
| sed 's/.*value="\(.*\)".*/\1/' > csrf2.txt
```

- Ora lo script è collegato e può agire. Inviare il modulo di download insieme al secondo token CSRF per salvare una copia di config.xml:

```
$ wget --keep-session-cookies --load-cookies cookies.txt --no-check-certificate \
--post-data "Submit=download&donotbackuprrd=yes& csrf_magic=$(head -n 1 csrf2.txt)
↪" \
https://192.168.1.1/diag_backup.php -O config-hostname-`date +%Y%m%d%H%M%S`.xml
```

Sostituire il nome utente e la password con le credenziali per il firewall, l'indirizzo IP può essere qualsiasi indirizzo IP è raggiungibile dal sistema di backup, e utilizzare HTTP o HTTPS per abbinare la GUI del firewall. Per il backup dei file RRD, omettere il parametro &donotbackuprrd=yes dall'ultimo comando.

Il sistema che esegue il backup avrà anche bisogno di accedere alla WebGUI, in modo da regolare le regole del firewall di conseguenza. Si sconsiglia di eseguire questa operazione sulla WAN. Come minimo, utilizzare HTTPS e limitare l'accesso alla WebGUI a un gruppo di indirizzi IP pubblici fidati. È preferibile farlo localmente o su una VPN.

11.3.2 «Spingere» con SCP

Il file di configurazione può anche essere spinto dal firewall Firew4LL ad un altro sistema UNIX con scp. Utilizzare scp per spingere un backup a mano una sola volta può essere utile, ma l'utilizzo in modo automatizzato comporta alcuni rischi. La riga di comando per scp varierà a seconda della configurazione del sistema, ma sarà simile alla seguente:

```
# scp /cf/conf/config.xml \
user@backuphost:backups/config-`hostname`-`date +%Y%m%d%H%M%S`.xml
```

Per spingere la configurazione in modo automatizzato, generare una chiave SSH senza una passphrase. A causa della natura insicura di una chiave senza una passphrase, generare una tale chiave viene lasciato come esercizio per il lettore. Questo aggiunge il rischio dovuto al fatto che chiunque abbia accesso a quel file ha accesso al conto designato, anche se, benché la chiave sia mantenuta sul firewall dove l'accesso è limitato, non è un rischio considerevole nella maggior parte degli scenari. Se questo viene fatto, assicurarsi che l'utente remoto sia isolato e abbia pochi o alcun privilegio sul sistema di destinazione.

Un ambiente chrooted scp può essere auspicabile in questo caso. La shell scponly è disponibile per la maggior parte delle piattaforme UNIX che permettono le copie di file SCP ma negano le funzionalità di login interattivo. Alcune versioni di OpenSSH hanno il supporto chroot per sftp (FTP Sicuro). Questi passaggi limitano notevolmente il rischio di compromissione rispetto al server remoto, ma lasciano comunque i dati di backup a rischio. Una volta configurato l'accesso, si può aggiungere una voce cron al sistema Firew4LL per richiamare scp. Per maggiori dettagli visitare la pagina Wiki della Documentazione Firew4LL o cercare sui forum.

11.3.3 Backup di base SSH

Simile al backup s**cp**, c'è un altro metodo che funzionerà da un sistema UNIX ad un altro. Questo metodo non invoca il livello SCP/SFTP, che in alcuni casi potrebbe non funzionare correttamente se un sistema è già in uno stato di fallimento:

```
$ ssh root@192.168.1.1 cat /cf/conf/config.xml > backup.xml
```

Una volta eseguito, questo comando produrrà un file chiamato backup.xml nella directory di lavoro corrente che contiene la configurazione del firewall remoto di Firew4LL. È anche possibile automatizzare questo metodo usando cron, ma questo metodo richiede una chiave SSH senza passphrase sull'host che esegue il backup. Questa chiave abilita l'accesso amministrativo al firewall, quindi deve essere strettamente controllata. (Vedere *Shell sicura (SSH)* per i dettagli).

11.4 Ripristino da backup

I backup non sono utili senza un mezzo per ripristinarli e, per estensione, per testarli. Firew4LL offre diversi mezzi per ripristinare le configurazioni. Alcuni sono più complessi di altri, ma ognuno avrà lo stesso risultato finale: un sistema in esecuzione identico a quando il backup è stato fatto.

11.4.1 Ripristino con la WebGUI

Il modo più semplice per la maggior parte degli utenti per ripristinare una configurazione è quello di utilizzare la WebGI:

- Accedere a **Diagnostica>Backup e ripristino**
- Individuare la sezione di **Ripristinare configurazione** (Figura *Ripristino con la WebGUI*).
- Selezionare la zona da ripristinare (tipicamente *TUTTI*)
- Fare clic su Sfogliare
- Individuare il file di backup sul PC locale
- Fare clic su **Ripristinare configurazione**

La configurazione sarà applicata, e il firewall verrà riavviato con le impostazioni ottenute dal file di backup.

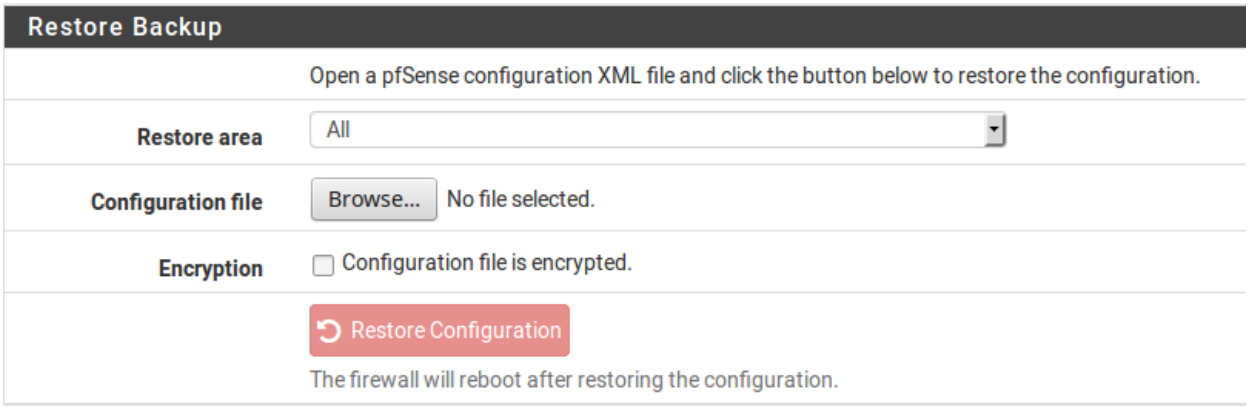


Fig. 2: Ripristino con la WebGUI

Sebbene sia facile da applicare, questo metodo ha bisogno di alcuni prerequisiti quando si tratta di un ripristino completo di un nuovo sistema. In primo luogo, dovrebbe essere fatto dopo che il nuovo sistema di destinazione è completamente installato e in esecuzione. In secondo luogo, richiede un PC aggiuntivo collegato a una rete di lavoro o un cavo di crossover dietro il firewall Firew4LL in fase di ripristino.

11.4.2 Ripristino dalla cronologia di configurazione

Per problemi minori, usare uno dei backup interni del firewall Firew4LL è il modo più semplice per annullare un cambiamento. Su installazioni complete, le 30 configurazioni precedenti vengono memorizzate nella cronologia di

configurazione, insieme alla configurazione corrente. Su NanoBSD sono memorizzate 5 configurazioni. Ogni riga mostra la data di creazione del file di configurazione, la versione di configurazione, l'utente e l'indirizzo IP di una persona che ha apportato una modifica alla GUI, la pagina che ha apportato la modifica e, in alcuni casi, una breve descrizione della modifica apportata. I pulsanti di azione a destra di ogni riga mostreranno una descrizione di ciò che fanno quando il puntatore del mouse è posizionato sopra il pulsante.

Per ripristinare una configurazione dalla cronologia:

- Accedere a **Diagnostica>Backup e ripristino**
- Fare clic sulla scheda **Cronologia di configurazione** (Figura *Cronologia di configurazione*).
- Individuare il backup desiderato nella lista
- Cliccare su  per ripristinare quel file di configurazione

La configurazione verrà ripristinata, ma il riavvio non è automatico dove richiesto. Modifiche minori non richiedono un riavvio, anche il ripristino di alcuni grandi cambiamenti lo vorrà.

Se una modifica è stata fatta solo in una sezione specifica, come le regole del firewall, attivare un aggiornamento in quell'area della GUI per abilitare le modifiche. Per le regole del firewall, sarebbe sufficiente ricaricare il filtro. Per OpenVPN, sarebbe sufficiente modificare e salvare l'istanza VPN. Le azioni necessarie da prendere dipendono da ciò che è cambiato nella configurazione, ma il modo migliore per garantire che la configurazione completa si attivi sarebbe un riavvio. Se necessario, riavviare il firewall con la nuova configurazione andando a **Diagnostics>Riavviare Sistema** e fare clic su **Sì**.

Le configurazioni precedentemente salvate possono essere cancellate facendo clic sull'icona  , ma non cancellandole a mano per risparmiare spazio; i vecchi backup di configurazione vengono eliminati automaticamente quando ne vengono creati di nuovi. E' auspicabile rimuovere un backup da modifiche di configurazione cattive-conosciute per garantire che non venga ripristinato accidentalmente.

Una copia della configurazione precedente può essere scaricata cliccando su  .

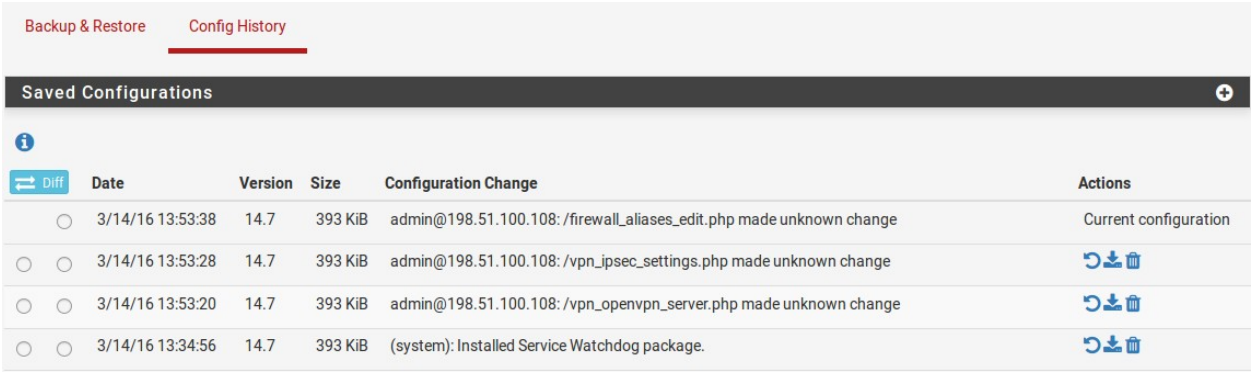


Fig. 3: Cronologia di configurazione

Impostazioni della cronologia di configurazione

La quantità di backup memorizzati nella cronologia di configurazione può essere modificata se necessario.

- Accedere a **Diagnostica>Backup & Ripristino**
- Fare clic sulla scheda **Cronologia di configurazione**
- Cliccare su  alla destra della barra delle **Configurazioni salvate** per espandere le impostazioni.

- Inserire il nuovo numero di configurazioni da trattenere
- Fare clic su **Salvare**

Insieme con la quantità di configurazioni, viene visualizzata anche la quantità di spazio occupato dai backup correnti.

Differenza della cronologia di configurazione

Le differenze tra due file di configurazione possono essere visualizzate nella scheda **Cronologia di configurazione**. A sinistra dell'elenco dei file di configurazione ci sono due colonne di pulsanti radio. Utilizzare la colonna a sinistra per selezionare il più vecchio dei due file di configurazione, e quindi utilizzare la colonna a destra per selezionare il più recente dei due file. Una volta che entrambi i file sono stati selezionati, fare clic su **Differenza** nella parte superiore o inferiore della colonna.

Cronologia di configurazione nella console

La cronologia di configurazione è disponibile anche dal menu della console, come opzione di 15, R**ipristino della configurazione recente**. La selezione di menu elencherà i file di configurazione recenti e consentirà loro di essere ripristinati. Questo è utile se una recente modifica ha bloccato gli amministratori dalla GUI o preso il sistema fuori dalla rete.

11.4.3 Ripristino per il montaggio del disco

Questo metodo è popolare tra gli utenti incorporati. Quando il CF o il disco dal firewall Firew4LL è collegato ad un computer che usa FreeBSD, l'unità può essere montata e una nuova configurazione può essere copiata direttamente sul sistema installato, o una configurazione da un sistema guasto può essere copiata al di fuori.

Nota: Questo può essere eseguito anche su un firewall Firew4LL separato al posto di un computer che usa FreeBSD, ma non usare un firewall di produzione attiva per questo scopo. Usate invece un firewall di riserva o di test..

Il file config.xml è conservato in /cf/conf/ sia per NanoBSD che per installazioni complete, ma la differenza sta nella posizione in cui si trova questa directory. Per le installazioni di NanoBSD, questo è su una porzione separata, come ad0s3 se il drive è ad0. Grazie alle etichette GEOM (struttura modulare di stoccaggio) sulle versioni recenti di FreeBSD e in uso sui filesystem incorporati basati su NanoBSD, questa porzione può anche essere accessibile indipendentemente dal nome del dispositivo usando l'etichetta /dev/ufs/cf. Per installazioni complete, è parte della porzione di root (in genere ad0s1a). I nomi delle unità variano a seconda del tipo e della posizione nel sistema.

Esempio di NanoBSD

In primo luogo, collegare il CF ad un lettore di schede USB su un sistema FreeBSD o un altro sistema Firew4LL inattivo (vedere la nota nella sezione precedente). Per la maggior parte, apparirà come da0. Verranno stampati anche i messaggi della console che riflettono il nome del dispositivo e le nuove etichette GEOM disponibili.

```
# mount -t ufs /def/ufs/cf /mnt
```

Ora montare la partizione di configurazione:

```
# cp /usr/backups/firew4ll/config-alix.example.com-20090606185703.xml \
/mnt/conf/config.xml
```

Se per qualche motivo le etichette GEOM non sono utilizzabili, usare il dispositivo direttamente come /dev/da0s3.

Ora, copiare una configurazione sulla scheda:

Quindi essere sicuri di smontare la partizione di configurazione:

Staccare la scheda, reinserirla nel firewall, e riaccendere. Il firewall sarà ora in esecuzione con la configurazione precedente.

Per copiare la configurazione dalla scheda, il processo è lo stesso ma gli argomenti al comando cp sono invertiti.

11.5 Backup di file e directory con il pacchetto di backup

Il pacchetto di Backup consente di eseguire il backup e il ripristino di qualsiasi gruppo di file/cartelle del sistema. Per la maggior parte, questo non è necessario, ma può essere utile per il backup dei dati RRD o per i pacchetti che possono avere file personalizzati che non sono conservati in config.xml.

Per installare il pacchetto:

- Navigare fino a **Sistema> Pacchetti**
- Individuare **Backup** nella lista
- Fare clic su **Installare**, alla fine della sua voce
- Cliccare su **Confermare** per avviare l'installazione

Una volta installato, il pacchetto è disponibile su **Diagnostica>File di Backup/Directory**. È abbastanza semplice da usare, come mostrato nel seguente esempio.

11.5.1 Backup dei dati RRD

Usare questo pacchetto di Backup è abbastanza facile per fare il backup dei dati di grafico RRD fuori dal metodo config.xml.

Monitoraggio Grafici

- Accedere a **Diagnostica> File di backup/Directory**
- Fare clic su **Aggiungere** per aggiungere una nuova posizione per il set di backup
- Inserire file RRD nel campo Nome
- Inserire /var/db/rrd nel campo **Percorso**
- Impostare **Abiltato** su *Vero*
- Inserire file di dati dei grafici RRD nella **Descrizione**
- Fare clic su **Salvare**
- Fare clic sul pulsante **Backup** per scaricare l'archivio di backup, che contiene i file e le directory configurati per il set di backup.
- Salvare il file in un luogo sicuro e prendere in considerazione di mantenere copie multiple, se i dati sono importanti.

11.5.2 Ripristino dei dati RRD

- Accedere a **Diagnostica>File di backup/Directory**
- Fare clic su **Sfogliare**
- Individuare e selezionare il file di archivio di backup precedentemente scaricato
- Fare clic su **Caricare** per ripristinare i file

Per questo esempio, poiché i file RRD vengono toccati solo una volta aggiornati ogni 60 secondi, non è necessario riavviare o riavviare i servizi una volta che i file vengono ripristinati.

11.6 Avvertenze e trucchi

Mentre il file XML di configurazione tenuto da Firew4LL include tutte le impostazioni, non include le modifiche che possono essere state apportate manualmente al sistema, come le modifiche manuali del codice sorgente. Inoltre alcuni pacchetti richiedono metodi di backup aggiuntivi per i loro dati.

Il file di configurazione può contenere informazioni sensibili come chiavi o certificati VPN e password (diverse dalla password di amministrazione) in testo semplice in alcuni casi. Alcune password devono essere disponibili in testo semplice durante il tempo di esecuzione, rendendo sicuro l'hashing di quelle password impossibili. Qualsiasi offuscamento sarebbe banale da invertire per chiunque con accesso al codice sorgente cioé tutti. In m0n0wall è stata presa una decisione consapevole di progettazione, che è proseguita in Firew4LL, di lasciare le password in modo chiaro per rendere estremamente chiaro che il file contiene contenuti sensibili e deve essere protetto come tale. Quindi copie di backup di questi file devono anche essere protette in qualche modo. Se sono memorizzate su supporti rimovibili, fare attenzione con la sicurezza fisica di tale supporto e/o crittografare l'unità.

Se la WebGUI deve essere usata sulla WAN senza una connessione VPN, o almeno usare HTTPS. In caso contrario, un backup viene trasmesso in chiaro, comprese le informazioni sensibili all'interno del file di backup. Si consiglia vivamente di utilizzare una rete di fiducia o una connessione crittografata.

Grazie al file di configurazione basato su XML utilizzato da Firew4LL, i backup sono una passeggiata. Tutte le impostazioni per il sistema sono contenute in un unico file (vedere *File di configurazione XML di \firew4ll*). Nella stragrande maggioranza dei casi, questo file può essere utilizzato per ripristinare un sistema ad uno stato completamente funzionante identico a quello che era in esecuzione in precedenza. Non c'è bisogno di fare un intero backup del sistema, perché i file di sistema di base non vengono modificati da un normale, in esecuzione, sistema.

Nota: In rari casi, i pacchetti possono memorizzare file al di fuori di config.xml, controllare la documentazione del pacchetto per ulteriori informazioni e suggerimenti di backup.

11.7 Strategie di backup

La migliore pratica è quella di fare un backup dopo ogni piccolo cambiamento, e sia prima e dopo ogni grande cambiamento o serie di modifiche. In genere, un backup iniziale viene preso nel caso in cui la modifica che è stata effettuata abbia effetti indesiderati. Dopo aver valutato il cambiamento e aver ottenuto il risultato desiderato, si effettua un backup post-evento. I backup periodici sono anche utili, indipendentemente dalle modifiche, soprattutto nei casi in cui un backup manuale può essere mancato per un motivo o l'altro.

Firew4LL effettua un backup interno ad ogni modifica, e si consiglia di scaricare anche un backup manuale. I backup automatici effettuati su ogni modifica sono utili per tornare a configurazioni precedenti dopo che le modifiche si sono dimostrate dannose, ma non sono buone per il ripristino d'emergenza perché sono sul sistema stesso e non

mantenute esternamente. Poiché si tratta di un processo abbastanza semplice e indolore, gli amministratori dovrebbero prendere l'abitudine di scaricare un backup di tanto in tanto e tenerlo in un luogo sicuro. Se è disponibile un abbonamento Firew4LL Gold, i backup possono essere gestiti facilmente e automaticamente utilizzando il pacchetto **AutoConfigBackup**.

Se sono state apportate modifiche ai file di sistema, come patch personalizzate o modifiche del codice, tali modifiche devono essere sottoposte a backup manuale o con il pacchetto di backup descritto in *file di backup e directory con il pacchetto di backup*, in quanto non saranno sottoposti a backup o ripristinati dal sistema di backup incorporato. Questo include modifiche ai file di sistema menzionati altrove nel libro, come /boot/device.hints, /boot/loader.conf.local, e altri.

Nota: Le patch personalizzate dovrebbero essere gestite utilizzando il pacchetto **Patch di sistema**, che viene eseguito con config.xml, piuttosto che salvare manualmente i file patchati.

Oltre a fare i backup, i **backup devono essere testati**. Prima di mettere un sistema in produzione, fare il backup della configurazione, pulire il disco, e quindi tentare alcune delle diverse tecniche di restauro in questo capitolo. Si consiglia inoltre di testare periodicamente i backup su una macchina non di produzione o su una macchina virtuale. L'unica cosa peggiore di un backup mancante è un backup inutilizzabile!

I dati del grafico RRD possono essere conservati opzionalmente nel backup del file di configurazione XML. Questo comportamento è disabilitato per impostazione predefinita a causa della dimensione risultante del file di backup. Ci sono anche altri modi per garantire che questi dati vengano salvati in modo sicuro. Vedere *File di backup e directory con il pacchetto di backup* più avanti in questo capitolo.

CAPITOLO 12

Firewall

12.1 Fondamenti di firewalling

Questa sezione tratta principalmente i concetti introduttivi del firewall e pone le basi per capire come configurare le regole del firewall usando Firew4LL.

12.1.1 Terminologia di base

Regola e *schema* sono due termini utilizzati in tutto questo capitolo:

Regola Si riferisce ad una singola voce nella schermata **Firewall>Regole**. Una regola dice al firewall come abbinare o gestire il traffico di rete.

Insieme di regole Si riferisce ad un gruppo di regole collettivamente. O *tutte* le regole del firewall nel loro insieme, o un insieme di regole in un contesto specifico come le regole di una scheda di interfaccia. L'insieme di regole completo del firewall è la somma di tutte le regole configurate e aggiunte automaticamente dall'utente, che sono coperte in questo capitolo.

Gli schemi di regole delle schede **Interfaccia** sono valutati per la prima volta da Firew4LL. Questo significa che la lettura dell'insieme di regole per un'interfaccia va dall'alto verso il basso, la prima regola che corrisponde sarà quella usata dal firewall. La valutazione si ferma dopo aver raggiunto questa corrispondenza e poi il firewall prende l'azione specificata da quella regola. Tenere sempre a mente questo quando si creano nuove regole, soprattutto per la creazione di regole per limitare il traffico. Le regole più permissive dovrebbero essere verso la parte inferiore della lista, in modo che le restrizioni o le eccezioni possano essere fatte sopra di loro.

Nota: La scheda **Floating** è l'unica eccezione a questa regola logica di elaborazione. È coperta in una sezione successiva questo capitolo.

12.1.2 Filtraggio dinamico

Firew4LL è uno «stateful» firewall, questo significa che ricorda le informazioni sulle connessioni che passano attraverso il firewall in modo che il traffico di risposta possa essere permesso automaticamente. Questi dati sono conservati nella tabella degli stati. Le informazioni di connessione nella tabella di stato includono la fonte, la destinazione, il protocollo, le porte e molto più: abbastanza per identificare univocamente una connessione specifica.

Utilizzando questo meccanismo, il traffico deve essere consentito solo sull'interfaccia in cui **entra** nel firewall. Quando una connessione corrisponde a una regola di passaggio, il firewall crea una voce nella tabella di stato. Al traffico di risposta alle connessioni è automaticamente permesso di tornare indietro attraverso il firewall confrontandolo con la tabella di stato, piuttosto che dover controllare le regole in entrambe le direzioni. Questo include qualsiasi traffico correlato che utilizza un protocollo diverso, come i messaggi di controllo ICMP che possono essere forniti in risposta a un TCP, UDP, o altro collegamento.

Vedi anche:

Vedere *Impostazioni avanzate del firewall* e *Tipo di stato* per ulteriori informazioni sulle opzioni di stato e tipi.

Dimensioni tabella di stato

La tabella di stato del firewall ha una dimensione massima per prevenire l'esaurimento della memoria. Ogni stato richiede circa 1 KB di RAM. La dimensione della tabella di stato predefinita in Firew4LL viene calcolata prendendo circa il 10% della RAM disponibile nel firewall. Su un firewall con 1GB di RAM, la dimensione della tabella di stato predefinita può contenere circa 100.000 voci.

Vedi anche:

Vedere *Grandi Tabelle stato* per maggiori informazioni sul dimensionamento della tabella di stato e l'utilizzo di RAM.

Ogni connessione utente tipicamente consiste di due stati: uno creato mentre entra nel firewall, e uno mentre lascia il firewall. Pertanto, con una tabella di stato di 1.000.000, il firewall può gestire circa 500.000 sessioni per utente che attraversa attivamente il firewall prima che qualsiasi connessione aggiuntiva venga eliminata. Questo limite può essere aumentato se necessario, purché non superi la quantità di RAM disponibile nel firewall.

Per aumentare la dimensione della tabella di stato:

- Passare al **Sistema>Impostazioni Avanzate** sulla scheda **Firewall e NAT**
- Digitare il numero desiderato per gli **stati massimi del Firewall** o lasciare la casella vuota per il valore calcolato di default. Vedere Figura *Dimensione della tabella di stato aumentata a 2.000.000*
- Fare clic su Salvare

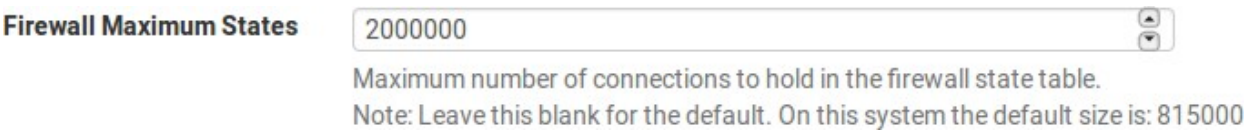


Fig. 1: Dimensione della tabella di stato aumentata a 2.000.000

L'uso della tabella di stato storico è monitorato dal firewall. Per visualizzare il grafico:

- Passare a **stato>Monitoraggio**
- Cliccare su  per espandere le opzioni del grafico
- Impostare **Categoria** per l'"**Asse sinistro** come *Sistema*
- Impostare il **grafico** per l'"**Asse Sinistro** come *Stati*
- Cliccare su  **Aggiornamento dei grafici**

12.1.3 Block vs Deny

Ci sono due modi per impedire il traffico usando le regole del firewall su Firew4LL: **Bloccare** e **Respingere**.

Una regola per **bloccare** farà cadere silenziosamente il traffico. Un client bloccato non riceverà alcuna risposta e quindi attenderà fino a che il suo tentativo di connessione non scada. Questo è il comportamento della regola predefinita di negazione in Firew4LL.

Una regola impostata per **rifiutare** risponderà al client per il traffico TCP e UDP negato, facendo sapere al mittente che la connessione è stata rifiutata. Il traffico TCP rifiutato riceve un TCP RST (reimpostare) in risposta, e il traffico UDP respinto riceve un messaggio ICMP irraggiungibile in risposta. Anche se lo scarto è una scelta valida per qualsiasi regola del firewall, i protocolli IP diversi da TCP e UDP non possono essere rifiutati; queste regole eliminano silenziosamente altri protocolli IP perché non esiste uno standard per rifiutare altri protocolli.

Decidere tra il blocco e il rifiuto

C'è stato molto dibattito tra i professionisti della sicurezza nel corso degli anni per quanto riguarda il valore del blocco contro quello del rifiuto. Alcuni sostengono che l'utilizzo del blocco ha più senso, sostenendo che «rallenta» aggressori che scansionano Internet. Quando una regola è impostata per rifiutare, una risposta viene inviata immediatamente quando la porta è chiusa, mentre il blocco fa silenziosamente scendere il traffico, in modo che lo scanner della porta dell'aggressore attende una risposta. Questo argomento non regge perché ogni buon scanner di porte può scansionare centinaia o migliaia di host contemporaneamente, e lo scanner non è bloccato in attesa di una risposta da porte chiuse. C'è una minima differenza nel consumo delle risorse e nella velocità di scansione, ma così lieve che non dovrebbe essere presa in considerazione.

Se il firewall blocca tutto il traffico da Internet, c'è una notevole differenza tra blocco e rifiuto: nessuno sa che il firewall è online. Se anche una singola porta è aperta, il valore di tale capacità è minimo perché l'aggressore può facilmente determinare che l'host è online e sa anche quali porte sono aperte se le connessioni bloccate sono state rifiutate dal firewall o meno. Anche se non c'è un valore significativo nel blocco rispetto al rifiuto, si consiglia ancora di utilizzare il blocco sulle regole WAN. C'è un certo valore nel non consegnare attivamente informazioni a potenziali aggressori, ed è anche una cattiva pratica per rispondere automaticamente a una richiesta esterna inutilmente.

Per le regole sulle interfacce interne si consiglia di utilizzare lo scarto nella maggior parte delle situazioni. Quando un host tenta di accedere a una risorsa che non è consentita dalle regole del firewall, l'applicazione che vi accede può rimanere fino a quando il programma del client non smette di cercare di accedere al servizio. Con lo scarto la connessione viene immediatamente rifiutata e il client evita questi blocchi. Questo di solito non è altro che un fastidio, ma ancora in genere si consiglia di utilizzare il rifiuto per evitare potenziali problemi di applicazione indotti dal silenzioso calo del traffico all'interno di una rete.

12.2 Filtraggio in ingresso

Il filtraggio degli ingressi si riferisce al concetto di firewalling del traffico che entra in rete da una fonte esterna come Internet. Nelle distribuzioni con multi-WAN, il firewall ha più punti di ingresso. La politica di default per l'ingresso di Firew4LL è quella di bloccare tutto il traffico in quanto non ci sono regole di autorizzazione per WAN nello schema di regole predefinito. Le risposte al traffico avviate dall'interno della rete locale sono automaticamente autorizzate a tornare attraverso il firewall dalla tabella di stato.

12.3 Filtraggio in uscita

Il filtraggio Egress si riferisce al concetto di firewalling del traffico avviato all'interno della rete locale, destinato ad una rete remota come Internet. Firew4LL, come quasi tutte le soluzioni commerciali e open source simili, è dotato di una regola LAN che consente tutto dalla LAN verso Internet. Questo non è tuttavia il modo migliore di operare.

È diventata una impostazione predefinita nella maggior parte delle soluzioni firewall perché è quello che la maggior parte della gente si aspetta. La percezione errata comune è «Tutto sulla rete interna è 'affidabile", quindi perché preoccuparsi di un filtraggio»?

12.3.1 Perchè impiegare il filtraggio in uscita?

Dalla nostra esperienza di lavoro con innumerevoli firewall presso numerosi rivenditori per diverse organizzazioni, la maggior parte delle piccole imprese e delle reti domestiche non utilizzano filtri in uscita. Si può aumentare l'onere amministrativo perché ogni nuova applicazione o servizio può richiedere apertura porte o protocolli aggiuntivi nel firewall. In alcuni ambienti è difficile perché gli amministratori non sanno completamente cosa sta succedendo sulla rete, e sono riluttanti a rompere le cose. In altri ambienti è impossibile per motivi di politica sul posto di lavoro. La pratica migliore è per gli amministratori di configurare il firewall per consentire solo il minimo traffico necessario per uscire da una rete, se possibile. Uno stretto numero di filtri egress è importante per diverse ragioni:

Limitare l'impatto di un sistema compromesso

Il filtraggio Egress limita l'impatto di un sistema compromesso. Il malware comunemente usa porte e protocolli che non sono richiesti sulla maggior parte delle reti aziendali. Alcuni bot si affidano alle connessioni IRC per telefonare a casa e ricevere istruzioni. Alcuni useranno porte più comuni come la porta TCP 80 (normalmente HTTP) per eludere il filtraggio delle uscite, ma molti non lo fanno. Se l'accesso alla porta TCP 6667, la solita porta IRC, non è consentito dal firewall, i bot che fanno affidamento su IRC per funzionare possono essere paralizzati dal filtraggio.

Un altro esempio è un caso in cui l'interfaccia interna di un'installazione Firew4LL abbia visto 50-60 Mbps di traffico mentre la WAN meno di 1 Mbps di flusso. Senza altre interfacce sul firewall. Alcune indagini indicano la causa in un sistema compromesso sulla LAN che esegue un bot dovuto ad un rifiuto distribuito dell'attacco del servizio (DDoS) contro un sito web cinese di gioco d'azzardo. L'attacco usa una porta 80 di UDP, e in questa porta 80 dell'UDP di rete non è consentito dal codice di uscita, perché tutto ciò il DDoS sta compiendo, sta stressando l'interfaccia interna del firewall con il traffico che viene abbandonato. In questa situazione, il firewall continua felicemente a scolarsi senza nessuna degradazione le prestazioni e l'amministratore della rete non sa che sta accadendo fino a quando non lo scopre per caso.

L'attacco descritto nel paragrafo precedente probabilmente ha utilizzato la porta 80 UDP per due motivi principali:

- UDP permette di inviare pacchetti di grandi dimensioni dal client senza completare una stretta di mano con il TCP. Poiché i firewall statici sono la norma, i grandi pacchetti TCP non passeranno finché la stretta di mano non sarà completata con successo, e questo limita l'efficacia del DDoS.
- Coloro che utilizzano filtri di uscita sono generalmente troppo permissivi, consentendo TCP e UDP dove è richiesto solo TCP, come nel caso di HTTP.

Questi tipi di attacchi sono comunemente lanciati da server web compromessi. Con un ampio sistema di regole di uscita aperto, il traffico andrà fuori da Internet, e ha il potenziale per far traboccare la tabella di stato sul firewall, ciò costa in termini di larghezza di banda, e/o degrada le prestazioni per tutto sulla connessione Internet.

L'SMTP in uscita è un altro esempio. Consente solo a SMTP (porta 25 di TCP) di lasciare qualsiasi rete da un server di posta. Oppure, se un server di posta è ospitato esternamente, permette solo ai sistemi interni di parlare con quello specifico sistema esterno sulla porta 25 TCP. Questo impedisce ad ogni altro sistema della rete locale di essere utilizzato come un bot di spam, dal momento che il loro traffico SMTP verrà eliminato. Molti fornitori di posta si sono spostati verso l'utilizzo della sola autenticazione da parte dei client che utilizzano la porta TCP 587, quindi i client non dovrebbero avere bisogno di accesso alla porta 25. Questo ha il vantaggio evidente di limitare lo spam, e impedisce anche che la rete sia aggiunta a numerose liste nere in tutto il Internet, ciò impedirà che quel sito invii e-mail legittime a molti server di posta elettronica. Ciò può anche impedire che l'ISP per quel sito spenga la sua connessione Internet a causa di abusi.

La soluzione ideale è prevenire questo tipo di cose.

Prevenire una compromissione

Il filtraggio Egress può impedire una compromissione in alcune circostanze. Alcuni exploit e vermi richiedono l'accesso in uscita per avere successo. Un esempio più vecchio ma buono di questo è il codice verme rosso del 2001. L'exploit causa l'infezione dei sistemi tirando un file eseguibile tramite TFTP (Protocollo di trasferimento di un file banale) per poi eseguirlo. Un server web quasi certamente non ha bisogno di utilizzare il protocollo TFTP, e bloccando TFTP tramite filtraggio di uscita previene l'infezione con il Codice Rosso anche su server non sigillati. Questo è in gran parte utile solo per fermare attacchi completamente automatizzati e vermi perché un vero aggressore umano troverà eventuali buchi che esistono nel filtraggio uscita per usarli a suo vantaggio. Ancora una volta, la soluzione corretta per prevenire tale compromesso è quello di risolvere le vulnerabilità della rete utilizzate come vettore di attacco, tuttavia il filtraggio di uscita può aiutare.

Limitare l'uso di applicazioni non autorizzate

Molte applicazioni come i client VPN, i software peer-to-peer, le messaggerie istantanee, e molti altri si affidano a porte o protocolli atipici per funzionare. Mentre un numero crescente di applicazioni peer-to-peer e instant messenger salteranno fino a trovare una porta da cui è permesso uscire dalla rete locale, a molti sarà impedito di funzionare da un codice di uscita restrittivo, e questo è un mezzo efficace per limitare molti tipi di connettività VPN.

Prevenire lo spoofing dell'IP

Questa è una ragione comunemente citata per l'utilizzo di filtri di uscita, ma Firew4LL blocca automaticamente il traffico di spoof tramite la funzionalità *antispoof* di f4l, quindi non è applicabile qui. Impedire lo spoofing dell'IP significa che i client dannosi non possono inviare traffico con indirizzi di origine ovviamente falsificati.

Impedire le perdite di informazioni

Alcuni protocolli non dovrebbero mai lasciare una rete locale. Esempi specifici di tali protocolli variano da un ambiente all'altro, ma alcuni esempi comuni sono:

- Microsoft RPC (Chiamata della procedura remota) sulla porta TCP 135
- NetBIOS sulle porte TCP e UDP da 137 a 139
- SMB/CIFS (Blocco dei messaggi del server/Fyle sistem di internet cmune) sulla porta TCP e UDP 445.

L'interruzione di questi protocolli può impedire la fuoriuscita di informazioni della rete interna su Internet, e impedirà ai sistemi locali di avviare tentativi di autenticazione con host di Internet. Questi protocolli rientrano anche in *Limitare l'impatto di un sistema compromesso* come discusso in precedenza, poiché molti worm hanno fatto affidamento su questi protocolli per funzionare. Altri protocolli che possono essere rilevanti sono syslog, SNMP e trappole SNMP. La limitazione di questo traffico impedirà ai dispositivi di rete mal configurati di inviare dati di accesso e altre informazioni potenzialmente sensibili su Internet. Piuttosto che preoccuparsi di quali protocolli possono perdere informazioni da una rete locale e devono essere bloccati, la migliore pratica è quella di consentire solo il traffico che è richiesto.

12.3.2 Approcci per l'attuazione di filtri in uscita

Su una rete che storicamente non ha impiegato filtri di uscita, può essere difficile sapere quale traffico è assolutamente necessario. Questa sezione descrive alcuni approcci per identificare il traffico e implementare il filtraggio delle uscite.

Consentire ciò che è noto, bloccare il resto, e lavorare attraverso le conseguenze

Un approccio è quello di aggiungere le regole firewall per il traffico richiesto noto di essere consentito. Iniziare con la compilazione di un elenco di cose note che deve essere richiesto, come in *Tabella Traffico egress richiesto*.

Tabella 1: Traffico egress richiesto

Descrizione	fonte	Destinazione	Porta di destinazione
HTTP e HTTPS da tutti gli host	rete LAN	Qualunque	TCP 80 e 443
SMTP dal server di posta	Server email	Qualunque	TCP 25
query DNS da server DNS interni	Server DNS	Qualunque	TCP e UDP 53

Dopo aver fatto l'elenco, configurare le regole firewall per passare solo quel traffico e lasciare che tutto il resto sia colpito dalla regola di default di negazione.

Registrare il traffico e analizzare i registri

Un'altra alternativa è abilitare la registrazione su tutte le regole di passaggio e inviare i log a un server syslog. I registri possono essere analizzati dal server syslog per vedere quale traffico sta lasciando la rete. Firew4LL utilizza un formato di log personalizzato, per cui i registri di solito devono essere analizzati da uno script personalizzato a meno che il server non abbia qualche conoscenza del formato di log dei filtri Firew4LL. L'analisi dei tronchi aiuterà a costruire le regole richieste con meno ricadute in quanto darà una migliore idea di quale traffico è necessario sulla rete locale.

12.4 Introduzione alla schermata delle regole del firewall

Questa sezione fornisce un'introduzione e una panoramica della schermata Regole del Firewall situato in **Firewall>Regole**. Questa pagina elenca le regole WAN con cui iniziare, che per impostazione predefinita non ha voci diverse da quelle per **Bloccare le reti private** e **Bloccare le reti bogon** se tali opzioni sono attive sull'interfaccia WAN, come mostrato in Figura *Regole WAN predefinite*.

Suggerimento: Fare clic sull'icon a  a destra delle regole **Bloccare le reti private** o **Bloccare le reti bogon** per raggiungere la pagina di configurazione dell'interfaccia WAN dove queste opzioni possono essere abilitate o disattivate. (Vedere *Bloccare reti private* e *Bloccare reti bogon* per maggiori dettagli).

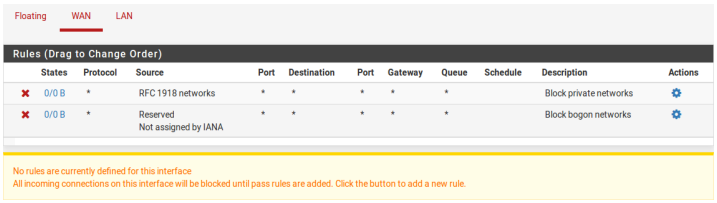


Fig. 2: Regole WAN predefinite

Fare clic sulla scheda **LAN** per visualizzare le regole LAN. Per impostazione predefinita, le uniche voci sono le regole *Permettere per impostazione predefinita la LAN a tutti* per IPv4 e IPv6 come si vede in Figura *Regole LAN predefinite*, e la **Regola anti-blocco** se è attiva. La regola anti-blocco è progettata per impedire agli amministratori di bloccarsi accidentalmente fuori dalla GUI. Fare clic su  accanto alla regola anti-blocco per raggiungere la pagina dove questa regola può essere disabilitata.

Vedi anche:

Per ulteriori informazioni su come funziona la regola anti-blocco e come disabilitare la regola, vedere la *Regola anti-blocco* e *Anti-lockout*.

Per visualizzare le regole per altre interfacce, fare clic sulle rispettive schede. Le interfacce OPT appariranno con i loro nomi descrittivi, quindi se l'interfaccia OPT1 è stata rinominata DMZ, allora la scheda per le sue regole dirà anche **DMZ**.

Alla sinistra di ogni regola c'è un'icona che mostra l'azione della regola: passare ( ), bloccare ( ), o respingere ( ). Se la registrazione è abilitata per la regola, l'icona è mostrata nella stessa area. Se la regola ha delle opzioni avanzate abilitate, viene anche visualizzata l'icona . Spostando il cursore del mouse su una qualsiasi di queste icone verrà visualizzato il testo che spiega il loro significato. Le stesse icone sono mostrate per le regole disabilitate, tranne che l'icona e la regola sono una tonalità più chiara del loro colore originale.

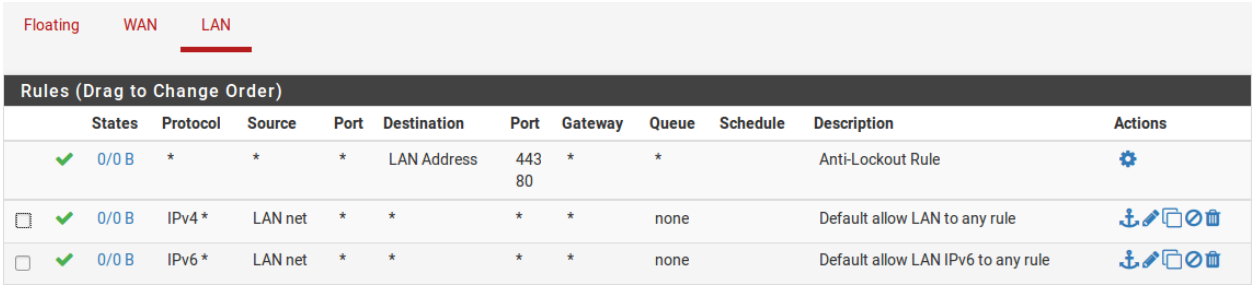


Fig. 3: Regole LAN predefinite

12.4.1 Aggiungere una regola al firewall

Per aggiungere una regola in cima alla lista, fare clic su **Aggiungere**.

Per aggiungere una regola in fondo alla lista, fare clic su **Aggiungere**.

Per creare una nuova regola simile a una regola esistente, fare clic su sulla destra della regola esistente. La schermata di modifica apparirà con le impostazioni della regola esistente pre-riempita, pronta per essere regolata. Quando si duplica una regola esistente, la nuova regola verrà aggiunta direttamente al di sotto della regola originale. Per ulteriori informazioni su come configurare la nuova regola, vedere *Configurare le regole del firewall*.

12.4.2 Modificare le regole del firewall

Per modificare una regola del firewall, fare clic su a destra della regola o fare doppio clic in qualsiasi punto della riga.

La pagina di modifica per quella regola verrà caricata, e da lì le regolazioni sono possibili. Vedere *Configurare le regole del firewall* per maggiori informazioni sulle opzioni disponibili quando si modifica una regola.

12.4.3 Spostare le regole del firewall

Le regole possono essere riordinate in due modi diversi: Trascinare e tralasciare (Drag-and-drop), e Selezionare e cliccare (select-and-click).

Per spostare le regole usando il metodo drag-and-drop:

- Spostare il mouse sulla regola del firewall da spostare, il cursore cambierà per indicare che il movimento è possibile.
- Fare clic e tenere premuto il pulsante del mouse verso il basso
- Trascinare il mouse nella posizione desiderata per la regola
- Rilasciare il pulsante del mouse
- Fare clic su  **Salva** per memorizzare il nuovo ordine delle regole

> **Avvertimento:** Il tentativo di allontanarsi dalla pagina dopo aver spostato una regola, ma prima di salvare la regola, si tradurrà nella presentazione di un errore del browser che conferma se uscire o meno dalla pagina. Se il browser si allontana dalla pagina senza salvare, la regola sarà ancora nella sua posizione originale.

Per spostare le regole dell'elenco in gruppi o selezionandole per prime, utilizzare il metodo select-and-click:

- Selezionare la casella accanto alla sinistra delle regole che devono essere spostate, o fare un solo un clic sulla regola. Quando la regola è selezionata, cambierà colore.
- Cliccare su  sulla riga sotto dove la regola deve essere spostata

---

Suggerimento: Tenere premuto **Maiuscolo** cliccando il mouse su  per spostare la regola sotto la regola selezionata invece che sopra.

Quando si spostano le regole con il metodo select-and-click, il nuovo ordine viene memorizzato automaticamente.

12.4.4 Eliminazione di regole del firewall

Per eliminare una singola regola, fare clic su  a destra della regola. Il firewall presenterà una richiesta di conferma prima di eliminare la regola.

Per eliminare più regole, selezionare la casella all'inizio delle righe che devono essere rimosse, quindi fare clic su  **Eliminare** in fondo alla lista. Le regole possono anche essere selezionate con un singolo clic in qualsiasi punto della loro linea.

12.4.5 Disattivazione e attivazione delle regole del firewall

Per disabilitare una regola, fare clic su  alla fine della riga. L'aspetto della regola cambierà in una tonalità più chiara per indicare che è disabilitata e l'icona  cambia in  .

Per abilitare una regola precedentemente disabilitata, fare clic su  alla fine della riga. L'aspetto della regola tornerà alla normalità e l'icona di abilitazione/disabilitazione tornerà all'originale  .

Una regola può anche essere disabilitata o abilitata modificando la regola e commutando la casella **Disabilitata**.

12.4.6 Separatori delle regole

I separatori delle regole del firewall sono barre colorate nello schema che contengono un po" di testo, ma non hanno alcuna azione sul traffico. Sono utili per separare visivamente o aggiungere note a parti speciali dello schema. La figura *Esempio di separatori delle regole del firewall* mostra come possono essere utilizzati per raggruppare e documentare lo schema di regole.

Per creare un nuovo separatore di regole:

- Aprire la scheda delle regole del firewall dove risiederà il separatore di regole
- Cliccare su  **Separatore**
- Inserire il testo di descrizione per il separatore di regole
- Scegliere il colore per il separatore di regole facendo clic sull'icona  del colore desiderato
- Fare clic e trascinare il separatore di regole nella sua nuova posizione
- Fare clic su  Salvare all'interno del separatore di regole per memorizzarne il contenuto
- Fare clic su  Salvare in fondo alla lista delle regole

Per spostare un separatore di regole:

- Aprire la scheda delle regole del firewall contenente il separatore di regole
- Fare clic e trascinare il separatore di regole nella sua nuova posizione
- Fare clic su  Salvare in fondo alla lista delle regole

Per eliminare un separatore di regole:

- Aprire la scheda delle regole del firewall contenente il separatore di regole
- Cliccare su  all'interno del Separatore di regole sul lato destro
- Fare clic su  Salvare in fondo alla lista delle regole

I separatori di regole non possono essere modificati. Se è richiesto un cambiamento di testo o colore, creare un nuovo separatore di regole e cancellare la voce esistente

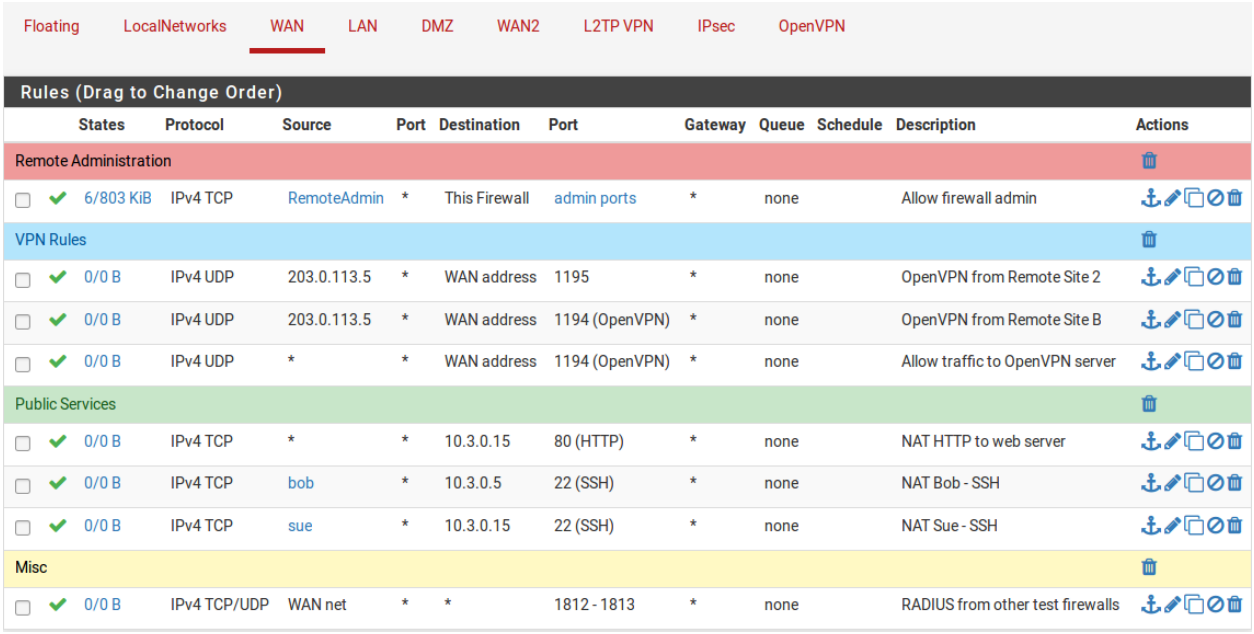


Fig. 4: Esempio di separatori delle regole del firewall

12.4.7 Monitoraggio delle modifiche delle regole del firewall

Quando una regola viene creata o aggiornata il firewall registra il nome di accesso dell'utente, l'indirizzo IP e un timestamp sulla regola per tenere traccia di chi ha aggiunto e/o ha modificato la regola in questione. Se il firewall ha creato automaticamente la regola, questo è anche annotato. Questo viene fatto per le regole del firewall così come per le porte forwards e le regole NAT in uscita. Un esempio di blocco di tracciamento dell'aggiornamento delle regole è mostrato in *Stampi dell'ora delle regole del Firewall*, che è visibile quando si modifica una regola del firewall in fondo alla schermata di modifica delle regole.

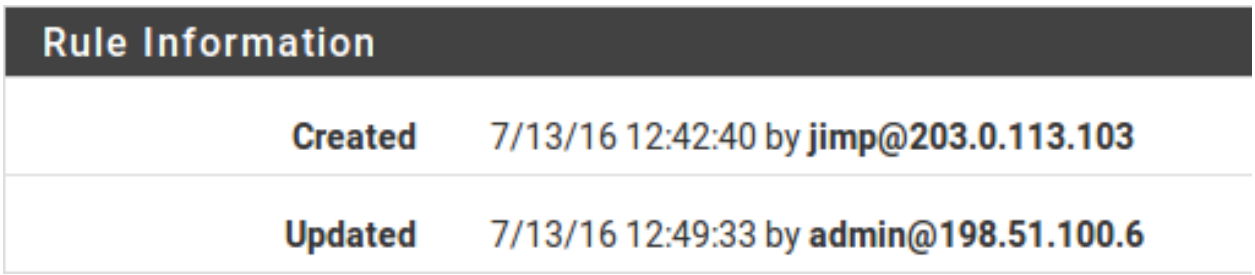


Fig. 5: Stampi dell'ora delle regole del Firewall

12.5 Alias

Gli alias definiscono un gruppo di porte, host o reti. Gli alias possono essere referenziati da regole del firewall, port forward, regole del NAT in uscita, e altri luoghi nella GUI del firewall. L'uso di alias si traduce in una serie di regole significativamente più brevi, auto-documentante e gestibili.

Nota: Non confondere gli alias in questo contesto con gli alias dell'IP dell'interfaccia, che sono un mezzo per aggiungere ulteriori indirizzi IP ad un'interfaccia di rete.

12.5.1 Fondamenti di alias

Gli alias si trovano in **Firewall>Alias**. La pagina è divisa in schede separate per ogni tipo di alias: **IP**, **Porte**, **URL**, e la scheda **Tutti** che mostra ogni alias in una grande lista. Quando si crea un alias, aggiungerlo a qualsiasi scheda e sarà ordinato nella posizione corretta in base al tipo scelto.

Possono essere creati i seguenti tipi di alias:

Host Alias contenenti singoli indirizzi IP o nomi host

Reti Alias contenenti elenchi mascherati CIDR di reti, nomi host, intervalli di indirizzi IP o singoli indirizzi IP

Porta Questi alias contengono elenchi di numeri di porta o intervalli di porte per TCP o UDP.

URL L'alias è costruito dal file all'URL specificato ma viene letto solo una volta, e poi diventa un normale alias di tipo di rete o porta.

Tabella URL L'alias è costruito dal file all'URL specificato ma viene aggiornato recuperando periodicamente l'elenco dall'URL.

Ogni tipo di alias è descritto in modo più dettagliato in questa sezione.

12.5.2 Alias nidificati

La maggior parte degli alias possono essere annidati all'interno di altri alias purché siano dello stesso tipo. Ad esempio, un alias può nidificare un alias contenente server web, un alias contenente server di posta e un alias server che contiene sia gli alias server web sia mail, tutti insieme in un alias server più grande. Gli alias della tabella URL non possono essere nidificati.

12.5.3 Utilizzare hostname in Alias

I nomi host possono essere usati anche in alias. Qualsiasi hostname può essere inserito in un host o in un alias di rete e sarà periodicamente risolto e aggiornato dal firewall. Se un hostname restituisce più indirizzi IP, tutti gli indirizzi IP restituiti vengono aggiunti all'alias. Questo è utile per il monitoraggio delle voci del DNS dinamico per consentire agli utenti specifici nei servizi da indirizzi IP dinamici.

Nota: Questa funzione **non** è utile per consentire o rifiutare agli utenti di grandi siti web pubblici. I siti grandi e occupati tendono ad avere costantemente la rotazione o risposte casuali alle interrogazioni DNS in modo che il contenuto dell'alias non corrisponda necessariamente con la risposta che un utente riceverà quando tenta dirisolvere lo stesso nome del sito. Può funzionare per i siti più piccoliche hanno solo pochi server e non includono insiemi incompleti di indirizzi nelle loro risposte DNS.

12.5.4 Mescolare indirizzi IPv4 e IPv6 in Alias

Gli indirizzi IPv4 e IPv6 possono essere mescolati all'interno di un alias. Il firewall userà il tipo di indirizzi appropriato quando l'alias è referenziato in una regola specifica.

12.5.5 Considerazioni sulla calibrazione dell'alias

La dimensione totale di tutte le tabelle deve corrispondere all'incirca alla **metà** della quantità di **voci massime della tabella del firewall**, che di default è di 200.000. Se il numero massimo di voci della tabella non è sufficiente per

contenere tutte le voci, le regole potrebbero non riuscirsi a caricare. Per informazioni su come modificare tale valore, vedere *Voci massime della tabella del firewall*. Gli alias devono essere inseriti due volte nell'area totale a causa del modo in cui gli alias vengono caricati e ricaricati; la nuova lista viene caricata accanto alla vecchia lista e quella vecchia viene rimossa.

Questo valore può essere aumentato quanto richiesto, a condizione che il firewall contenga RAM sufficiente per contenere le voci. L'uso della RAM è simile, ma inferiore, alla tabella di stato, ma è più sicuro assumere 1K per ogni voce affinché sia conservata.

12.5.6 Configurazione Alias

Per aggiungere un alias:

- Andare a **Firewall>Alias**
- Fare clic su **Aggiungere**
- **Inserire** un **nome** per l'alias. Il nome può contenere solo caratteri a-z, A-Z, 0-9 e _.
- Inserire una **descrizione** per l'alias stesso
- Selezionare il **tipo** di alias. I vari tipi sono discussi in questa sezione.
- Inserire le informazioni specifiche per tipo come è necessario. Ogni tipo ha un campo di dati e un campo di descrizione per ogni voce.

Per aggiungere nuovi membri a un alias, fare clic su **Aggiungere** in fondo alla lista delle voci.

Per rimuovere i membri da un alias, fare clic su Eliminare alla fine della riga per rimuoverli.

Quando l'alias è completo, fare clic su **Salva** per memorizzare il contenuto dell'alias.

Ogni alias inserito manualmente è limitato a 5.000 membri, ma alcuni browser hanno difficoltà a visualizzare o utilizzare la pagina con più di circa 3.000 voci. Per un gran numero di voci, utilizzare un tipo di tabella URL alias che è in grado di gestire elenchi più grandi.

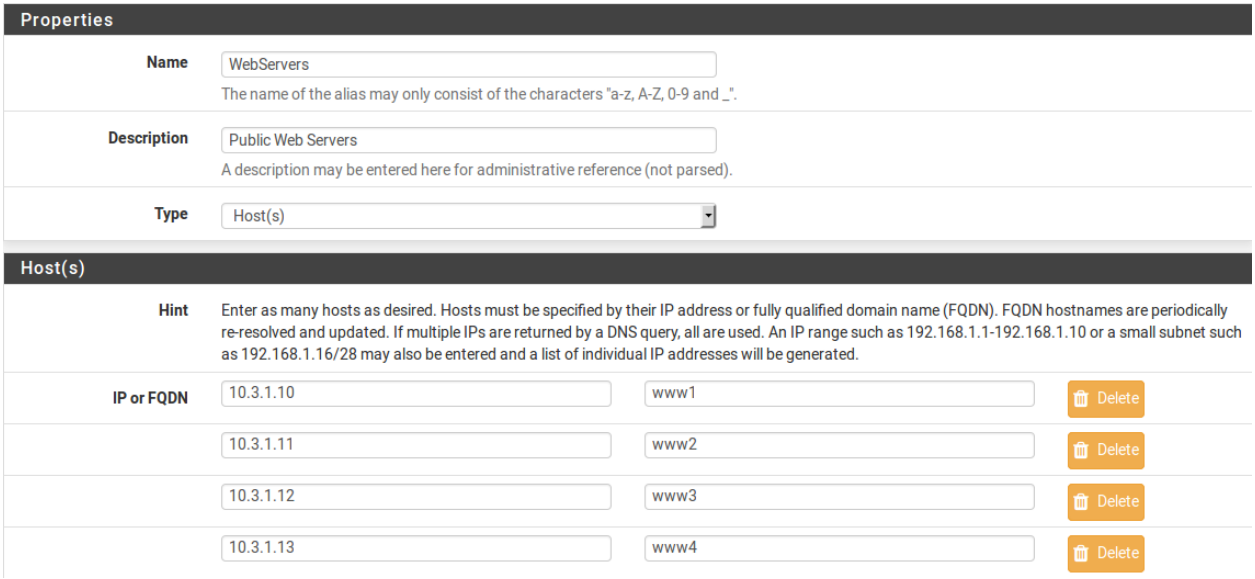


Fig. 6: Esempio alias dell'host

Altri alias tipo dell'host possono essere annidati all'interno di questa voce. Nomi host possono essere utilizzati anche come voci, come spiegato in precedenza.

Alias di rete

Gli alias di tipo di rete contengono gruppi di reti o intervalli di indirizzi IP. Gli host singoli possono anche essere inclusi negli alias di rete selezionando una maschera di rete */32* per gli indirizzi IPv4 o una lunghezza di prefisso */128* per gli indirizzi IPv6. La figura *Esempio di alia di rete* mostra un esempio di alias di rete che viene utilizzato più avanti in questo capitolo.

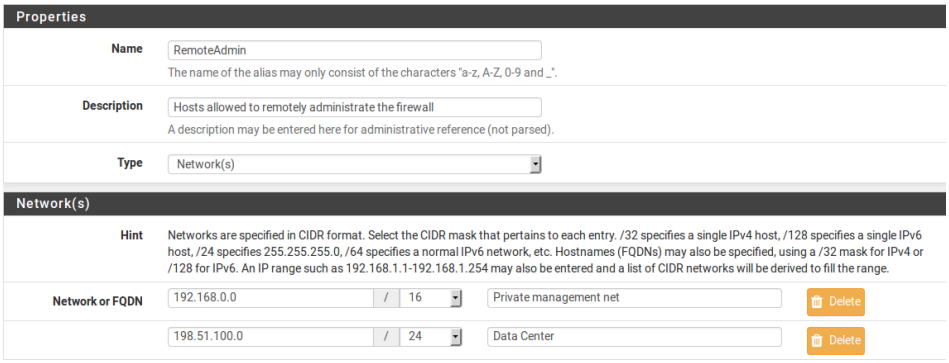


Fig. 7: Esempio di alia di rete

Altri alias host o di rete possono essere annidati all'interno di questa voce. I nomi host possono anche essere usati come voci, come spiegato in precedenza.

Quando una voce alias contiene un intervallo IPv4 viene automaticamente tradotta dal firewall in un gruppo equivalente di reti CIDR IPv4 che conterranno esattamente l'intervallo fornito. Come mostrato in Figura *Esempio di Intervallo IP, dopo*, l'intervallo viene espanso quando l'alias viene salvato, e l'elenco risultante delle reti CIDR IPv4 corrisponderà esattamente all'intervallo richiesto, niente di più, niente di meno.

Fig. 8: Esempio di Intervallo IP, prima

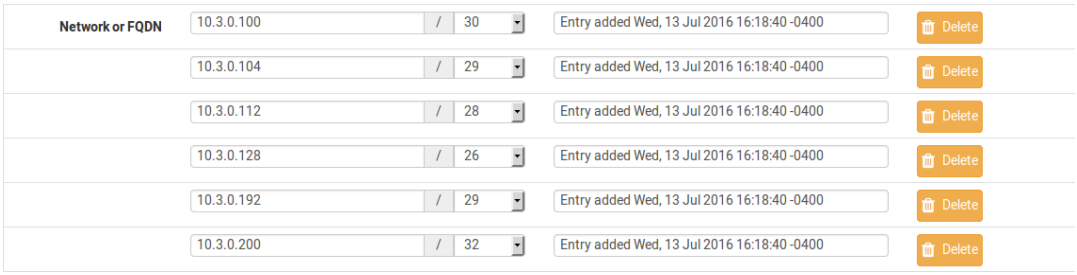


Fig. 9: Esempio di Intervallo IP, dopo

Port Alias

Gli alias di tipo porta contengono gruppi di porte e gamme di porte. Il protocollo non è specificato nell'alias; la regola del firewall in cui viene utilizzato l'alias definirà il protocollo come TCP, UDP, o entrambi. La figura *Esempio di alias di porte* mostra un esempio di un alias di tipo porta.

Inserire un altro nome alias di tipo porta nel campo **Porta** per nidificare altri alias di tipo porta all'interno di questo alias.

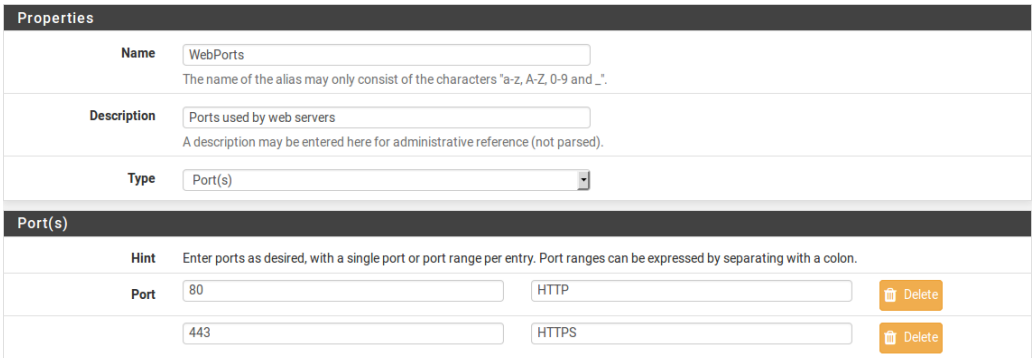


Fig. 10: Esempio di alias di porte

Alias dell'URL

Con un alias di tipo URL, viene impostato un URL che punta ad un file di testo che contiene un elenco di voci. Si possono inserire più URL. Quando si fa clic su Salvare, fino a 3.000 voci da ogni URL vengono lette dal file e importate in un alias di tipo di rete.

Se si seleziona URL (*IP*), gli URL devono contenere l'indirizzo IP o voci di rete mascherate CIDR, e il firewall creerà un alias di tipo rete dal contenuto.

Se l'URL (*Porte*) è selezionato, allora l'URL deve contenere solo i numeri o gli intervalli delle porte, e il firewall creerà un alias di tipo porta dal contenuto.

Alias della tabella di URL

Un alias della tabella URL si comporta in modo significativamente diverso dall'alias URL. Per cominciare, non importa il contenuto del file in un alias normale. Questo scarica il contenuto del file in una posizione speciale sul firewall e usa il contenuto per quella che è chiamata tabella di persistenza, anche conosciuta come un alias basato su file. Il contenuto completo dell'alias non è direttamente modificabile nella GUI, ma può essere visualizzato nel visualizzatore delle tabelle (vedi *Visualizzare i contenuti delle tabelle*).

Per un alias dell tabella URL, l'elenco a discesa dopo la / controlla quanti giorni devono passare prima che il contenuto dell'alias venga recuperato di nuovo dall'URL memorizzato dal firewall. Al momento opportuno, il contenuto degli alias verrà aggiornato durante la notte da uno script che recupera nuovamente i dati.

Gli alias della tabella di URL possono essere abbastanza grandi, contenenti migliaia di voci. Alcuni client li usano per tenere elenchi di tutti i blocchi IP in un dato paese o regione, i quali possono facilmente superare le 40.000 voci. Il pacchetto f4lBlocker usa questo tipo di alias quando si trattano elenchi di paesi e altre azioni simili.

Attualmente, gli alias della tabella di rete non possono essere nidificati.

Se viene selezionata la *tabella URL* (*IP*), gli URL devono contenere l'indirizzo IP o voci di rete mascherate CIDR, e il firewall creerà un alias di tipo rete dal contenuto.

Se viene selezionata la *tabella URL* (*Porte*), l'URL deve contenere solo i numeri o gli intervalli delle porte, e il firewall creerà un alias del tipo porta dal contenuto.

12.5.7 Importazione di massa di Alias di rete

Un altro metodo per importare più voci in un alias è quello di utilizzare la funzione di importazione di massa. Per utilizzare la funzione di importazione:

- Andare in **Firewall>Alias**

- Fare clic su **Importare**
- Inserire il **nome alias** e la **descrizione**
- Inserire il contenuto nell'area di testo **Alias da importare**, una voce per riga.
- Fare clic su **Salva**

Esempi di utilizzo comuni per questa pagina includono elenchi di indirizzi IP, reti e liste nere. L'elenco può contenere indirizzi IP, reti mascherate CIDR, intervalli IP o numeri di porta. Il firewall tenterà di determinare automaticamente il tipo di alias di destinazione.

Il firewall importa elementi in un alias normale che può essere modificato successivamente.

12.5.8 Utilizzare gli Alias

Quando una lettera viene digitata in una casella di input che supporta gli alias, viene visualizzato un elenco di alias corrispondenti. Selezionare l'alias desiderato dall'elenco, o digitare il suo nome completamente.

> **Nota:** Il completamento automatico dell'Alias non è sensibile al caso, ma è limitato dal tipo. Ad esempio, un alias di tipo rete o Host sarà elencato in completamento sutomatico per il campo rete, ma un alias di porta non lo sarà; un alias di porta può essere usato in un campo porta, ma un alias di rete non sarà nell'elenco.

La figura il *completamento automatico di alias di host* mostra come l'alias dei server web, configurato come mostrato in figura *Esempio di alias host*, può essere utilizzato nel campo **Destinazione** quando si aggiunge o si modifica una regola firewall.

- Modificare la regola del firewall
- Selezionare un *host singolo o alias*
- Quindi digitare la prima lettera dell'alias desiderato: digitare W e l'alias appare come mostrato.

Fig. 11: Completamento automatico di alias di host

La figura *completamento automatico di alias di porte* mostra il completamento automatico delle alias di porte configurato come mostrato in Figura *Esempio di alias di porte*. Se più alias corrispondono alla lettera inserita, sono elencati tutti gli alias corrispondenti del tipo appropriato. Fai clic sull'alias desiderato per selezionarlo.

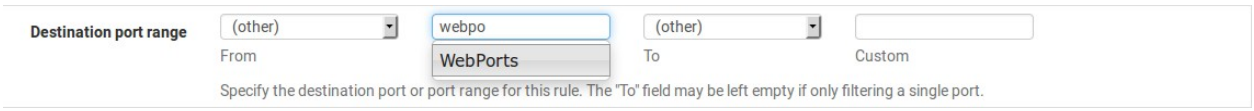


Fig. 12: Completamento automatico di alias di porte

La figura *Esempio di regole che usano alias* mostra la regola creata utilizzando gli alias serverWeb e porteWeb. Questa regola è sulla WAN, e permette qualsiasi fonte per gli indirizzi IP definiti nell'alias dei serverweb quando si usano le porte definite nell'alias porteWeb.

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	✔ 0/0 B	IPv4 TCP	*	*	WebServers	WebPorts	*	none		Allow access to WebPorts on WebServers

Fig. 13: Esempio di regole che usano alias

Spostando il cursore del mouse su un alias nella pagina **Firewall>Regole**, viene visualizzato un suggerimento che mostra il contenuto dell'alias con le descrizioni incluse nell'alias. La figura *l'hovering mostra i contenuti dell'host* visualizza questo per l'alias del serverWeb e la figura *l'hovering mostra i contenuti delle porte* per le porte alias.

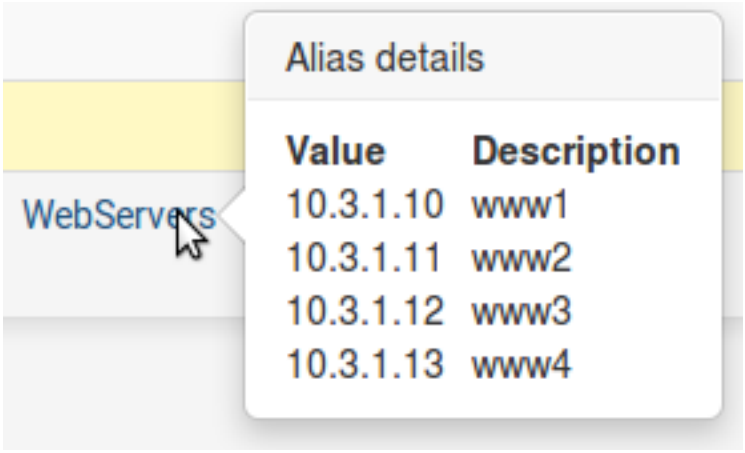


Fig. 14: L'hovering mostra i contenuti dell'host

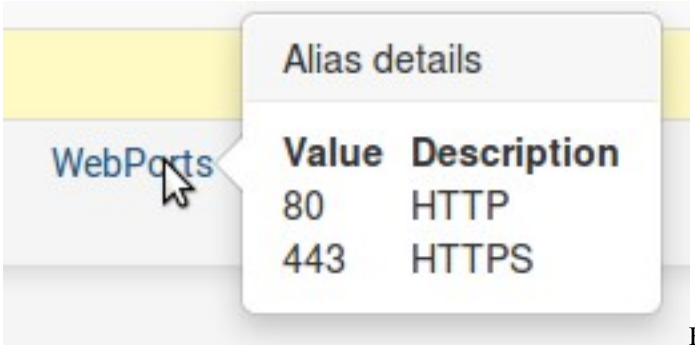


Fig. 15: L'hovering mostra i contenuti delle porte

12.5.9 Buona prassi per le regole del firewall

Questa sezione riguarda la buona prassi da seguire in generale per la configurazione delle regole del firewall.

12.5.10 Default Deny

Ci sono due filosofie di base nella sicurezza del computer relative al controllo dell'accesso: accesso predefinito e negazione predefinita. Una strategia di negazione predefinita per le regole del firewall è la migliore pratica. Gli amministratori del firewall dovrebbero configurare le regole per consentire solo il traffico minimo richiesto per le esigenze di una rete, e lasciare che il traffico rimanente cada con la regola di default di negazione integrata in Firew4LL. Seguendo questa metodologia, il numero di regole di diniego in un insieme di regole sarà minimo. Esse hanno ancora un posto per alcuni usi, ma saranno minimizzate nella maggior parte degli ambienti seguendo una strategia di negazione predefinita.

In una configurazione LAN e WAN a due interfacce di default, Firew4LL utilizza la negazione predefinita sulla WAN e l'accesso predefinito sulla LAN. Tutto ciò che entra da Internet viene negato, e tutto ciò che esce da Internet dalla LAN è permesso. Tutti i router di livello home utilizzano questa metodologia, come tutti i progetti open source simili e la maggior parte delle offerte commerciali simili. E' quello che la maggior parte delle persone si aspettano, quindi è la configurazione predefinita. Detto questo, anche se è un modo conveniente per iniziare, non è il mezzo raccomandato per un funzionamento a lungo termine.

Gli utenti di Firew4LL si chiedono spesso «Quali cose negative dovrei bloccare?» ma questa è la domanda sbagliata in quanto si applica ad una metodologia di permesso predefinita. Il noto professionista della sicurezza Marcus Ranum include l'accesso di default nel suo scritto «Sei idee stupide in sicurezza informatica», di cui si consiglia di lettura per qualsiasi professionista della sicurezza. Permettere solo ciò che una rete richiede ed evitare di lasciare per impostazione predefinita che tutte le regole sulla LAN siano consentite e di aggiungere di regole di blocco per le «cose cattive» sopra la regola di permesso.

12.5.11 Essere breve

Più è corto un gruppo di regole, più facile è da gestire. Gruppo di regole lunghi sono difficili da usare, aumentano le probabilità di errori umani, tendono a diventare eccessivamente permissivi e sono molto più difficili da controllare. Utilizzare gli alias per mantenere lo schema più breve possibile.

12.5.12 Revisione delle regole del firewall

Raccomandiamo una revisione manuale delle regole del firewall e della configurazione NAT su base periodica per garantire che corrispondano ancora ai requisiti minimi dell'ambiente di rete attuale. La frequenza raccomandata di tali recensioni varia da un ambiente all'altro. Nelle reti che non cambiano frequentemente, con un numero ridotto di amministratori di firewall e buone procedure di controllo dei cambiamenti, trimestralmente o semestralmente è di solito adeguato. Per ambienti in rapida evoluzione o con un basso controllo dei cambiamenti e con diverse persone con accesso firewall, rivedere la configurazione almeno su base mensile.

Abbastanza spesso quando si rivedono le regole con i clienti, chiediamo regole specifiche e rispondono con «Abbiamo rimosso quel server sei mesi fa.» Se qualcos'altro avesse assunto lo stesso indirizzo IP interno del server precedente, allora il traffico sarebbe stato permesso al nuovo server che potrebbe non esserne stato destinato.

12.5.13 Documentare la configurazione

In tutte le reti tranne le più piccole, può essere difficile ricordare ciò che è configurato dove e perché. Si consiglia sempre di utilizzare il campo **Descrizione** in firewall e regole del NAT per documentare lo scopo delle regole. Nelle distribuzioni più grandi o complesse, creare e mantenere un documento di configurazione più dettagliato che descriva l'intera configurazione di Firew4LL. Nel rivedere la configurazione del firewall in futuro, questo aiuterà a determinare quali regole sono necessarie e perché ci sono. Questo vale anche per qualsiasi altro settore della configurazione.

È altresì importante mantenere aggiornato questo documento. Quando si effettuano revisioni periodiche di configurazione, rivedere anche questo documento per assicurarsi che rimanga aggiornato con la configurazione attuale. Assicurarsi che questo documento sia aggiornato ogni volta che vengono apportate modifiche alla configurazione.

12.5.14 Ridurre il disturbo nei log

Per default, Firew4LL registrerà i pacchetti bloccati dalla regola di negazione predefinita. Ciò significa che tutto il disturbo che viene bloccato da Internet verrà registrato. A volte non ce ne sarà molto nei registri, ma in molti ambienti ci sarà inevitabilmente qualcosa incessantemente crea spam nei registri.

Sulle reti che utilizzano grandi domini di trasmissione - una pratica comunemente impiegata dagli ISP via cavo - è il più delle volte il NetBIOS che trasmette da individui con mancanza di definizione che collegano le macchine

Windows direttamente alle loro connessioni a banda larga. Queste macchine pomperanno costantemente le richieste di trasmissione per la navigazione di rete, tra le altre cose. Anche i pacchetti del protocollo di instradamento ISP possono essere visibili, o protocolli di ridondanza del router come VRRP o HSRP. In ambienti di co-locazione come i centri dati, può essere presente una combinazione di tutte queste cose.

Poiché non c'è alcun valore nel sapere che il firewall ha bloccato 14 milioni di trasmissioni del NetBIOS nel giorno scorso, e che il disturbo potrebbe coprire i registri che sono importanti, è una buona idea aggiungere una regola di blocco sull'interfaccia WAN per il disturbo ripetuto del traffico. Aggiungendo una regola di blocco senza la registrazione abilitata sull'interfaccia WAN, questo traffico sarà comunque bloccato, ma non riempirà più i registri.

La regola mostrata nella figura *Regola del firewall per prevenire la registrazione di trasmissioni* è configurata su un sistema di test in cui la «WAN» è su una LAN interna dietro un margine del firewall. Per sbarazzarsi del disturbo del registro e poter vedere le cose di interesse, abbiamo aggiunto questa regola per bloccare - ma non registrare - nulla con la destinazione dell'indirizzo di trasmissione di quella sottorete.

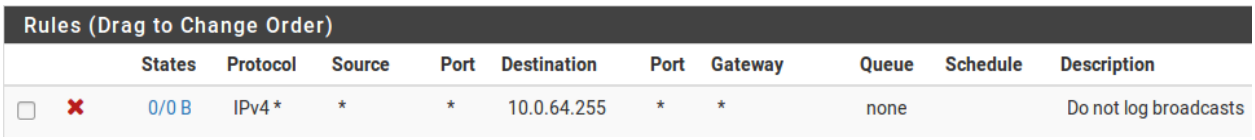


Fig. 16: Regola del firewall per prevenire la registrazione di trasmissioni

Si consiglia di aggiungere regole simili, che corrispondono alle specifiche di qualsiasi disturbo di registro osservato in un ambiente. Controllare i registri del firewall sotto la scheda **stato>Firewall, registri di sistema** per vedere che tipo di traffico il firewall stia bloccando, e rivedere quanto spesso appare nel registro. Se un traffico particolare viene costantemente registrato più di 5 volte al minuto, e il traffico non è dannoso o degno di nota, aggiungere una regola di blocco per ridurre il disturbo di registro.

12.5.15 Pratiche di registrazione

Firew4LL non registra alcun traffico passato e registra tutto il traffico caduto. Questo è il tipico comportamento di default di quasi tutti i firewall open source e commerciali. E "il più pratico, perché la registrazione di tutto il traffico passato è raramente auspicabile a causa dei livelli di carico e i registri generati. Questa metodologia, tuttavia, è un po" indietro dal punto di vista della sicurezza. Il traffico bloccato non può danneggiare una rete, quindi il suo valore di log è limitato, mentre il traffico che viene superato potrebbe avere informazioni di log molto importanti se un sistema è compromesso. Dopo aver eliminato qualsiasi disturbo di blocco inutile come descritto nella sezione precedente, il resto è di un certo valore ai fini dell'analisi di tendenza. Se si osserva un volume di registro significativamente maggiore o minore del solito, è probabilmente opportuno esaminare la natura del traffico registrato. OSSEC, un sistema di rilevamento delle intrusioni basato su host open source (IDS), è un sistema in grado di raccogliere i log da Firew4LL tramite syslog e alert sulla base di anomalie del volume di log.

12.6 Metodologia delle regole

In Firew4LL, le regole sulle schede di interfaccia sono applicate per interfaccia, sempre nella direzione in entrata su tale interfaccia. Ciò significa che il traffico avviato dalla LAN viene filtrato utilizzando le regole dell'interfaccia LAN. Il traffico avviato da Internet è filtrato con le regole dell'interfaccia WAN. Poiché tutte le regole in Firew4LL sono stateful per impostazione predefinita, viene creata una voce della tabella di stato quando il traffico corrisponde a una regola di accesso. Tutto il traffico di risposta è permesso automaticamente da questa voce della tabella di stato.

L'eccezione a questo sono le regole di fluttuazione (*Regole di floating*), che possono agire su qualsiasi interfaccia che si usa in entrata, in uscita, o in entrambe le direzioni. Le regole in uscita non sono mai necessarie, perché il filtraggio è applicato sulla direzione in entrata di ogni interfaccia. In alcune circostanze limitate, come un firewall con numerose interfacce interne, disponendone si può ridurre significativamente il numero di regole del firewall richieste. In tal caso, applicare le regole di uscita per il traffico Internet come regole in uscita sulla WAN per evitare di doverle duplicare per

ogni interfaccia interna. L'uso di filtri in entrata e in uscita rende una configurazione più complessa e più soggetta ad errori da parte dell'utente, ma può essere auspicabile in applicazioni specifiche.

12.6.1 Gruppi di interfaccia

I gruppi di interfaccia, discussi nei *gruppi di interfaccia*, sono un metodo per stabilire regole su più interfacce allo stesso tempo. Questo può semplificare alcune configurazioni di regole se regole simili sono richieste su molte interfacce nello stesso modo. Le regole del gruppo di interfacce, come le regole di interfaccia, vengono elaborate solo in direzione inbound. Le schede VPN per OpenVPN, L2TP, e il server PPPoE sono tutti gruppi di interfaccia speciali che vengono creati automaticamente dietro le quinte.

Ad esempio, un gruppo può essere utilizzato per una raccolta di interfacce, comprese tutte le interfacce di tipo LAN o DMZ, o per un gruppo di VLAN.

Nota: gruppi di interfaccia non sono efficaci con Multi-WAN perché le regole di gruppo non possono gestire correttamente le risposte. A causa di tale carenza, il traffico che corrisponde a una regola di gruppo su una WAN che non ha il gateway predefinito uscirà dalla WAN con il gateway predefinito, e non attraverso l'interfaccia in cui è entrato.

12.6.2 Ordine di elaborazione delle regole

Finora abbiamo parlato di come le regole vengono elaborate su una scheda di interfaccia, ma ci sono tre classi principali di regole: Regolari regole di interfaccia, Regole di fluttuazione, e regole per gruppo di interfacce (tra cui le regole delle schede VPN). L'ordine di trattamento di questi tipi è significativo, e funziona così:

1. Regole di fluttuazione
2. Regole del gruppo di interfacce
3. Regole di interfaccia

Le regole sono ordinate in questo modo nel vero e proprio schema di regole, bisogna tenerlo a mente quando si creano regole. Ad esempio, se un gruppo di interfacce contiene una regola per bloccare il traffico, questa regola non può essere sovrascritta una scheda interfaccia, poiché il traffico è già soggetto alla regola di gruppo, che è stata identificata per prima nello schema di regole.

Le regole vengono elaborate fino a quando non viene trovata una corrispondenza, tuttavia, quindi se un pacchetto non è abbinato nelle regole del gruppo, può ancora essere abbinato da una regola di interfaccia.

Un altro posto significativo in cui questo fattore entra in gioco è con le interfacce OpenVPN assegnate. Se c'è una regola «permettere tutto» nella scheda OpenVPN, questa viene abbinata alle regole del gruppo. Ciò significa che le regole nella scheda dell'interfaccia non si applicano. Questo può essere un problema se le regole OpenVPN devono avere risposta al fine di garantire alcune uscite di traffico attraverso la VPN.

Vedi anche:

Vedere *Ordine dell'elaborazione del NAT e del firewall* per un'analisi più dettagliata dell'elaborazione delle regole e del flusso attraverso il firewall, compreso come le regole NAT entrano in gioco.

12.6.3 Regole del firewall aggiunte automaticamente

Firew4LL aggiunge automaticamente le regole interne del firewall per una serie di motivi. Questa sezione descrive le regole aggiunte automaticamente e il loro scopo.

Regola Anti-blocco

Per evitare di bloccare un amministratore dall'interfaccia web, Firew4LL abilita una regola anti-blocco per impostazione predefinita. Questa è configurabile nella pagina **Sistema>Avanzate** sotto **Anti-blocco**. Questa regola aggiunta automaticamente permette il traffico da qualsiasi sorgente all'interno della rete contenente la regola, a qualsiasi protocollo di amministrazione firewall in ascolto sull'indirizzo IP LAN. Ad esempio, permette l'accesso alla porta TCP 443 per la WebGUI, alla porta TCP 80 per il reindirizzamento GUI e alla porta TCP 22 se SSH è abilitato. Se la porta WebGUI è stata modificata, la porta configurata è quella consentita dalla regola anti-blocco.

Negli ambienti sensibili alla sicurezza, la migliore pratica è disabilitare questa regola e configurare le regole LAN in modo che solo alias di host fidati possano accedere alle interfacce amministrative del firewall. Una migliore pratica è di non consentire l'accesso dalla LAN, ma solo da una rete di gestione amministrativa isolata.

Limitare l'accesso all'interfaccia amministrativa dalla LAN

In primo luogo, per configurare le regole del firewall come desiderato per limitare l'accesso all'interfaccia di gestione richiesta (interfacce). In questo tipico esempio di caso d'uso, sia SSH che HTTPS sono utilizzati per la gestione, in modo da creare un alias di porte di gestione che contiene queste porte (Figura *Alias per porte di gestione*).

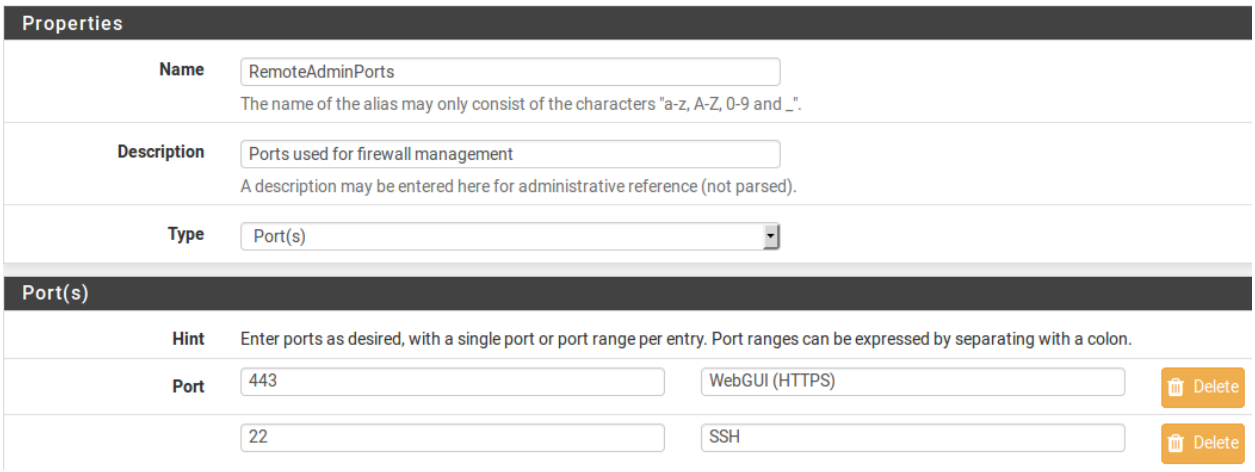


Fig. 17: Alias per porte di gestione

Quindi creare un alias per gli host e/o le reti che avranno accesso alle interfacce di gestione (Figure *Alias per gli host di gestione).*

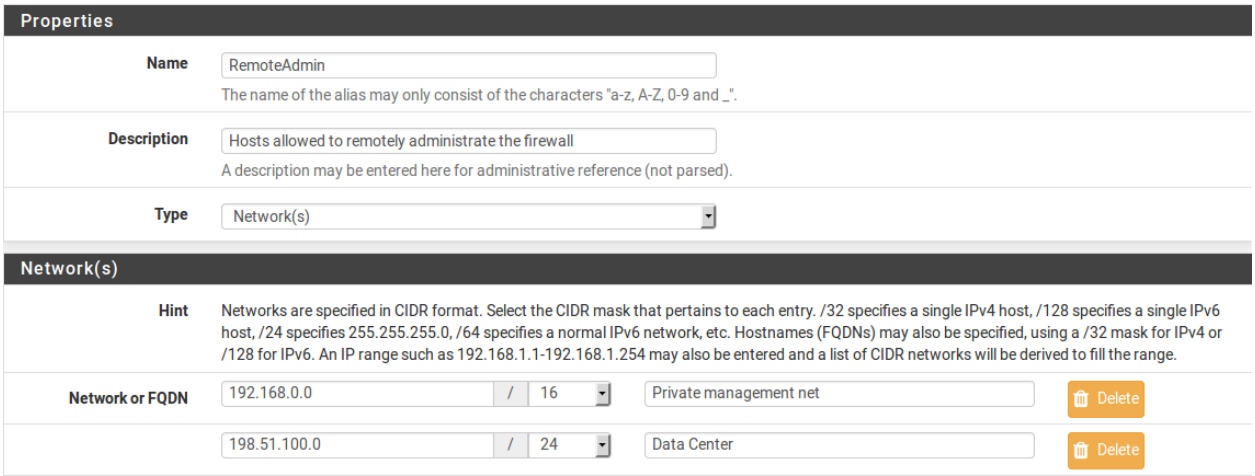


Fig. 18: Alias per gli host di gestione

Gli alias risultanti sono mostrati nella figura *Elenco degli alias*.

RemoteAdmin	192.168.0.0/16, 198.51.100.0/24
RemoteAdminPorts	443, 22

Fig. 19: Elenco degli alias

Quindi le regole del firewall LAN devono essere configurate per consentire l'accesso agli host precedentemente definiti, e negare l'accesso a tutti gli altri. Ci sono numerosi modi per realizzare questo, a seconda delle specifiche dell'ambiente e di come il filtraggio di uscita è gestito. La figura *Esempi di regole ristrette della LAN di gestione* mostra due esempi. Il primo permette le richieste DNS all'indirizzo IP LAN, che è necessario se il risolutore del DNS o il forwader del DNS sono abilitati, e permette che gli host LAN rintraccino l'indirizzo IP LAN. Poi rifiuta tutto l'altro traffico. Il secondo esempio permette l'accesso dagli host di gestione alle porte di gestione, quindi rifiuta tutto il resto del traffico alle porte di gestione. Scegliere la metodologia che funziona meglio per l'ambiente di rete in questione. Ricordare che la porta sorgente non è la stessa della porta di destinazione.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	✔ 0/0 B	IPv4 TCP/UDP	10.0.0.0/8	*	LAN address	53 (DNS)	*	none		Allow internal network to query the DNS Resolver
☐	✔ 0/0 B	IPv4 ICMP echoreq	10.0.0.0/8	*	LAN address	*	*	none		Allow internal network to ping the LAN IP Address
☐	✔ 0/0 B	IPv4 TCP	RemoteAdmin	*	LAN address	RemoteAdminPorts	*	none		Allow access to firewall management
☐	0/0 B	IPv4 *	*	*	LAN address	*	*	none		Reject everything else to the LAN IP address
☐	✔ 0/2.59 MiB	IPv4 *	10.0.0.0/8	*	*	*	*	none		LAN Traffic

Fig. 20: Esempi di regole ristrette della LAN di gestione

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	✔ 0/0 B	IPv4 TCP	RemoteAdmin	*	LAN address	RemoteAdminPorts	*	none		Allow access to firewall management
☐	0/0 B	IPv4 TCP	*	*	LAN address	RemoteAdminPorts	*	none		Reject access to firewall management from other host
☐	✔ 0/2.59 MiB	IPv4 *	10.0.0.0/8	*	*	*	*	none		LAN Traffic

Fig. 21: Esempio alternativo delle regole lan di gestione ristrette

Una volta configurate le regole del firewall, disabilitare la regola Webgui anti-blocco sulla Sistema>Avanzate (Figura *Regola anti-blocco disabilitata*). Selezionare la casella e fare clic su **Salva**.

Anti-lockout ☐ Disable webConfigurator anti-lockout rule

When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

Fig. 22: Regola anti-blocco disabilitata

Nota: Se l'interfaccia di gestione non è più accessibile dopo aver disabilitato la regola anti-blocco, le regole del firewall non sono state configurate in modo appropriato. Riattivare la regola anti-blocco utilizzando l'opzione **Impostare l'indirizzo IP dell'interfaccia (interfacce)** nel menu della console, quindi scegliere di ripristinare l'indirizzo IP LAN. Impostarlo al suo indirizzo IP attuale, e la regola verrà automaticamente riabilitata.

Regole anti-spoofing

Firew4LL utilizza la funzione antispoof in f4l per bloccare il traffico di spoof. Questo fornisce la funzionalità di Forwarding del percorso inverso unicast (Unicast Reverse Path Forwarding, uRPF) come definito in RFC 3704. Il firewall controlla ogni pacchetto rispetto alla sua tabella di instradamento, e se un tentativo di connessione viene da un indirizzo IP di origine su un'interfaccia dove il firewall sa che la rete non risiede, viene eliminato. Ad esempio, un pacchetto che arriva in WAN con un indirizzo IP sorgente di una rete interna viene eliminato. Tutto ciò che viene avviato sulla rete interna con un indirizzo IP sorgente che non si trova sulla rete interna viene eliminato.

Blocco delle reti private

L'opzione **Bloccare le reti private** sull'interfaccia WAN inserisce automaticamente una regola di blocco per le sottoreti RFC 1918. A meno che lo spazio IP privato non sia in uso sulla WAN, abilitare questa opzione. Questo vale solo per il traffico avviato sul lato WAN. I client locali possono comunque raggiungere gli host su reti private dall'interno del firewall. Questa opzione è disponibile per qualsiasi interfaccia, ma è generalmente utilizzata solo su interfacce tipo WAN. Una regola simile può essere creata manualmente per bloccare le reti private sulle interfacce creando un alias contenente le sottoreti RFC 1918 e aggiungendo una regola firewall alla parte superiore delle regole di interfaccia per bloccare il traffico con una fonte che corrisponde a tale alias. (Vedere *Indirizzi IP privati* per maggiori informazioni sugli indirizzi IP privati).

Block delle reti bogon

Le reti Bogon sono quelle che non dovrebbero mai essere viste su Internet, compreso lo spazio riservato e non assegnato di indirizzo IP. La presenza di traffico da queste reti potrebbe indicare sia il traffico spoof o una sottorete inutilizzata che è stata dirottata per uso dannoso. Firew4LL fornisce due elenchi di bogon che vengono aggiornati come necessario, uno per le reti di bogon IPv4 e uno per le reti di bogon IPv6. Se l'opzione **Bloccare le reti bogon** è abilitata, il firewall recupera un elenco aggiornato di bogon il primo giorno di ogni mese dal file.lfirew4lll.org. Lo script viene eseguito alle 3:00 a.m. ora locale, e dorme una quantità casuale di tempo fino a 12 ore prima di eseguire l'aggiornamento. Questo elenco non cambia molto frequentemente, e nuove assegnazioni di indirizzi IP vengono rimosse dalla lista bogon mesi prima che siano effettivamente utilizzate, quindi un aggiornamento mensile è adeguato. Se l'elenco deve essere aggiornato più frequentemente, cambiare la frequenza di aggiornamento per i bogon in **Sistema>Avanzate** nella scheda del **Firewall e NAT**.

Nota: L'elenco bogon per IPv6 è abbastanza grande e potrebbe non essere caricato se non c'è abbastanza memoria nel sistema, o se il numero massimo di voci della tabella non è abbastanza grande da contenerlo. Vedere *Entrate massime della tabella del Firewall* per informazioni sulla modifica di tale valore.

Assicurarsi che il firewall possa risolvere i nomi host del DNS, altrimenti l'aggiornamento fallirà. Per garantire che il firewall risolva il DNS, navigare fino a **Diagnostica>Cercare DNS**, e provare a risolvere files.lfirew4lll.org. Se questo funziona, poi andare a **Diagnostica>Porta di prova** e cercare di connettersi a file.lfirew4lll.org sulla porta 80, come dimostrato nella figura *Test di connettività per gli aggiornamenti bogon*.

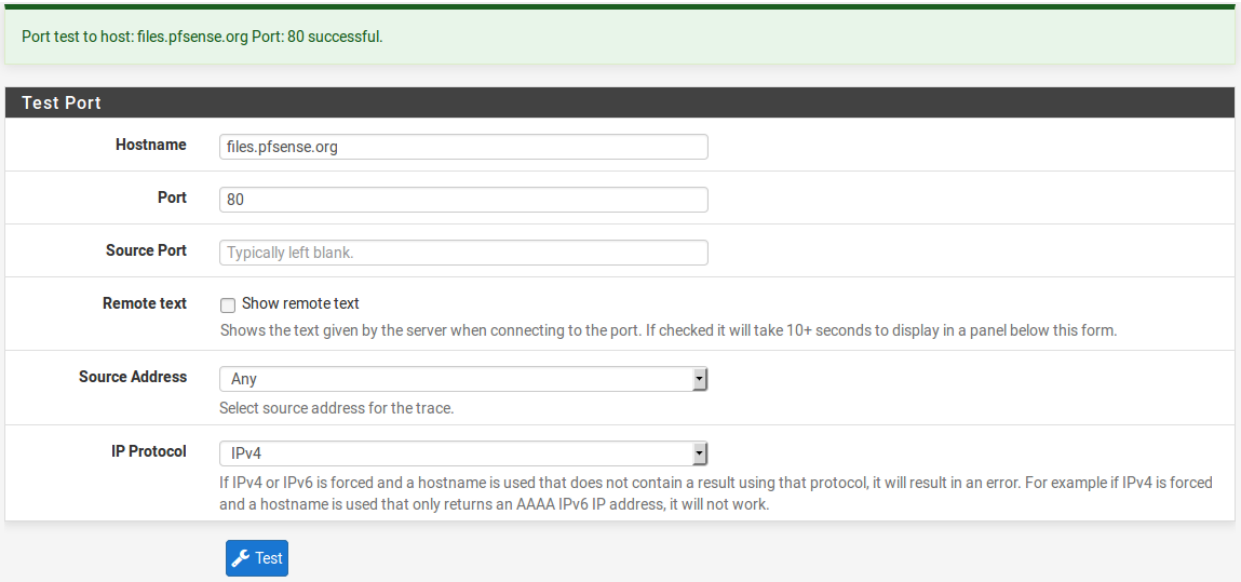


Fig. 23: Test di connettività per gli aggiornamenti bogon

Forzare un aggiornamento bogon

Con le modifiche relativamente rare all'elenco dei bogon e l'avviso preventivo di nuove assegnazioni pubbliche di IP, un aggiornamento mensile dei bogon è adeguato. Tuttavia ci possono essere scenari in cui un aggiornamento manuale bogon può aiutare, come ad esempio se gli aggiornamenti bogon sono stati in difetto a causa di una configurazione DNS errata. Eseguire un aggiornamento tramite l'interfaccia web del firewall a **Diagnostica>Tabelle**, selezionando bogon o bogonsv6 quindi fare clic su **Aggiornamento**.

IPsec

Quando una connessione da sito a sito IPsec è abilitata, vengono aggiunte automaticamente regole che consentono l'accesso remoto all'indirizzo IP dell'endpoint tunnel alle porte UDP 500 e 4500, e il protocollo ESP sull'indirizzo IP della WAN utilizzato per la connessione. Quando IPsec per i client mobili è abilitato lo stesso traffico è consentito, ma da una fonte qualsiasi, piuttosto che da un indirizzo sorgente specifico.

A causa del modo in cui la politica di routing funziona, qualsiasi traffico che corrisponda a una regola che specifica un gateway sarà forzato su Internet e bypasserà l'elaborazione IPsec. Le regole vengono aggiunte automaticamente per negare le politica del routing per il traffico destinato alle sottoreti VPN remote, ma non sempre hanno l'effetto desiderato. Per disabilitare le regole di negazione automatica, vedere *Disabilitare le regole di negazione* e aggiungere una regola di firewall in cima alle regole dell'interfaccia interna per far pasaare il traffico sulla VPN *senza un gateway impostato*.

Vedi anche:

Le regole IPsec aggiunte automaticamente vengono discusse in modo più approfondito in *IPsec*.

Regola Default Deny

Le regole che non corrispondono a nessuna delle regole definite dall'utente e a nessuna delle altre regole aggiunte automaticamente vengono silenziosamente bloccate dalla regola di default sulla negazione (come discusso in *Negazione predefinita*).

12.7 Configurazione delle regole del firewall

Quando si configurano le regole del firewall sotto **Firewall>Regole** molte opzioni sono disponibili per controllare come il traffico è abbinato e controllato. Ognuna di queste opzioni sono elencate in questa sezione.

12.7.1 Azione

Questa opzione specifica se la regola farà passere, bloccherà o rifiuterà il traffico.

Pass Un pacchetto corrispondente a questa regola potrà passare attraverso il firewall. Se il tracciamento dello stato è abilitato per la regola, viene creata una voce della tabella di stato che permette al relativo traffico di ritorno di passare. Vedere *Filtraggio stateful* per ulteriori informazioni.

Blocco Un pacchetto corrispondente a questa regola verrà scartato.

Rifiuto Un pacchetto che corrisponda a questa regola verrà scartato e per i protocolli supportati, verrà inviato un messaggio verrà all'originatore indicando che la connessione è stata rifiutata.

Vedi anche:

Vedere *Blocco contro rifiuto* per una descrizione più approfondita delle opzioni e per un aiuto nella decisione tra Blocco e rifiuto.

12.7.2 Disabilitato

Per disabilitare una regola senza rimuoverla dall'elenco delle regole, selezionare questa casella. Si mostrerà ancora nella schermata delle regole del firewall, ma la regola apparirà in grigio per indicare il suo stato disabilitato.

12.7.3 Interfaccia

Il menù a discesa dell'**interfaccia** specifica che il traffico di ricezione di interfaccia deve essere controllato da questa regola. Ricordare che sulle regole della tabella di interfaccia e di gruppo, il traffico viene filtrato solo sull'interfaccia in cui il traffico *viene avviato*. Il traffico avviato dalla LAN è destinato a Internet o da qualsiasi altra interfaccia sul firewall viene filtrato dall'insieme di regole LAN.

12.7.4 Versione TCP/IP

Ordina la regola di applicare per IPv4, IPv6, o entrambi i traffici IPv4+IPv6. Le regole corrisponderanno solo ai pacchetti che corrispondono al protocollo corretto. Possono essere utilizzati alias che contengono entrambi i tipi di indirizzi IP e la regola corrisponderà solo agli indirizzi del protocollo corretto.

12.7.5 Protocollo

Il protocollo a cui questa regola corrisponderà. La maggior parte di queste opzioni sono auto-esplicative. TCP/UDP corrisponderà sia al traffico TCP che a quello UDP. Specificando l'ICMP verrà mostrata un'ulteriore casella a discesa per selezionare il tipo di ICMP. Sono disponibili anche molti altri protocolli comuni.

Nota: Questo campo di default è TCP per una nuova regola perché è un'impostazione predefinita comune e mostrerà i campi previsti per quel protocollo. Per far sì che la regola si applichi a qualsiasi protocollo,cambiare questo campo in *qualsiasi*. Uno degli errori più comuni nella creazione di nuove regole è la

creazione accidentale di una regola TCP che non faccia passare altro traffico non-TCP come il ping, DNS, ecc.

12.7.6 Tipo ICMP

Quando ICMP è selezionato come protocollo, questo menu a discesa contiene tutti i possibili tipi di ICMP da abbinare. Quando si passa a ICMP, la migliore pratica è quella di superare i tipi richiesti solo quando possibile. Il caso d'uso più comune è quello di far passare solo un tipo di richiesta Echo che permetterà ad un ping ICMP di passare.

Suggerimento: Storicamente, ICMP ha una cattiva reputazione, ma è generalmente vantaggioso e non merita questa reputazione sulle reti moderne. Consentire un tipo ICMP *qualsiasi* è generalmente accettabile quando si consente ICMP.

12.7.7 Sorgente

Questo campo specifica l'indirizzo IP sorgente, la sottorete o l'alias che corrispondono a questa regola.

Il menu a discesa per la sorgente consente diversi tipi di sorgenti predefinite:

Qualsiasi Indirizzo che corrisponde.

Singolo host o Alias Corrisponde a un singolo indirizzo IP o nome alias. Quando questo è attivo, un nome alias può essere digitato nel campo **Indirizzo della sorgente**.

Rete Utilizza sia un indirizzo IP che una maschera di sottorete per abbinare una serie di indirizzi.

Client PPPoE Una macro che corrisponderà sl traffico della gamma di indirizzi client per il server PPPoE se il server PPPoE è abilitato.

Client L2TP Una macro che corrisponde al traffico dell'intervallo di indirizzi client per il server L2TP se il server L2TP è abilitato.

Interfaccia di rete Una voce in questa lista è presente per ogni interfaccia del firewall. Queste macro specificano esattamente la sottorete per tale interfaccia, comprese eventuali sottoreti VIP alias IP che differiscono dalla sottorete di interfaccia definita.

Indirizzo d'interfaccia Una voce in questa lista è presente per ogni interfaccia del firewall. Queste macro specificano l'indirizzo IP configurato su tale interfaccia.

Avvertimento: La scelta della rete WAN per origine o destinazione significa solo la sottorete dell'interfaccia WAN. Non significa «Internet» o qualsiasi host remoto.

Per le regole corrispondenti a TCP e/o UDP, la porta di origine può anche essere specificata facendo clic su **Visualizzare avanzate**. La porta sorgente è nascosta dietro il pulsante **Visualizzare Avanzate** perché normalmente la porta sorgente deve rimanere impostata su *qualsiasi*, perché le connessioni TCP e UDP sono provenienti da una porta casuale nell'intervallo di porta effimera (tra 1024 e 65535, l'intervallo esatto utilizzato varia a seconda del sistema operativo e la versione OS che sta avviando la connessione). La porta di origine non è quasi mai la stessa della porta di destinazione, e non dovrebbe mai essere configurata come tale a meno che l'applicazione in uso non sia nota per utilizzare questo comportamento atipico. È anche sicuro definire una porta sorgente come un intervallo da 1024 a 65535.

Selezionando **Invertire corrisondenza** verrà negata la corrispondenza in modo che tutto il traffico tranne questo valore sorgente attiverà la regola.

12.7.8 Destinazione

Questo campo specifica l'indirizzo IP di destinazione, la sottorete o l'alias che corrispondono a questa regola. Vedere la descrizione dell'opzione **Sorgente** in *Sorgente* per maggiori dettagli.

Per le regole che specificano TCP e/o UDP, la porta di destinazione, l'intervallo delle porte o l'alias sono specificati anche qui. A differenza della sorgente, la configurazione di una porta di destinazione è necessaria in molti casi, in quanto è più sicuro che utilizzare *qualsiasi* e la porta di destinazione di solito sarà nota in anticipo sulla base del protocollo. Molti valori delle porte comuni sono disponibili negli elenchi a discesa, o selezionare (*altro*) per inserire un valore manualmente o per utilizzare un alias di porta.

Suggerimento: Per specificare una gamma continua di porte, immettere la porta inferiore nella sezione **Da** e il valore della porta superiore nella sezione **A**.

12.7.9 Registro

Questa casella determina che, se i pacchetti che corrispondono a questa regola, saranno registrati nel registro del firewall. La registrazione è discussa più dettagliatamente nelle *Pratiche di registrazione*.

12.7.10 Descrizione

Inserire una descrizione qui per riferimento. Questa è facoltativa e non influisce sulla funzionalità della regola. La migliore pratica è quella di inserire un testo che descriva lo scopo della regola. La lunghezza massima è di 52 caratteri.

12.7.11 Opzioni avanzate

Opzioni, meno probabili siano richieste o che hanno funzionalità che confondono i nuovi utenti, sono state nascoste in questa sezione della pagina. Fare clic su  **Visualizzare Avanzate** per visualizzare tutte le opzioni avanzate. Se è stata impostata un'opzione in questa sezione della pagina, apparirà quando la regola verrà caricata in futuro.

OS sorgente

Una delle caratteristiche più uniche di f4l e quindi Firew4LL è la capacità di filtrare in base al sistema operativo che avvia una connessione. Per le regole TCP, f4l consente il rilevamento delle impronte digitali del sistema operativo passivo («p0f») che consente di allineare le regole in base al sistema operativo che avvia la connessione TCP. La funzione p0f di f4l determina il sistema operativo in uso confrontando le caratteristiche del pacchetto TCP SYN che avvia le connessioni TCP con un file di impronte digitali. Si noti che è possibile modificare le impronte digitali di un sistema operativo per assomigliare a un altro sistema operativo, soprattutto con sistemi operativi open source come BSD e Linux. Questo non è facile, ma se una rete contiene utenti tecnicamente abili con livello d'accesso amministratore o root ai sistemi, è possibile.

Diffserv code point

Un punto del codice dei servizi differenziati è un modo per le applicazioni per indicare all'interno dei pacchetti come dovrebbero preferire i router per trattare il loro traffico perché venga inoltrato lungo il suo percorso. L'uso più comune di questo è per la qualità del servizio o per la finalità della configurazione del traffico. Il nome lungo è spesso abbreviato in *Diffserv Code Point* o abbreviato come *DSCP* e talvolta indicato come il *campo TOS*.

Il programma o dispositivo che genera i pacchetti, ad esempio Asterisk tramite i suoi parametri di configurazione tos_sip e tos_audio, imposterà il campo DSCP nei pacchetti e poi dipenderà dal firewall e da altri router intermedi abbinare e accodare o agire sui pacchetti.

Per far corrispondere questi parametri nel firewall, utilizzare la voce del menù a discesa **Diffserv Code Point** che corrisponde al valore impostato dal dispositivo di origine. Ci sono numerose opzioni, ognuna con un significato speciale specifico per il tipo di traffico. Consultare la documentazione relativa al dispositivo che ha dato origine al traffico per maggiori dettagli sui valori da confrontare.

Il rovescio della medaglia del DSCP è che assume il supporto router o agisce sul campo, e ciò può essere o non essere una cosa da fare. Router diversi possono trattare lo stesso valore DSCP in modo indesiderato o non corrispondente. Peggio ancora, alcuni router possono deselezionare completamente il campo DSCP nei pacchetti man mano che li inoltra. Inoltre, da momento che f4l corrisponde al traffico, il valore DSCP deve essere impostato sul primo pacchetto di una connessione che crea uno stato, poiché ogni pacchetto non viene ispezionato individualmente una volta creato uno stato..

Nota: Questa opzione può solo leggere e corrispondere al valore DSCP. Non imposta un valore nei pacchetti.

Opzioni IP

Selezionando questa casella i pacchetti con opzioni IP definite potranno passare. Per default, f4l blocca tutti i pacchetti che hanno opzioni IP impostate per impedire le impronte digitali del sistema operativo, tra le altre ragioni. Marcare questa casella per far passare IGMP o altro traffico multicast contenente opzioni IP.

Disabilitare «risposta a» (Reply-To)

Il firewall aggiunge la parola chiave di reply-to per le regole sulle interfacce di tipo WAN per impostazione predefinita per garantire che il traffico che entri in una WAN parta anche attraverso la stessa WAN. In alcuni casi questo comportamento è indesiderabile, come quando un certo traffico è instradato tramite un firewall/router separato sull'interfaccia WAN. In questi casi, selezionare questa opzione per disabilitare la risposta solo per il traffico che corrisponda a questa regola, piuttosto che disabilitare reply-to globalmente..

TAG e TAGGED

I campi **TAG** e **TAGGED** sono utili in concerto con le regole variabili, quindi il firewall può contrassegnare un pacchetto con una stringa specifica quando entra in un'interfaccia, e agire in modo diverso su un pacchetto abbinato all'uscita con una regola variabile. Vedere *Marcatura e corrispondenza* per maggiori informazioni su questo argomento.

Massime voci di stato che questa regola può creare

Questa opzione limita il numero massimo di connessioni, totali, che può essere consentito da questa regola. Se più connessioni corrispondono a questa regola mentre è al suo limite di connessione, questa regola verrà saltata nella valutazione delle regole. Se una regola successiva corrisponde, il traffico ha l'azione di quella regola applicata, altrimenti

colpisce la regola di default di negazione. Una volta che il numero di connessioni consentite da questa regola scende al di sotto di questo limite di connessione, il traffico può ancora una volta corrispondere a questa regola.

Numero massimo di host di origine unici

Questa opzione specifica quanti indirizzi IP di origine totali possono connettersi simultaneamente per questa regola. Ogni indirizzo IP di origine è consentito per un numero illimitato di connessioni, ma il numero totale di indirizzi IP di origine distinti permesso è limitato a questo valore.

Numero massimo di connessioni stabilite per host

Per limitare l'accesso in base alle connessioni per host, utilizzare questa impostazione. Questo valore può limitare una regola ad un numero specifico di connessioni per host sorgente (ad es. 10), invece di un totale specifico di connessioni globale. Questa opzione controlla quante connessioni (handshake complete) completamente stabilite sono permesse per ogni host che corrisponde alla regola. Questa opzione è disponibile solo per l'utilizzo con connessioni TCP

Numero massimo di voci di stato per host

Questa impostazione funziona in modo simile al conteggio stabilito descritto sopra, ma controlla solo le voci di stato piuttosto che monitorare se una connessione è stata effettuata con successo.

Numero massimo di nuove connessioni al secondo

Questo metodo di limitazione della velocità aiuta a garantire che un alto tasso di connessioni TCP non sovraccarichi un server o la tabella di stato sul firewall. Ad esempio, i limiti possono essere posti sulle connessioni in entrata ad un server di posta, riducendo l'onere di essere sovraccarichi dagli spambot (bot di spam). Può anche essere utilizzato su regole di traffico in uscita per impostare limiti che impedirebbero a qualsiasi singola macchina di caricare la tabella di stato sul firewall o fare troppe connessioni rapide, comportamenti che sono comuni con i virus. Una quantità di connessioni e un numero di secondi per il periodo di tempo possono essere configurati per la regola. Qualsiasi indirizzo IP che superi il numero specificato di connessioni entro il periodo di tempo specificato sarà bloccato dal firewall per un'ora. Dietro le quinte, questo è gestito dalla tabella virusprot, chiamata così per il suo tipico scopo di protezione dai virus. Questa opzione è disponibile solo per l'utilizzo con connessioni TCP.

Timeout di stato in secondi

Usando questo campo, può essere definito un timeout di stato per il traffico che corrisponda a questa regola, sovrascrivendo il timeout di stato predefinito. Tutte le connessioni inattive saranno chiuse quando la connessione è stata inattiva per questo periodo di tempo. Il timeout di stato di default dipende dall'algoritmo di ottimizzazione del firewall in uso. Le scelte di ottimizzazione sono coperte in *Opzioni di ottimizzazione del firewall*.

Nota: Questa opzione controlla solo il traffico in direzione diarrivo, quindi non è molto utile da solo. Il traffico in uscita per una connessione corrispondente avrà comunque il timeout di stato predefinito. Per utilizzare correttamente questa impostazione, è richiesta anche una regola variabile corrispondente nel percorso in uscita preso dal traffico con una impostazione simile di timeout di stato.

Flag TCP

Per impostazione predefinita, le nuove regole di passaggio per TCP controllano solo l'impostazione del flag TCP SYN, fuori da un possibile set di SYN e ACK. Per tenere conto di scenari più complessi, come l'utilizzo di instradamenti asimmetrici o altre combinazioni non tradizionali di flusso di traffico, utilizzare questa serie di controlli per modificare il modo in cui i flag sono abbinati alla regola firewall.

La prima riga controlla quali flag devono essere impostati per corrispondere alla regola. La seconda riga definisce l'elenco dei flag che verranno consultati sul pacchetto per cercare una corrispondenza.

I significati dei flag più comunemente utilizzati sono:

SYN Sincronizza i numeri di sequenza. Indica un nuovo tentativo di connessione.

ACK Indica il riconoscimento ACK dei dati. Queste sono le risposte per far sapere al mittente che i dati sono stati ricevuti come OK.

FIN Indica che non ci sono più dati dal mittente, chiudendo una connessione.

RST Ripristino della connessione. Questo flag è impostato quando si risponde ad una richiesta di apertura di una connessione su una porta che non ha un daemon in ascolto. Può anche essere impostato da un software di firewall per allontanare connessioni indesiderabili.

PSH Indica che i dati devono essere spinti o lavati, compresi i dati in questo pacchetto, passando i dati fino all'applicazione.

URG indica che il campo urgente è significativo, e questo pacchetto dovrebbe essere inviato prima dei dati che non sono urgenti.

Per consentire il TCP con eventuali flag impostati, selezionare **Qualsiasi flag**.

Tipo di stato

Ci sono tre opzioni per il tracciamento dello stato in Firew4LL che possono essere specificate in base alla regola:

Mantenere Quando selezionata, il firewall creerà e manterrà una voce nella tabella di stato per il traffico consentito. Questa è l'impostazine di default, e la scelta migliore nella maggior parte delle situazioni.

stato Approssimativi (sloppy) Sloppy è un mezzo meno rigoroso di mantenere lo stato che è destinato per gli scenari con instradamento asimmetrico. Quando il firewall può vedere solo la metà del traffico di una connessione, i controlli di validità dello stato predefinito si guasteranno e il traffico sarà bloccato. I meccanismi in f4l che impediscono certi tipi di attacchi non si attiveranno durante un controllo di stato approssimativo.

Synproxy Questa opzione fa in modo che Firew4LL gestisca connessioni TCP in arrivo per il proxy. Le connessioni TCP iniziano con un handshake a tre vie. Il primo pacchetto di una connessione TCP è un SYN dalla sorgente, che suscita una risposta SYN ACK dalla destinazione, poi un ACK in cambio dalla sorgente per completare la stretta di mano. Normalmente l'host dietro il firewall gestirà la cosa da solo, ma lo stato synproxy fa in modo che il firewall completi questa stretta di mano. Questo aiuta a proteggere da un tipo di attacco DoS, le inondazioni di SYN. Questo è tipicamente usato solo con le regole sulle interfacce WAN. Questo tipo di attacco è oggi meglio gestito a livello del sistema operativo di destinazione, perché ogni moderno sistema operativo include le capacità di gestirlo da solo. Poiché il firewall non può sapere quali estensioni TCP supporta l'host back-end, quando si utilizza lo stato di synproxy, si annuncia che non sono supportate estensioni TCP. Questo significa che le connessioni create che utilizzano lo stato di synproxy non utilizzeranno la scala delle finestre, SACK, né timestamp che porterà a prestazioni significativamente ridotte nella maggior parte dei casi. Può essere utile quando si aprono porte TCP ad host che non gestiscono bene gli abusi di rete, dove le prestazioni migliori non sono un problema.

Niente Questa opzione non manterrà lo stato su questa regola. Questo è necessario solo in alcuni scenari avanzati altamente specializzati, nessuno dei quali è coperto in questo libro perché estremamente raro.

> **Nota:** L'impostazione **Niente** qui riguarda solo il traffico in direzione di arrivo, quindi non è molto utile di per sé in quanto uno stato sarà ancora creato in direzione di uscita. Deve essere accoppiato con una regola variabile nella direzione di uscita che ha anche la stessa opzione scelta.

Nessuna sincronizzazione XML-RPC

Selezionando questa casella si impedisce questa regola di sincronizzazione con altri membri del cluster di elevata disponibilità tramite XMLRPC. Questo argomento è trattato in *Elevata disponibilità*. Ciò non impedisce che una regola su un nodo secondario sia sovrascritta dal primario.

Priorità VLAN (Corrispondenza e impostazione)

802.1p, noto anche come IEEE P802.1p o Punto del codice di priorità (Priority Code Point), è un modo per abbinare e taggare i pacchetti con una specifica qualità della priorità di un servizio. A differenza di DSCP, 802.1p opera al livello 2 con VLAN. Tuttavia, come DSCP, il router upstream deve anche supportare 802.1p perché sia utile.

Ci sono due opzioni in questa sezione. La prima corrisponderà ad un campo 802.1p in modo che il firewall possa agire su di esso. Il secondo inietterà un tag 802.1p in un pacchetto mentre passa attraverso questo firewall. Alcuni ISP possono richiedere un tag 802.1p da impostare in alcune aree, come la Francia, al fine di gestire correttamente voce/video/dati su VLAN segregate alla giusta priorità per garantire la qualità.

Ci sono otto livelli di priorità per 802.1p, e ciascuno ha un codice di due lettere nella GUI. Nell'ordine dalla priorità più bassa alla più alta, sono:

BK Sfondo

BE Massimo sforzo

EE Sforzo eccellente

CA Applicazioni critiche

VI Video

VO Voce

IC Controllo del lavoro interno

NC Controllo della rete

Programma

Questa opzione configura una pianificazione che specifica i giorni e gli orari di applicazione della regola. Selezionando «ninte» la regola sarà sempre abilitata. Per ulteriori informazioni, vedere le *regole basate sul tempo* più avanti in questo capitolo.

Gateway

Questa opzione configura un gateway o un gruppo di gateway da utilizzare per il traffico che corrisponde a questa regola. Questo è incluso nella politica di routing.

Pipe di In/Out (limitatori)

Queste selezioni elencano i limitatori definiti per applicare un limite di larghezza di banda al traffico che entra in questa interfaccia (In) e che esce da questa interfaccia (Out). Maggiori dettagli sui limitatori si possono trovare in *limitatori*.

Ackqueue (coda ACK) / queque (coda)

Queste opzioni definiscono quali code di traffico ALTQ vengono applicate al traffico che entra ed esce da questa interfaccia. Per ulteriori informazioni sulla configurazione del traffico, vedere *Shaper del traffico*.

12.8 Regole variabili (floating)

Le **regole variabili** sono un tipo speciale di regole avanzate che possono eseguire azioni complicate che non sono possibili con regole su schede di interfaccia o di gruppo. Le regole variabili possono agire su più interfacce in arrivo, in uscita, o in entrambe le direzioni. L'uso di filtri in entrata e in uscita rende la progettazione delle regole più complesse e soggette ad errori da parte dell'utente, ma possono essere desiderabili in applicazioni specifiche.

La maggior parte delle configurazioni del firewall non avranno mai regole variabili, o le hanno solo dal regolatore del traffico.

12.8.1 Precauzioni/Avvertenze

Le regole variabili possono essere molto più potenti di altre regole, ma anche più confuse, ed è più facile fare un errore che potrebbe avere conseguenze indesiderate nel passaggio o nel blocco del traffico.

Le regole variabili nella direzione di arrivo, applicate a più WAN, non riceveranno reply-to aggiunto come accadrebbe con le regole di interfaccia individuali, quindi lo stesso problema esiste qui come esisteva con i gruppi di interfaccia: Il traffico uscirà sempre dalla WAN con il gateway predefinito, e non restituirà correttamente la WAN che ha inserito.

Data la relativa mancanza di familiarità di molti utenti con le regole variabili, questi potrebbero non pensare di cercare lì per le regole quando si compie la manutenzione del firewall. Così, per l'amministrazione può essere un po" più difficile, in quanto non può essere un luogo ovvio per cercare regole.

Fare attenzione quando si considerano la fonte e la destinazione dei pacchetti a seconda della direzione di arrivo e di uscita. Per esempio, le regole nella direzione di uscita su una WAN avrebbero la sorgente locale del firewall (dopo il NAT) e la destinazione remota.

12.8.2 Utilizzo potenziale

L'uso più comune di regole variabili è per la modellazione del traffico ALTQ. Le regole di tabulazione variabili sono l'unico tipo di regole che possono far corrispondere e mettere in coda il traffico senza farlo passare esplicitamente.

Un altro modo di usare le regole variabili è controllare il traffico che parte dal firewall stesso. Le regole floating possono impedire al firewall di raggiungere specifici indirizzi IP, porte e così via.

Altri usi comuni sono quelli di garantire che nessun traffico possa uscire da altri percorsi in una rete sicura, a prescindere dalle regole esistenti su altre interfacce. Bloccando l'uscita verso una rete sicura da tutte le località tranne quelle approvate, la probabilità di consentire in seguito il traffico accidentalmente attraverso un altro percorso indesiderato è ridotta. Allo stesso modo, possono essere utilizzate per evitare che il traffico destinato alle reti private lasci un'interfaccia WAN, per evitare perdite di traffico VPN.

Come accennato in precedenza nelle regole di interfaccia, essi possono anche efficacemente emanare timeout di stato, tag/corrispondenza di operazioni, regole di "nessuno stato", e regole di "stato approssimativo" per l'instradamento asimmetrico.

12.8.3 Ordine di elaborazione

Nella direzione in entrata, le regole variabili funzionano essenzialmente allo stesso modo delle regole di interfaccia o di gruppo, salvo che esse sono elaborate per prime. Nella direzione di uscita, però, le cose diventano un po" più confuse.

Le regole del firewall sono elaborate dopo le regole NAT, quindi le regole in direzione di uscita su una WAN non possono mai corrispondere a un indirizzo IP locale/privato se il NAT in uscita è attivo su quell'interfaccia. Quando si tocca la regola, l'indirizzo sorgente del pacchetto è ora l'indirizzo IP dell'interfaccia WAN. Nella maggior parte dei casi questo può essere risolto utilizzando le opzioni di corrispondenza per contrassegnare un pacchetto sulla LAN durante l'ingresso e quindi la corrispondenza con quel tag durante l'uscita dal firewall.

Le regole variabili vengono elaborate prima delle regole del gruppo di interfaccia e delle regole di interfaccia, in modo che possano essere prese in considerazione.

12.8.4 Azione di corrispondenza (match)

L'azione di *corrispondenza* è unica per le regole variabili. Una regola con l'azione *match* non fa passare o blocca un pacchetto, ma lo abbina solo allo scopo di assegnare traffico a code o limitatori per la configurazione del traffico. Le regole di corrispondenza non funzionano con l'opzione *Rapido* abilitata.

12.8.5 Rapido (quick)

Rapido controlla se l'elaborazione delle regole si interrompe quando una regola è abbinata. Il comportamento **rapido** viene aggiunto a tutte le regole della scheda interfaccia automaticamente, ma sulle regole variabili è opzionale. Senza l'opzione *rapido* selezionata, la regola avrà effetto solo se nessun'altra regola corrisponde al traffico. Questo inverte il comportamento di «la prima corrispondenza vince» diventando «l'ultima corrispondenza vince».

Utilizzando questo meccanismo, si può creare un'azione di tipo predefinito che avrà effetto solo quando non corrispondono altre regole, come le regole predefinite sulle WAN.

Nella maggior parte dei casi, si consiglia di avere **rapido** selezionata. Ci sono alcuni scenari specifici in cui lasciare **rapido** deselezionata è necessario, ma sono pochi e lontani tra loro. Per la maggior parte degli scenari, le uniche regole che dovrebbero essere senza rapido selezionata sono le regole del moderatore del traffico delle regole di corispondenza.

12.8.6 Interfaccia

La selezione dell"**interfaccia** per le regole variabili è diversa da quella per le regole di interfaccia normali: si tratta di una casella multi-selezione in modo da poter selezionare una, più interfacce o tutte le interfacce possibili. Fare click+Ctrl sulle interfacce per selezionarle una per una, o utilizzare altre combinazioni di click/trascinare o shift-click per selezionare più interfacce.

12.8.7 Direzione

Le regole variabili non si limitano alla direzione in entrata come le regole di interfaccia. Esse possono anche agire nella direzione di uscita selezionando qui, o in entrambe le direzioni selezionando qualsiasi. La direzione *in entrata* è anche disponibile

La direzione *in uscita* è utile per filtrare il traffico dal firewall stesso, per abbinare altro traffico indesiderato che cerchi di uscire da un'interfaccia, o per configurare completamente le regole dello «stato approssimativo», le regle di «nessuno stato» regole, o timeout di stato alternativo.

12.8.8 Marcatura e corrispondenza

Utilizzando i campi **Taggare** e **Taggato**, una connessione può essere contrassegnata da una scheda di interfaccia e poi abbinata in direzione di uscita su una regola variabile. Questo è un modo utile per agire sul traffico WAN in uscita da uno specifico host interno che non potrebbe essere altrimenti abbinato a causa del NAT che mascheri la fonte. Può anche essere utilizzato in modo simile per l'applicazione della modellazione in uscita sulla WAN da traffico specificamente taggato sulla via per il firewall firewall.

Ad esempio, su una regola LAN, utilizzare una stringa corta nel campo **Taggare** per contrassegnare un pacchetto da una sorgente di 10.3.0.56. Poi su una regola variabile, rapida, in uscita sulla WAN, usare **Taggato** con la stessa stringa per agire sul traffico corrispondente alla regola LAN.

12.9 I metodi di utilizzo di ulteriori indirizzi IP pubblici

I metodi di diffusione di ulteriori indirizzi IP pubblici variano a seconda del modo in cui gli indirizzi sono delegati, della dimensione della locazione e degli obiettivi per l'ambiente specifico della rete. Per utilizzare ulteriori indirizzi IP pubblici con NAT, ad esempio, il firewall avrà bisogno di indirizzi IP virtuali.

Ci sono due opzioni per assegnare direttamente indirizzi IP pubblici agli host: sottoreti IP pubbliche instradate e ponte.

12.9.1 Scegliere tra di routing, bridging e NAT

Ulteriori indirizzi IP pubblici possono essere utilizzati assegnandoli direttamente sui sistemi che li utilizzeranno o utilizzando il NAT. Le opzioni disponibili dipendono dalla locazione degli indirizzi da parte dell'ISP.

Ulteriori indirizzi IP statici

I metodi di utilizzo di indirizzi IP pubblici statici aggiuntivi variano a seconda del tipo di assegnazione. Ciascuno degli scenari comuni è descritto qui.

Sottorete dell'IP unica sulla WAN

Con un'unica sottorete pubblica IP sulla WAN, uno degli indirizzi IP pubblici sarà sul router upstream, comunemente appartenente all'ISP, e un altro degli indirizzi IP sarà assegnato come indirizzo IP suula WAN su Firew4LL. Gli indirizzi IP rimanenti possono essere utilizzati sia con NAT, sia tramite bridging o con una combinazione dei due.

Per utilizzare gli indirizzi con NAT, aggiungere Proxy ARP, alias di IP o indirizzi IP virtuali di tipo CARP.

Per assegnare indirizzi IP pubblici direttamente agli host dietro il firewall, un'interfaccia dedicata per questi host deve essere collegata alla WAN. Quando usati con il bridging, gli host con gli indirizzi IP pubblici direttamente assegnati devono usare lo stesso gateway predefinito del WAN del firewall: il router ISP di upstream. Questo creerà difficoltà se gli host con indirizzi IP pubblici hanno bisogno di avviare le connessioni agli host dietro altre interfacce del firewall, dal momento che il gateway ISP non instrada il traffico per le sottoreti interne al firewall.

La figura *Più indirizzi IP pubblici in uso sulla sottorete IP unica* mostra un esempio di utilizzo di più indirizzi IP pubblici in un unico blocco con una combinazione di NAT e bridging.

Vedi anche:

Per informazioni sulla configurazione, NAT viene ulteriormente trattatonella sezione *Traduione dell'indirizzo di rete* e il bridging in *Bridging*.

Piccola sottorete IP della wan con una più grande sottorete dell'IP della LAN

Alcuni ISP locheranno una piccola sottorete IP come assegnazione del «lato WAN», a volte è chiamata rete di trasporto o di interconnessione, e instraderanno una più grande sottorete «interna» al firewall. Comunemente questo è un /30 sul lato WAN e un /29 o più grande per l'uso interno del firewall. Al router del fornitore di servizi viene assegnato un estremo del /30, di solito l'indirizzo IP più basso, e al firewall viene assegnato l'indirizzo IP più alto. Il fornitore poi instrada la seconda sottorete all'indirizzo IP della WAN del firewall. La sottorete dell'IP aggiuntivo può essere utilizzata dal firewall su un'interfaccia LAN o OPT con un'interfaccia pubblica con indirizzi IP assegnati direttamente agli host, con NAT che utilizzano altri tipi di VIP, o una combinazione dei due. Poiché gli indirizzi IP sono indirizzati al firewall, non è necessario ARP quindi le voci VIP non sono necessarie per l'uso con NAT.

Poiché Firew4LL è il gateway del segmento locale, l'instradamento dagli host di sottorete locale pubblica alla LAN è molto più facile che nello scenario bridge richiesto quando si utilizza una singola sottorete IP pubblica. La figura *Indirizzi IP pubblici multipli che usano due sottoreti IP* mostra un esempio che combina una sottorete IP instradata e il NAT. L'instradamento degli indirizzi IP pubblici è spiegato in *Instradamento degli indirizzi IP pubblici* e il NAT nella *traduzione degli indirizzi di rete*.

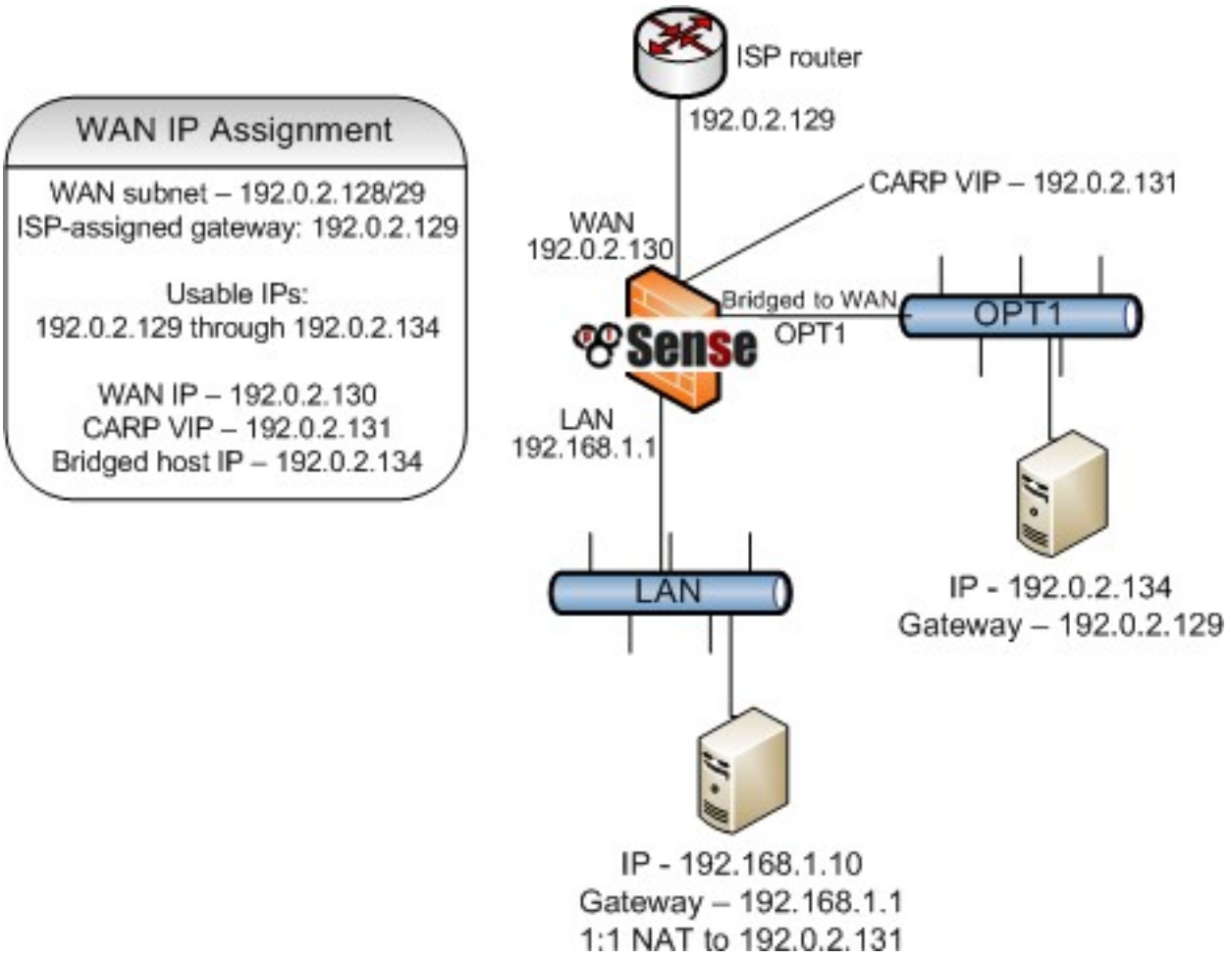


Fig. 24: Più indirizzi IP pubblici in uso sulla sottorete IP unica

Se il firewall fa parte di un cluster ad alta disponibilità che utilizza CARP, la sottorete di lato WAN dovrà essere un /29 in modo che ogni firewall abbia il proprio indirizzo IP della WAN più un VIP del CARP in questo tipo di configurazione. Il fornitore invierà la rete interna più grande al VIP del CARP della WAN. La sottorete IP interna deve essere indirizzata ad un indirizzo IP che è sempre disponibile indipendentemente dal firewall attivo, e la più piccola sottorete utilizzabile con CARP è una /29. Tale configurazione con CARP è la stessa illustrata sopra, con il gateway OPT1 è un VIP del CARP, e il provider di routing a un VIP del CARP piuttosto che l'indirizzo IP della WAN. CARP è illustrato in *Alta disponibilità*.

Sottoreti IP multiple

In altri casi, un sito può ricevere dall'ISP più sottoreti IP. Di solito quando questo accade, il sito ha iniziato con una delle due disposizioni precedentemente descritte, e più tardi quando si richiedono ulteriori indirizzi IP il sito è stato fornito con un ulteriore sottorete IP. Idealmente, questa sottorete aggiuntiva sarà instradata al firewall dall'ISP, sia al suo indirizzo Ip di WAN nel caso di un singolo firewall, o a unVIP del CARP quando si utilizza l'alta disponibilità. Se il fornitore rifiuta di instradare la sottorete IP al firewall, ma piuttosto la instrada al proprio router e utilizza uno degli indirizzi IP della sottorete come indirizzo IP del gateway, il firewall dovrà usare i VIP del Proxy ARP, il VIP Alias dell'IP, o una combinazione di IP Alias e VIP del CARP per la sottorete aggiuntiva. Se possibile, il fornitore dovrebbe instradare la sottorete IP al firewall in quanto rende più facile lavorare indipendentemente dal firewall utilizzato. Elimina inoltre la necessità di masterizzare 3 indirizzi IP nella sottorete aggiuntiva, uno per gli indirizzi di rete e broadcast e uno per l'indirizzo IP del gateway. Con una sottorete instradata, l'intera sottorete è utilizzabile in combinazione con il NAT.

Se la sottorete IP è indirizzata al firewall, lo scenario descritto in *Piccole sottoreti dell'IP della WAN si sottoreti più grandi dell'Ip della LAN* si applica ad una sottorete interna aggiuntiva. La sottorete può essere assegnata a una nuova interfaccia OPT, utilizzata con NAT, o una combinazione dei due.

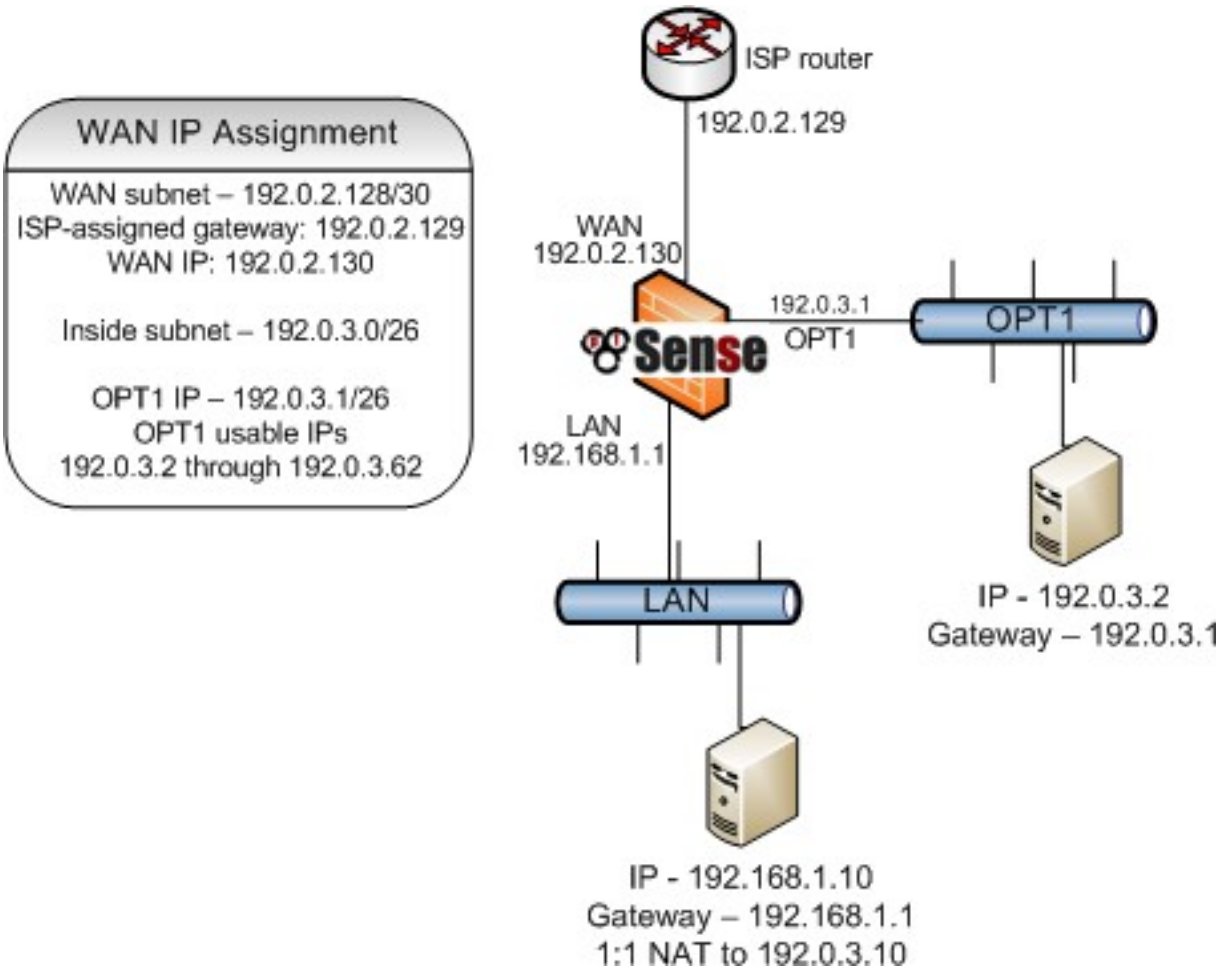


Fig. 25: Indirizzi IP pubblici multipli che usano due sottoreti IP

Ulteriori indirizzi IP tramite DHCP

Alcuni ISP richiedono ulteriori indirizzi IP da ottenere tramite DHCP. Questo non è un buon mezzo per ottenere più indirizzi IP pubblici, e deve essere evitato in qualsiasi rete seria. Una connessione business-class non dovrebbe richiedere questo. Firew4LL è uno dei pochi firewall che possono essere utilizzati in qualsiasi capacità con indirizzi IP aggiuntivi da DHCP. Questo offre una flessibilità limitata in ciò che il firewall può fare con questi indirizzi, lasciando solo due opzioni possibili.

Bridging

Se gli indirizzi IP aggiuntivi di DHCP devono essere assegnati direttamente ai sistemi che li utilizzeranno, il collegamento è l'unica opzione. Utilizzare un'interfaccia OPT collegata con WAN per questi sistemi, e i sistemi devono essere configurati per ottenere i loro indirizzi utilizzando DHCP.

Pseudo multi-WAN

L'unica opzione per fare in modo che il firewall estragga questi indirizzi DHCP come leasing è una pseudo distribuzione multi-WAN. Installare un'interfaccia di rete per indirizzo IP pubblico e configurare ciascuna per DHCP. Collegare tutte le interfacce con uno switch tra il firewall e il modem o router. Dal momento che il firewall avrà più interfacce

che condividono un singolo dominio di broadcast, consentire **la soppressione dei messaggi ARP** sulla scheda di **Networking** in **Sistema>Avanzate**, per eliminare gli avvisi ARP nel registro di sistema, che sono normali in questo tipo di distribuzione.

L'unico uso di indirizzi IP pubblici assegnati in questo modo è per l'inoltro delle porte. Le porte d'inoltro possono essere utilizzate su ogni interfaccia WAN che utilizza un indirizzo IP assegnato a tale interfaccia dal server DHCP dell'ISP. Il NAT in uscita per le OPT della WAN non funzionerà a causa della limitazione per cui ogni WAN deve avere un indirizzo IP gateway unico per dirigere correttamente il traffico fuori da tale WAN. Questo è discusso ulteriormente in *Connessioni WAN multiple*.

12.10 Indirizzi IP virtuali (VIP)

Firew4LL consente l'uso di più indirizzi IP in combinazione con il NAT o servizi locali attraverso IP virtuali (VIP).

Ci sono quattro tipi di indirizzi IP virtuali disponibili in Firew4LL: *Alias dell'IP*, *CARP*, *Proxy ARP* e *altri*. Ciascuno è utile in situazioni diverse. Nella maggior parte dei casi, Firew4LL dovrà rispondere alla richiesta ARP di un VIP, il che significa che devono essere utilizzati alias IP, Proxy ARP o CARP. In situazioni in cui non è richiesto ARP, ad esempio quando ulteriori indirizzi IP pubblici sono indirizzati da un fornitore di servizi all'indirizzo WAN IP sul firewall, utilizzare altri tipi di VIP.

Firew4LL non risponderà ai ping destinati all'ARO del Proxy e a VIP di altro tipo indipendentemente dalla configurazione delle regole del firewall. Con l'ARP del Proxy e VIP di altri tipi, il NAT deve essere presente sul firewall, inoltrando il traffico ad un host interno perché il ping funzioni. Per ulteriori informazioni, vedere *Traduzione indirizzi di rete*.

12.10.1 Alias dell'IP

Gli alias IP funzionano come qualsiasi altro indirizzo IP su un'interfaccia, come l'indirizzo IP dell'interfaccia. Risponderanno al livello 2 (ARP) e possono essere utilizzati come indirizzi vincolanti dai servizi sul firewall. Possono anche essere utilizzati per gestire più sottoreti sulla stessa interfaccia. Firew4LL risponderà al ping su un alias IP, e i servizi sul firewall che si collegano a tutte le interfacce risponderanno anche su VIP dell'alias di IP a meno che il VIP non sia usato per inoltrare le porte ad un altro dispositivo (ad es. il NAT 1:1).

I VIP di alias IP possono usare *host locali* come interfaccia per collegare i servizi che usano indirizzi IP da un blocco di indirizzi instradati senza assegnare specificamente gli indirizzi IP ad un'interfaccia. Questo è utile principalmente in HA con scenari CARP in modo che gli indirizzi IP non debbano essere consumati da una configurazione CARP (un IP per ciascun nodo, poi il resto come VIP del CARP) quando la sottorete esiste solo all'interno del firewall (ad es. NAT o servizi firewall come VPN).

Gli alias IP da soli non si sincronizzano con i peer di sincronizzazione di configurazione XMLRPC, perché ciò comporterebbe un conflitto di indirizzi IP. Un'eccezione sono i VIP dell'alias dell'IP che utilizzano una "interfaccia" con VIP del CARP per la loro interfaccia. Quelli non si traducono in un conflitto perchè si sincronizzano. Un'altra eccezione sono i VIP dell'alias dell'IP legati agli host locali come interfaccia. Poiché questi non sono attivi al di fuori del firewall stesso, non c'è possibilità di un conflitto nella sincronizzazione.

12.10.2 Proxy ARP

I VIP del Proxy ARP funzionano strettamente al livello 2, fornendo risposte ARP per l'indirizzo IP specificato o per l'intervallo CIDR di indirizzi IP. Questo permette a Firew4LL di accettare traffico mirato a quegli indirizzi all'interno di una sottorete condivisa. Ad esempio, Firew4LL può inoltrare il traffico inviato a un indirizzo aggiuntivo all'interno della sua sottorete WAN secondo la sua configurazione NAT. L'indirizzo o l'intervallo di indirizzi non sono assegnati a nessuna interfaccia su Firew4LL, perché non è necessario che lo siano. Questo significa che nessun servizio su Firew4LL può rispondere su questi indirizzi IP.

I VIP dell'ARP del proxy non si sincronizzano con i peer della sincronizzazione della configurazione XML-RPC perché così facendo causerebbero un conflitto di indirizzo IP.

12.10.3 CARP

I VIP del CARP sono utilizzati principalmente con le distribuzioni ridondanti ad elevata disponibilità che utilizzano CARP. I VIP del CARP hanno ognuno il proprio indirizzo MAC derivato dal loro VHID, che può essere utile anche al di fuori di una distribuzione ad elevata disponibilità.

Vedi anche:

Per informazioni sull'uso di dei VIP del CARP, vedere *elevata disponibilità*.

I VIP del CARP possono essere usati anche con un solo firewall. Questo viene fatto tipicamente nei casi in cui la distribuzione Firew4LL sarà infine convertita in un nodo cluster della HA, o quando avere un indirizzo MAC unico è un requisito. In rari casi un fornitore richiede che ogni indirizzo IP univoco su un segmento WAN abbia un indirizzo MAC distinto, fornito dai VIP del CARP.

I VIP del CARP e degli Alias dell'IP possono essere combinati in due modi:

- Per ridurre la quantità di heartbeat del CARP impilando VIP dell'alias dell'IP su VIP del CARP. Vedere *Uso di alias di IP per ridurre il traffico di heartbeat*.
- Usare i VIP del CARP in sottoreti multiple su una singola interfaccia. Vedere *Interfaccia*.

12.10.4 Altro

Altri tipi VIP definiscono indirizzi IP aggiuntivi da utilizzare quando non sono necessarie risposte ARP per l'indirizzo IP. L'unica funzione dell'aggiunta di VIP di *altro tipo* è quella di rendere tale indirizzo disponibile nei selettori a discesa della configurazione del NAT. Questo è conveniente quando il firewall ha un blocco dell'IP pubblico instradato al suo indirizzo IP della WAN, alias dell'IP, o un VIP del CARP.

12.11 Regole basate sul tempo

Le regole basate sul tempo consentono alle regole del firewall di attivarsi nei giorni e/o intervalli di tempo specificati. Le regole basate sul tempo funzionano allo stesso modo di qualsiasi altra regola, tranne che esse non sono effettivamente presenti nello schema al di fuori degli orari previsti.

12.11.1 Logica delle regole basate sul tempo

Quando si tratta di regole basate sul tempo, lo schema determina quando applicare l'azione specificata nella regola firewall. Quando l'ora o la data corrente non sono coperte dalla pianificazione, il firewall agisce come se la regola non ci fosse. Per esempio, una regola che passa il traffico di sabato la bloccherà solo in altri giorni se sotto di essa esiste una regola a blocchi separata. Le regole vengono elaborate dall'alto verso il basso, come le altre regole del firewall. Viene usata la prima corrispondenza, e una volta trovata una corrispondenza, viene intrapresa un'azione se la regola è in programma, e non vengono valutate altre regole.

Suggerimento: Bisogna ricordare quando si usano gli orari che la regola non avrà **alcun effetto** al di fuori degli orari programmati. La regola **non** avrà la sua azione invertita perché l'ora attuale non rientra tempo previsto. La mancata considerazione di questo comportamento potrebbe portare a dare ai client l'accesso indesiderato al di fuori delle fasce di tempo definite in un programma.

12.11.2 Configurare gli orari delle regole basate sul tempo

Gli orari devono essere definiti prima di poter essere usati sulle regole del firewall. Gli orari sono definiti sotto **Firewall>Orari**, e ogni programma può contenere intervalli di tempo multipli. Nel seguente esempio, una società vuole negare l'accesso a HTTP durante le ore di lavoro, e consentirlo tutte le altre volte del giorno

Definire i tempi per una pianificazione

Per aggiungere un programma:

- Passare a **Firewall>Orari**
- Fare clic su **Aggiungere** per aprire la schermata di modifica della pianificazione, come si vede in figura *Aggiungere un intervallo di tempo*.
- Inserire un **nome per la pianificazione**. Questo è il nome che apparirà nell'elenco di selezione per l'uso nelle regole del firewall. Proprio come i nomi di alias, questo nome deve contenere solo lettere e cifre, senza spazi. Ad esempio: orariodilavoro
- Inserire una **descrizione** di questo orario, come le ore di lavoro normali.
- Definire uno o più intervalli di tempo:
- Impostare il **mese** selezionando un mese e dei giorni specifici, o facendo clic sul giorno dell'inizio della settimana per gli orari settimanali ricorrenti.
- Scegliere **un'ora di inizio** e un"**ora di arresto** che controllano quando la regola è attiva nei giorni selezionati. L'ora non può attraversare la mezzanotte in qualsiasi giorno. Un giorno intero è dalle *0:00* alle *23:59*.
- Indicare una facoltativa **descrizione dell'intervallo di tempo** per questo intervallo specifico, ad es. settimana lavorativa
- Fare clic su **Aggiungere tempo** per aggiungere la scelta come intervallo
- Ripetere il **mese**, il **tempo** e i passi per gli intervalli supplementari
- Fare clic su **Salva**

Una pianificazione può applicarsi a giorni specifici, come il 2 settembre 2016, o a giorni della settimana, come il lunedì-mercoledì. Per selezionare un giorno qualsiasi entro l'anno successivo, scegliere il mese dall'elenco a discesa, quindi fare clic sul giorno o giorni specifici sul calendario. Per selezionare un giorno della settimana, fare clic sul suo nome nelle intestazioni della colonna.

Per questo esempio, cliccare su **lun**, **mar**, **mer**, **gio**, e **ven**. Questo renderà il programma attivo per qualsiasi lunedì-venerdì, indipendentemente dal mese. Ora selezionare l'ora in cui questo programma sarà attivo, in formato 24 ore. Le ore per questo esempio sono dalle 9:00 alle 17:00 (5pm). Tutti gli orari sono indicati nel fuso orario locale.

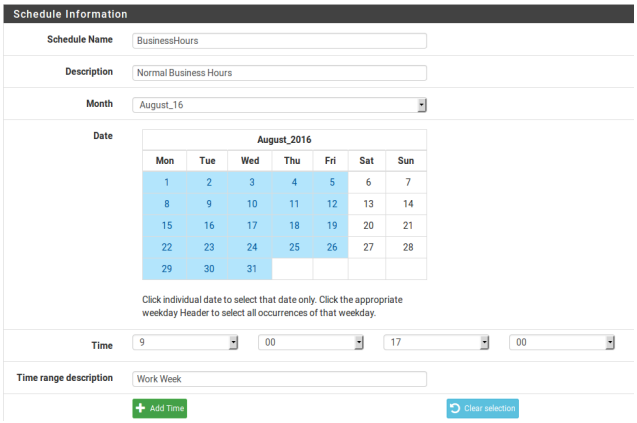


Fig. 26: Aggiungere un intervallo di tempo

Dopo che l'intervallo di tempo è stato definito, apparirà nella lista in fondo alla schermata di modifica del programma, come in figura *Intervallo di tempo aggiunto*.

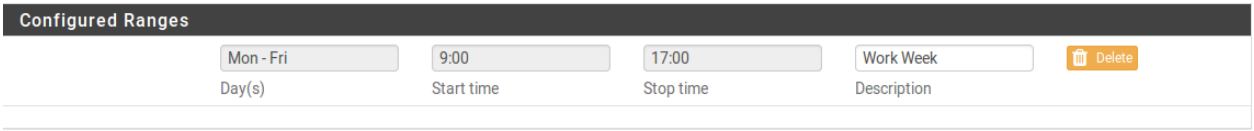


Fig. 27: Aggiunto Intervallo di tempo

Per espandere questa impostazione, ci può essere una mezza giornata il Sabato da definire, o forse il negozio si apre in ritardo il lunedì. In tal caso, definire un intervallo di tempo per i giorni identici, e poi un altro intervallo per ciascun giorno con diversi intervalli di tempo. Questa raccolta di intervalli di tempo sarà il programma completo.

Una volta che la voce di pianificazione è stata salvata, il browser tornerà all'elenco del programma, come in Figura *Lista degli orari dopo l'aggiunta*. Questo programma sarà ora disponibile per l'utilizzo nelle regole del firewall.

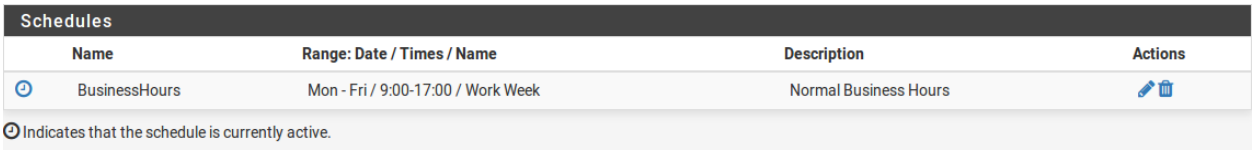


Fig. 28: Lista degli orari dopo l'aggiunta

Usare la pianificazione in una regola del firewall

Per creare una regola firewall che utilizzi questa pianificazione, creare una nuova regola sull'interfaccia desiderata. Vedere *Aggiungere una regola firewall* e *Configurare le regole firewall* per maggiori informazioni sull'aggiunta e la modifica delle regole. Per questo esempio, aggiungere una regola per rifiutare il traffico TCP sull'interfaccia LAN dalla sottorete LAN a qualsiasi destinazione sulla porta HTTP. Nelle opzioni avanzate per la regola, individuare l'impostazione dell'**orario** e scegliere il calendario degli *orari di lavoro*, come nella figura *Scegliere un oratio per una regola di firewall*.

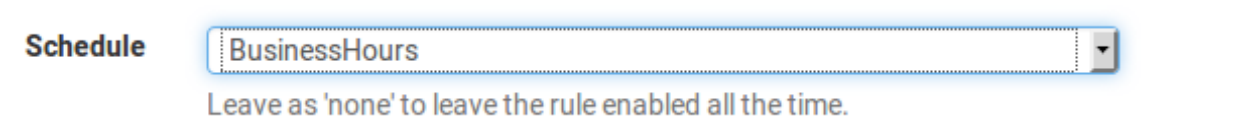


Fig. 29: Scegliere un orario per una regola del firewall

Dopo aver salvato la regola, il programma apparirà nell'elenco delle regole del firewall insieme ad un'indicazione dello stato attivo della pianificazione. Come mostrato nella figura *Elenco delle regole del firewall con orario*, questa è una regola di rifiuto, e la colonna di pianificazione indica che la regola è attualmente in stato di blocco attivo perché viene visualizzato in un momento all'interno dell'intervallo programmato. Se il cursore del mouse passa sopra l'indicatore di stato della pianificazione, un suggerimento viene visualizzato dal firewall che mostra come la regola si comporterà all'ora corrente. Dal momento che viene visualizzato all'interno dei tempi definiti nel calendario degli orari di lavoro, questo dirà «Il traffico corrispondente a questa regola è attualmente negato». Se c'è una regola di passaggio che corrisponderebbe al traffico sulla porta 80 dalla rete LAN dopo questa regola, allora sarebbe consentito al di fuori delle ore programmate.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	0/0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none	BusinessHours	Block HTTP access during business hours	

Fig. 30: Elenco delle regole del firewall con orario

Ora che la regola è definita, testarla sia all'interno che al di fuori degli orari previsti per garantire che il comportamento desiderato sia emanato.

Suggerimento: Per impostazione predefinita, gli stati sono cancellati per le connessioni attive consentite da una regola pianificata quando la pianificazione scade. Questo blocca l'accesso per chiunque sia autorizzato dalla regola mentre era attiva. Per consentire a queste connessioni di rimanere aperte, controllare **Non uccidere le connessioni quando la pianificazione** sotto **Sistema>Avanzate** nella scheda **Varie**.

12.12 Esaminare il registro del firewall

Il firewall crea le voci di registro per ogni regola configurata nel registro e per la regola di negazione predefinita. Ci sono diversi modi per visualizzare queste voci, ognuna con diversi livelli di dettaglio. Non c'è un metodo «migliore» chiaro in quanto dipende dalle preferenze e dal livello di abilità degli amministratori del firewall, anche se usare la GUI è il metodo più semplice

---

Suggerimento: Il comportamento di registrazione delle regole di negazione predefinite e di altre regole interne può essere controllato utilizzando la scheda **Impostazioni** sotto **stato>Registro di sistema**. Vedere *Modificare le impostazioni dei registri* per i dettagli.

Come altri registri in Firew4LL, i registri del firewall conservano solo un certo numero di voci che usano il formato del registro circolare binario, *clog*. Se le esigenze di un'organizzazione richiedono una registrazione permanente dei registri del firewall per un periodo di tempo più lungo, vedere *Registri di sistema* per informazioni sulla copia di queste voci di registro in un server del syslog quando essi accadono.

12.12.1 Visualizzazione della WebGUI

I registri del firewall sono visibili nella WebGUI in **stato>Registri di sistema**, nella scheda **Firewall**. Da lì, i registri possono essere visti come un registro analizzato, che è più facile da leggere, o come un registro grezzo, che contiene maggiori dettagli. C'è anche un'impostazione per mostrare queste voci in ordine crescente o inverso. Se l'ordine delle voci di registro visualizzate è sconosciuto, controllare l'orario della prima e dell'ultima riga, o selezionare *Modificare impostazioni di registro* per informazioni su come visualizzare e modificare queste impostazioni.

I log della WebGUI analizzati, visti nella figura *Esempio di voci di registro viste dalla WebGUI*, sono in 6 colonne: **Azione**, **Tempo**, **Interfaccia**, **Sorgente**, **Destinazione** e **Protocollo**.

Azione Mostra cosa è successo al pacchetto che ha generato la voce di registro (ad es. passaggio o blocco)

Ora L'ora in cui il pacchetto è arrivato.

Interfaccia Dove il pacchetto è entrato nel firewall.

Fonte L'indirizzo IP e la porta della sorgente.

Destinazione Indirizzo IP e porta di destinazione.

Protocollo Il protocollo del pacchetto, ad es. ICMP, TCP, UDP, ecc.

Action	Time	Interface	Source	Destination	Protocol
✖	Aug 3 08:59:02	WAN	198.51.100.1:67	198.51.100.2:68	UDP
✖	Aug 3 15:02:10	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:02:10	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:14:02	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:14:02	WAN	198.51.100.108:138	198.51.100.255:138	UDP

Fig. 31: Esempio di voci di registro viste dalla WebGUI

L'icona **Azione** è un collegamento che esegue la ricerca e visualizza la regola che ha causato la registrazione. Il più delle volte, questo dice «Regola di negazione predefinita», ma con i problemi di risoluzione delle regole può aiutare a restringere i sospetti.

Suggerimento: Nella scheda **Impostazioni** sotto **stato>Registri di sistema**, questa descrizione di regola può essere configurata per essere mostrata direttamente nelle voci di registro. Il firewall può visualizzare la descrizione in una colonna separata o in una riga separata. Vedere *Modificare le impostazioni del registro* per i dettagli.

Accanto agli indirizzi IP di sorgente e di destinazione si trova . Quando questa icona viene cliccata il firewall effettuerà una ricerca DNS sull'indirizzo IP. Se l'indirizzo ha un nome di host valido verrà visualizzato sotto l'indirizzo IP in tutte le istanze di quell'indirizzo nella pagina.

Le voci di registro per i pacchetti TCP contengono informazioni ulteriori aggiunte al campo del protocollo che visualizza i flag TCP presenti nel pacchetto. Questi flag indicano vari stati di connessione o attributi dei pacchetti. I flag comuni includono:

S - SYN Sincronizza i numeri di sequenza. Indica un nuovo tentativo di connessione quando è impostato solo SYN.

A - ACK Indica il riconoscimento dei dati. Queste sono le risposte per far sapere al mittente che i dati sono stati ricevuti come OK.

F - FIN Indica che non ci sono più dati dal mittente, chiudendo una connessione.

R - RST Ripristino della connessione. Questo flag è impostato quando si risponde ad una richiesta di apertura di una connessione su una porta che non ha un daemon in ascolto. Può anche essere messo dal software di firewall per allontanare connessioni indesiderabili.

Vedi anche:

Ci sono diversi altri flag e i loro significati sono delineati in molti materiali sul protocollo TCP. L'articolo di Wikipedia su TCP contiene maggiori informazioni.

L'output del registro mostrato nella GUI può essere filtrato per trovare voci specifiche, purché esistano nel log corrente.

Fare clic su per visualizzare le opzioni di filtraggio. Vedere *Filtrare le voci di registro* per maggiori informazioni.

L'aggiunta di regole firewall dalla vista del registro (regola semplice, Easy Rule)

La regola facile rende semplice aggiungere rapidamente le regole del firewall dalla vista di log del firewall.

L'icona  accanto all'indirizzo IP di sorgente aggiunge una regola di **blocco** per quell'indirizzo IP sull'interfaccia. Per essere più precisi, crea o aggiunge un alias contenente indirizzi IP aggiunti da Easy Rule e li blocca sull'interfaccia selezionata.

L'icona  accanto all'indirizzo IP di destinazione funziona in modo simile all'azione di blocco, ma aggiunge una regola di **passaggio** più precisa. Questa regola permette il traffico sull'interfaccia ma deve corrispondere allo stesso protocollo, indirizzo IP sorgente, indirizzo IP di destinazione e porta di destinazione.

Utilizzo di Easy rule per aggiungere le regole del firewall dalla shell

La versione shell di Easy Rule, easyrule, può essere usata per aggiungere una regola firewall da un prompt della shell. Quando comando easyrule viene eseguito senza parametri, un messaggio di utilizzo viene stampato per spiegare la sua sintassi.

Il modo in cui si aggiunge una regola di blocco che utilizza un alias, o una regola di passaggio precisa che specifica il protocollo, la sorgente e la destinazione, funziona in maniera analoga alla versione GUI. Ad esempio, per aggiungere una regola di blocco, eseguire:

```
# easyrule block wan 1.2.3.4
```

Una regola di passaggio deve essere più precisa:

```
# easyrule pass wan tcp 1.2.3.4 192.168.0.4 80
```

12.12.2 Visualizzazione del menù dalla console

I registri grezzi possono essere visualizzati e seguiti in tempo reale dal file filter.log utilizzando l'opzione 10 dal menu della console. Un esempio semplice è una voce di registro come quella vista sopra nella figura *Esempio di voci di registro viste dalla WebGUI*:

Aug 3 08:59:02 master filterlog: 5,16777216,,1000000103,igb1,match,block,in,4,0x10,,128,0,0,none,17,udp,328,198.51.100.1,198.51.100.2,67,68,308

Questo mostra che l'id 1000000103 è stato abbinato, che ha portato ad un'azione di blocco sull'interfaccia igb1. Gli indirizzi IP di sorgente e destinazione sono mostrati vicino alla fine della voce del registro, seguiti dalla porta di origine e destinazione. I pacchetti da altri protocolli possono mostrare significativamente più dati.

Vedi anche:

Il formato del file di registro dei filtri è descritto in dettaglionella wiki di documentazione di Firew4LL..

12.12.3 Visualizzazione dalla Shell

Quando si utilizza la shell, sia da SSH o dalla console, ci sono numerose opzioni disponibili per visualizzare i registri dei filtri.

Quando si visualizza direttamente il contenuto del file clog, le voci di registro possono essere abbastanza complesse e verbose.

Visualizzazione del contenuto attuale del file di registro

Il registro dei filtri è contenuto in un registro circolare binario quindi strumenti tradizionali come cat, grep, e così via non possono essere utilizzati direttamente sul file. Il registro deve essere riletto con il programma clog ed allora può essere intubato con un altro programma.

Per visualizzare l'intero contenuto del file di registro, eseguire il seguente comando:

```
# clog /var/log/filter.log
```

Per limitare l'output del log alle ultime righe, eseguirlo attraverso il comando tail:

```
#       clog /var/log/filter.log | tail
```

Seguire l'output del registro in tempo reale

Per «seguire» l'output del file di log, utilizzare il parametro -f per il colg. Questo è l'equivalente di tail -f per quelli abituati a lavorare con i file di log normali su sistemi UNIX:

```
# clog -f /var/log/filter.log
```

Questo produrrà l'intero contenuto del file di log, ma non si fermerà dopo. Attenderà invece più voci e le stamperà così come accadono. Questo output può essere eseguito anche su altri comandi, se necessario.

Visualizzazione dell'output del registro analizzato nella shell

C'è un registro analizzato semplice scritto in PHP che può essere usato dalla shell per produrre un output ridotto al posto del registro grezzo completo. Per visualizzare il contenuto analizzato del log corrente, eseguire:

```
# clog /var/log/filter.log | filterparser.php
```

L'output delle voci di log sono uno per riga, con output semplificato:

Aug 3 08:59:02 block igb1 UDP 198.51.100.1:67 198.51.100.2:68

Trovare la regola che ha causato una voce di registro

Quando si visualizza uno dei formati di registro grezzi, viene visualizzato il numero di identificazione di una voce. Questo numero di regola può essere usato per trovare la regola che ha causato la corrispondenza. Nell'esempio seguente, quale regola con id 1000000103:

```
# pfctl -vvsr | grep 1000000103
```

@5(1000000103) block drop in log inet all label «Default deny rule IPv4»

Come mostrato nell'output precedente, questa era la regola di default per negare IPv4.

12.12.4 Perché ci sono voci di registro bloccate per connessioni legittime?

A volte sono presenti voci di log che, mentre sono etichettate con la regola «Negazione predefinita», appaiono come se appartenessero a connessioni legittime. L'esempio più comune è vedere una connessione bloccata che coinvolge un server web.

È probabile che ciò accada quando un pacchetto FIN del TCP, che normalmente chiuderebbe la connessione, arriva dopo che lo stato della connessione è stato rimosso o quando un ACK viene ricevuto al di fuori del tempo di finestra accettabile. Questo accade perché a volte un pacchetto viene perso o ritardato e quelli trasmissi nuovamente vengono bloccati perché il firewall ha già chiuso la connessione.

Queste registrazioni sono innocue e non indicano una connessione effettivamente bloccata. Tutti i firewall statici lo fanno, anche se alcuni non generano messaggi di log per questo traffico bloccato anche quando tutto il traffico bloccato è registrato.

Questo comportamento sarà presente occasionalmente anche se esiste una regola per tipo «consentire tutto» su tutte le interfacce del firewall perché una regola impostata per «consentire tutto» per le connessioni TCP permette solo ai pacchetti SYN del TCP di creare uno stato. Tutti gli altri traffici TCP saranno parte di uno stato esistente nella tabella di stato, o saranno pacchetti con flag TCP falsificati o altrimenti non validi.

Una speciale variazione di questo comportamento che può indicare problemi è quando l'instradamento asimmetrico esiste su una rete. In questi casi saranno presenti voci di log che mostrano i pacchetti TCP:SA (SYN+ACK) bloccati piuttosto che FIN o RST. Vedere *Regole di bypass del firewall per il traffico sulla stessa interfaccia* e *Filtraggio della route statica* per informazioni su come gestire l'instradamento asimmetrico.

12.13 Come bloccare l'accesso a un sito Web?

Una domanda che ci viene posta molto spesso è «Come faccio a bloccare l'accesso a un sito web?» o per essere più precisi: «Come faccio a bloccare l'accesso a Facebook?» E non è sempre una domanda facile a cui rispondere. Ci sono diverse tattiche possibili per raggiungere l'obiettivo, alcuni sono discussi altrove nel libro.

12.13.1 Utilizzare il DNS

Se il Risolutore o il Forwader del DNS sono attivi è possibile inserire una modifica locale per risolvere il sito indesiderato a un indirizzo IP non valido come 127.0.0.1.

12.13.2 Utilizzare le regole firewall

Se un sito web cambia raramente gli indirizzi IP, l'accesso ad esso può essere bloccato utilizzando un alias contenente i suoi indirizzi IP e quindi utilizzando questo alias nelle regole del firewall. Questa non è una soluzione fattibile per i siti che restituiscono TTL bassi e diffondono il carico su molti server e/o centri dati, come Google e siti simili molto grandi. La maggior parte dei siti di piccole e medie dimensioni può essere efficacemente bloccato utilizzando questo metodo in quanto raramente cambiano gli indirizzi IP.

Un hostname può anche essere all'interno di un alias di rete. L'hostname verrà risolto periodicamente e aggiornato se necessario. Questo è più efficace che cercare manualmente gli indirizzi IP, ma sarà comunque breve se il sito restituisce i record del DNS in un modo che cambia rapidamente o randomizza i risultati da un pool di server su ogni query, che è comune per i grandi siti.

Un'altra opzione è trovare tutte le locazioni di sottorete dell'IP di un sito, creando un alias con queste reti, e bloccando il traffico verso quelle destinazioni. Questo è particolarmente utile con siti come Facebook che diffondono grandi quantità di spazio IP, ma sono vincolati all'interno di pochi blocchi di rete. L'utilizzo di siti di registro regionali come ARIN può contribuire a rintracciare tali reti. Per esempio, tutte le reti utilizzate da Facebook nella regione coperta da ARIN possono essere trovate all'indirizzo http://whois.arin.net/rest/org/THEFA-3.html sotto «Reti correlate». Le aziende possono avere altri indirizzi in diverse regioni, quindi bisogna controllare altri siti regionali, come RIPE, APNIC, ecc.

In alternativa alla ricerca dei blocchi IP manuale, localizzare il numero sel Sistema Autonomo (AS) BGP dell'azienda di destinazione facendo una ricerca whois su uno dei loro indirizzi IP, quindi utilizzarlo per trovare tutte le loro locazioni. Per esempio, il numero AS di Facebook è AS32934:

```
# whois -h whois.radb.net -- '-i origin AS32934' | awk '/^route:/ {print $2;}' | sort␣
↪| uniq
```

Copiare i risultati di quel comando in un nuovo alias e ciò coprirà tutte le loro reti attualmente assegnate. Controllare periodicamente i risultati per gli aggiornamenti.

Il pacchetto f4lBlocker offre meccanismi che possono essere utili in questo settore, come il DNSBL, il blocco dell'indirizzo IP geografico e l'automazione del processo di ricerca AS.

12.13.3 Utilizzare un proxy

Se il traffico web passa attraverso un server proxy, tale server proxy può probabilmente essere utilizzato per impedire l'accesso a questi siti. Per esempio, Squid ha un add-on chiamato squidguard che permette di bloccare i siti web da URL o altri criteri simili. C'è una breve introduzione a Squid e squidguard che si può trovare in *Una breve introduzione alle proxy del Web e al Reporting: Squid, squidguard e Lightsquid.*

12.13.4 Prevenire il bypass delle restrizioni

Con uno dei metodi di cui sopra, ci sono molti modi per aggirare i blocchi definiti. Il più semplice e probabilmente più diffuso è l'utilizzo di qualsiasi numero di siti web proxy. Trovare e bloccare tutti questi individualmente e mantenere l'elenco aggiornato è impossibile. Il modo migliore per garantire che questi siti non siano accessibili è utilizzare un proxy esterno o un filtro dei contenuti in grado di bloccare per categoria.

Per mantenere ulteriormente il controllo, utilizzare un codice di uscita restrittivo e consentire solo il traffico verso servizi specifici e/o host. Ad esempio, consentire solo l'accesso DNS al firewall o ai server DNS specificamente utilizzati per i client LAN. Inoltre, se un proxy è in uso sulla rete, assicurarsi di non consentire l'accesso diretto a HTTP e HTTPS attraverso il firewall e consentire solo il traffico verso e/o dal server proxy

12.14 Risoluzione dei problemi delle regole del firewall

Questa sezione fornisce una guida per la risoluzione dei problemi con le regole del firewall.

12.14.1 Controllare I registri del firewall

Il primo passo quando la risoluzione dei problemi sospetta il traffico bloccato è quello di controllare i registri firewall (**stato>Registri di sistema**, sulla scheda **Firewall**).

Per default Firew4LL registrerà tutto il traffico caduto e non registrerà il traffico passato. A meno che non esistano regole di blocco o di rigetto che non utilizzano la registrazione, tutto il traffico bloccato sarà registrato. Se non ci sono voci di registro con un'icona rossa  nei registri del firewall che corrispondono al traffico in questione, Firew4LL probabilmente non farà cadere il traffico..

12.14.2 Controllare la tabella di stato

Tentare una connessione e controllare immediatamente la tabella di stato in **Diagnostica>Stati** e il filtro sulla sorgente o sulla destinazione per vedere se uno stato esiste. Se è presente una voce della tabella di stato, il firewall ha superato il traffico.

Se la regola in questione è una regola di passaggio, l'entrata della tabella di stato significa che il firewall ha fatto passare il traffico e il problema può essere altrove e non sul firewall.

Se la regola è una regola di blocco e c'è una voce della tabella di stato, la connessione aperta non verrà interrotta. Per vedere un effetto immediato di una nuova regola di blocco, gli stati devono essere reimpostati. Vedere *Stati del firewall* per maggiori informazioni.

12.14.3 Revisione dei parametri della regola

Modificare la regola in questione e rivedere i parametri per ogni campo. Per il traffico TCP e UDP, ricordate che la porta sorgente non è quasi mai la stessa della porta di destinazione, e di solito dovrebbe essere impostata su *qualsiasi*.

Se la regola di default di negazione è da clpevolizzare, creare una nuova regola di passaggio che corrisponderà al traffico da consentire. Se il traffico è ancora bloccato, ci può essere qualche altro aspetto speciale dei pacchetti che richiedono una gestione aggiuntiva nella configurazione delle regole. Per esempio, può essere necessario **abilitare opzioni IP** per il traffico multicast, oppure le voci di log possono essere dovute ad un instradamento asimmetrico, oppure i pacchetti possono avere una combinazione non valida di parametri come un pacchetto frammentato con «Non frammentare» impostato all'interno.

> **Vedi anche:**
>
> Per informazioni su come gestire l'instradamento asimmetrico, vedere *Regole di bypass del firewall per il traffico sulla stessa interfaccia* e *Filtraggio della route statica*.

In tali casi avanzati, l'esecuzione di un pacchetto di cattura per il traffico in questione può aiutare a diagnosticare il problema. Fare riferimento a *Cattura dei pacchetti* per maggiori informazioni su come catturare e analizzare i pacchetti.

12.14.4 Revisione dell'ordine delle regole

Ricordate che per le regole della scheda di interfaccia, la prima regola corrispondente vince - ulteriori regole vengono valutate.

12.14.5 Regole e interfacce

Assicurarsi che le regole sono sulla corretta interfaccia per funzionare come previsto. Il traffico è filtrato solo dalle regole configurate sull'interfaccia in cui viene avviato il traffico. Il traffico proveniente da un sistema sulla LAN destinato ad un sistema su qualsiasi altra interfaccia è filtrato solo dalle regole LAN. Lo stesso vale per tutte le altre interfacce.

12.14.6 Abilitare la registrazione della regola

Determinare quale regola corrisponde al traffico in questione. I contatori di hit nell'elenco delle regole possono aiutare in qualche modo. Abilitando le regole di accesso, i registri del firewall mostreranno una singola voce specifica per determinare quale regola ha superato la connessione.

12.14.7 Risoluzione dei problemi con la cattura dei pacchetti

Le acquisizioni di pacchetti possono essere preziose per la ricerca di guasti e il debug di problemi di traffico. Con la cattura di un pacchetto, è facile dire se il traffico sta raggiungendo l'interfaccia esterna o lasciando un'interfaccia interna, tra i molti altri usi. Vedere *Cattura dei pacchetti* per maggiori dettagli sulla risoluzione dei problemi con le acquisizioni dei pacchetti.

12.14.8 Le nuove regole non vengono applicate

Se una nuova regola non sembra applicarsi, ci sono un paio di spiegazioni possibili.

In primo luogo, se la regola è una regola di blocco e c'è una voce della tabella di stato, la connessione aperta non verrà tagliata. Vedere *Controllare la tabella di stato*.

In secondo luogo, lo schema di regole potrebbe non ricaricarsi correttamente. Controllare **stato>Ricarica del filtro** per vedere se viene visualizzato un errore. Fare clic sul pulsante  **Ricarica del filtro** in quella pagina per forzare una nuova ricarica del filtro. Se viene visualizzato un errore, risolvere il problema come necessario. Se la causa non è ovvia, consultare il supporto per l'assistenza.

Se nessuna delle cause di cui sopra sono da colpevolizzare, è possibile che la regola non abbia corrispondenza con tutti, quindi bisogna revisionare il traffico e la regola di nuovo.

12.14.9 Altre cause

Ci sono altre insidie nelle regole del firewall, NAT, routing e progettazione della rete che possono interferire con la connettività. Vedere l'articolo della wiki doc sulla *risoluzione dei problemi di connettività* per ulteriori suggerimenti.

> **Vedi anche:**
>
> Per ulteriori informazioni, è possibile accedere all'archivio Hangouts per visualizzare l'hangout di giugno 2016 sulla risoluzione dei problemi della connettività che contiene procedure di risoluzione dei problemi molto più dettagliate.

Una delle funzioni principali svolte da Firew4LL è quella di filtrare il traffico. Questo capitolo tratta i fondamenti del firewall, le migliori pratiche e le informazioni necessarie per configurare le regole del firewall.

CAPITOLO 13

NAT (Network Address Translation)

13.1 Porte d'inoltro (Port Forward)

Il port forward consente l'accesso dall'esterno a una porta specifica, a un intervallo di porte o a un protocollo su un dispositivo di rete interno. Il nome «port forward» è stato scelto perché è quello che la maggior parte delle persone capisce in questo contesto, ed è stato preferito rispetto a quello più tecnicamente appropriato di «NAT d'entrata» dopo innumerevoli reclami da utenti confusi. Una funzionalità simile è chiamata «NAT di destinazione» in altri prodotti. Tuttavia, «Port Forward» è un nome improprio, perché le regole delle port forward possono reindirizzare i protocolli GRE e ESP in aggiunta alle porte TCP e UDP, e possono essere utilizzate per vari tipi di reindirizzamento del traffico così come le port forward tradizionali. Questo è usato più comunemente quando si ospitano server, o utilizzano applicazioni che richiedono connessioni in entrata da Internet.

13.1.1 Rischi del port forward

In una configurazione predefinita, Firew4LL non lascia entrare alcun traffico avviato da host su Internet. Questo fornisce protezione da chiunque scansioni Internet alla ricerca di sistemi da attaccare. Quando esiste una regola di port forward, Firew4LL consente il traffico conforme alla regola di firewall corrispondente. Non conosce la differenza tra un pacchetto con un carico dannoso e uno che è benigno. Se la connessione corrisponde alla regola del firewall, è permessa. I controlli basati su host devono essere utilizzati dal sistema di destinazione per proteggere i servizi consentiti attraverso il firewall.

13.1.2 Port forward e servizi locali

Le port forward hanno la precedenza su tutti i servizi in esecuzione localmente sul firewall, come l'interfaccia web, SSH, e così via. Per esempio questo significa che se l'accesso all'interfaccia web remota è permesso dalla WAN utilizzando HTTPS sulla porta TCP 443, una porta forward su WAN per TCP 443 avrà la precedenza e l'interfaccia web non sarà più accessibile da WAN. Questo non influisce sull'accesso su altre interfacce, ma solo sull'interfaccia che contiene la Port Forward.

13.1.3 Port forward e NAT 1:1

Anche le port forward hanno la precedenza sul NAT 1:1. Se una porta forward è definita su un indirizzo IP esterno che inoltra una porta ad un host, e una voce NAT 1:1 è definita anche sullo stesso indirizzo IP esterno che inoltra tutto in un host diverso, allora la Port Forward rimane attiva e continua ad inoltrare all'host originale.

13.1.4 Aggiungere port forward

Il port forward è gestitp da **Firewall>NAT**, nella scheda **Port Forward**. Le regole di questa schermata sono gestite nello stesso modo delle regole del firewall (vedere *Introduzione alla schermata delle regole del firewall*).

Per iniziare ad aggiungere una Port Forward, fare clic sul pulsante  **Aggiungere** per raggiungere la schermata di modifica **Port Forward**. Sono disponibili le seguenti opzioni:

Disabilitare una casella di controllo per disabilitare opzionalmente questa Port Forward del NAT. Per disattivare la regola, selezionare questa casella.

Nessun RDR (NO) nega il significato di questa Port Forward, indicando che non si dovrebbe effettuare alcun reindirizzamento se questa regola è allineata. La maggior parte delle configurazioni non utilizzerà questo campo. Questo sarebbe usato per sovrascrivere un'azione di inoltro, che può essere necessario in alcuni casi per consentire l'accesso a un servizio sul firewall su un IP utilizzato per NAT 1:1, o un altro scenario avanzato simile.

Interfaccia L'interfaccia dove la Port Forward sarà attiva. Nella maggior parte dei casi questa sarà una WAN. Per ulteriori collegamenti WAN o reindirizzamenti locali questa può essere una interfaccia diversa. L'interfaccia è la posizione sul firewall in cui entra il traffico per questa Port Forward.

Protocollo Il protocollo del traffico in arrivo da corrispondere. Questo deve essere impostato in modo da corrispondere al tipo di servizio inoltrato, sia che si tratti di TCP, UDP, o di un'altra scelta disponibile. La maggior parte dei servizi comuni che vengono inoltrati sarà TCP o UDP, ma consultare la documentazione per il servizio o anche una rapida ricerca web per confermare la risposta. L'opzione TCP/UDP inoltra insieme TCP e UDP in un'unica regola.

Sorgente Queste opzioni sono nascoste dietro un pulsante delle **Avanzate** per impostazione predefinita, e impostate su *qualsiasi* sorgente. Le opzioni **Sorgente** limitano gli indirizzi IP di sorgente e le porte che possono accedere a questa porta. Queste non sono tipicamente necessarie. Se la Port Forward deve essere raggiungibile da qualsiasi posizione su Internet, la sorgente deve essere *qualsiasi*. Per i servizi ad accesso ristretto, utilizzare un alias qui in modo che solo una serie limitata di indirizzi IP possano accedere alla porta foerward. A meno che il servizio non richieda assolutamente una porta sorgente specifica, l'intervallo delle porte sorgente deve essere lasciato come *qualsiasi* dal momento che quasi tutti i client useranno porte sorgente randomizzate.

Destinazione L'indirizzo IP dove il traffico da inoltrare è inizialmente destinato. Per le port forward su WAN, nella maggior parte dei casi questo è l'indirizzo WAN. Se sono disponibili più indirizzi IP pubblici, può trattarsi di un IP virtuale (vedere *Indirizzi IP virtuali*) su WAN.

Intervallo delle porte di destinazione La porta di destinazione originale del traffico, quando sta arrivando da Internet, prima di essere reindirizzato all'host di destinazione specificato. Se si inoltra una singola porta, digitarla nella casella **Da porta** e lasciare la casella **A porta** vuota. Un elenco dei servizi comuni è disponibile nelle caselle a discesa di questo gruppo. Gli alias di porta possono essere usati anche qui per inoltrare una serie di servizi. Se qui viene usato un alias, lo stesso alias deve essere usato come **Porta di destinazione a cui reindirizzare**

IP meta del reindirizzamento L'indirizzo IP in cui il traffico verrà inoltrato, o tecnicamente reindirizzato. Viene inserito un alias qui, ma l'alias deve contenere **solo un indirizzo**. Se l'alias contiene più

indirizzi, la porta sarà inoltrata alternativamente a ciascun host, che non è quello che la maggior parte delle persone vogliono. Per impostare il bilanciamento del carico di una porta su più server interni, vedere *Bilanciamento del carico del server*.

Porta meta del reindirizzamento Dove inizierà l'intervallo della Port Forward. Se viene inoltrata una serie di porte, ad es. 19000-19100, viene specificato solo il punto di partenza locale in quanto il numero di porte deve corrispondere a uno a uno.

Questo campo permette di aprire una porta diversa esterna rispetto all'host interno in ascolto. Ad esempio la porta esterna 8888 può inoltrare alla porta locale 80 per HTTP su un server interno. Un elenco di servizi comuni è disponibile per scegliere nel menu a discesa.

Gli alias della porta possono essere usati anche qui per inoltrare una serie di servizi. Se qui viene usato un alias, lo stesso alias deve essere usato come **Intervallo della porta di destinazione**.

Descrizione Come in altre parti di Firew4LL, questo campo è disponibile per una breve frase su cosa fa la Port Forward o perché esiste.

Nessuna sincronizzazione XML-RPC Questa opzione è rilevante solo se è in uso una configurazione di cluster HA, altrimenti dovrebbe essere saltata. Quando si utilizza un cluster HA con sincronizzazione della configurazione, selezionare questa casella impedirà che la regola sia sincronizzata con gli altri membri di un cluster (vedere *Elevata disponibilità*). In genere tutte le regole dovrebbero sincronizzarsi, comunque. Questa opzione è efficace solo sui nodi master, non impedisce che una regola venga sovrascritta sui nodi slave.

Nat Reflection Questo argomento è trattato più dettagliatamente più avanti in questo capitolo (*Nat Reflection*). Questa opzione permette di abilitare o disabilitare in base ad una regola per sovrascrivere le impostazioni predefinite totali. Le opzioni in questo campo sono spiegate più dettagliatamente nella *Riflessione NAT*.

Associazione di regole di fitro Questa ultima opzione è molto importante. Una porta di ingresso definisce solo quale traffico verrà reindirizzato, una regola firewall è necessario per passare qualsiasi traffico attraverso tale reindirizzamento. Per impostazione predefinita, viene selezionata la regola di filtro associata. Le scelte disponibili sono:

Nessuno Se questo viene scelto, non verrà creata nessuna regola del firewall.

Aggiungere una regole di filtro associata Questa opzione crea una regola del firewall che è collegata a questa regola di avanzamento della porta NAT. Le modifiche apportate alla regola NAT vengono aggiornate automaticamente nella regola firewall. Questa è la scelta migliore per la maggior parte dei casi d'uso. Se si sceglie questa opzione, dopo che la regola è stata salvata viene posizionato un collegamento che porta alla regola firewall associata.

Aggiungere una regola di filtro non associata Questa opzione crea una regola del firewall che separa questa Port Forward del NAT. Le modifiche apportate alla regola NAT devono essere modificate manualmente nella regola firewall. Questo può essere utile se devono essere impostate altre opzioni o restrizioni sulla regola firewall piuttosto che sulla regola NAT.

Passare Questa scelta utilizza una speciale parola chiave pf sulla regola della Port Forward del NAT che fa passare il traffico senza bisogno di una regola firewall. Poiché non esiste una regola separata sul firewall, qualsiasi traffico corrispondente a questa regola viene inoltrato al sistema di destinazione.

Nota: Le regole che utilizzano *Passare* funzionano solo sull'interfaccia che contiene il gateway predefinito per il firewall, quindi non funzionano efficacemente con Multi-WAN.

- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**

La figura *Esempio di Port Forward* contiene un esempio della schermata di modifica della Port Forward con le impostazioni corrette per inoltrare HTTP in ingresso sulla WAN destinato all'indirizzo IP della WAN al sistema interno al 10.3.0.15.

Dopo aver fatto clic su **Salvare**, l'elenco delle port forward viene visualizzato di nuovo, e la voce appena creata sarà presente nell'elenco, come in Figura *Elenco di port forward*.

Ricontrollare la regola del firewall, come visto sotto **Firewall>Regole** sulla scheda per l'interfaccia su cui è stata creata la Port Forward. La regola mostrerà che il traffico è permesso nell'indirizzo IP interno sulla porta corretta, come mostrato in Figura *Regola del firewall per la Port Forward*.

La sorgente della regola generata automaticamente dovrebbe essere limitata ove possibile. Per cose come la posta e i server web che tipicamente devono essere ampiamente accessibili, questo non è pratico, ma per i servizi di gestione remota come SSH, RDP e altri, ci sono probabilmente solo un piccolo numero di host che dovrebbero essere in grado di connettersi utilizzando tali protocolli in un server da tutto Internet. Una pratica molto più sicura è quella di creare un alias di host autorizzati, e poi cambiare la sorgente da *qualsiasi* per gli alias. In caso contrario, il server è ampiamente aperto a tutto Internet. Provare la Port Forward prima con la sorgente senza restrizioni, e dopo che la verifica funziona, limitare la sorgente come desiderato.

Se tutto sembra a posto, la Port Forward funzionerà se provata dall'esterno della rete. Se qualcosa è andato storto, vedere *Risoluzione dei problemi per la Port Forward* più avanti in questo capitolo.

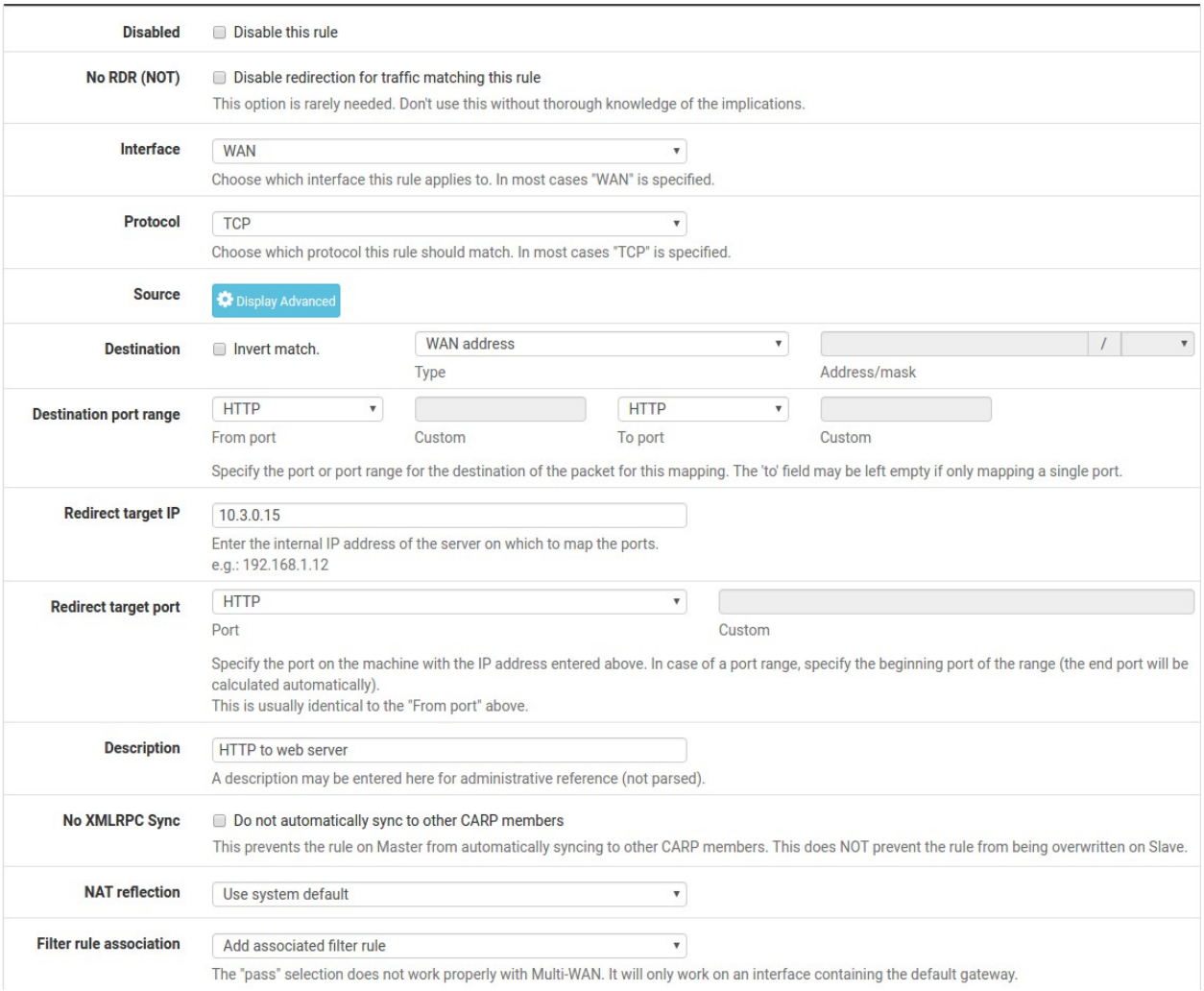


Fig. 1: Esempio di Port Forward

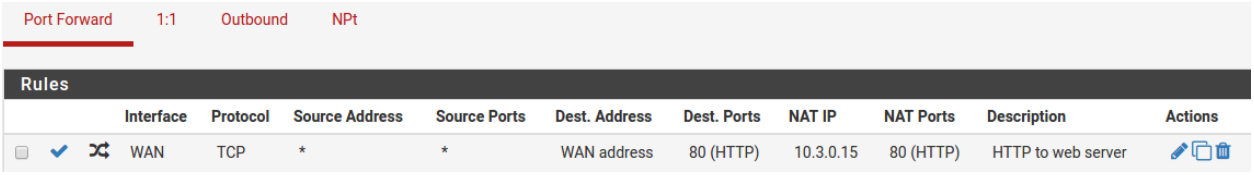


Fig. 2: Elenco di port forward

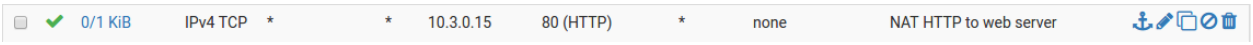


Fig. 3: Regola del firewall per la Port Forward

13.1.5 Tracciare le modifiche ai port forward

Come indicato in Figura *Timbro orario delle regole del firewall* per le regole del firewall, un timestamp viene aggiunto ad una voce della porta forward quando viene creata o modificata, per mostrare quale utente ha creato la regola, e l'ultima persona a modificare la regola. Le regole del firewall create automaticamente dalle regole NAT associate sono marcate come tali anche sul timestamp di creazione.

13.1.6 Limitazioni del Port Forward

Una singola porta può essere inoltrata solo a un host interno per ogni indirizzo IP pubblico disponibile. Ad esempio, se è disponibile un solo indirizzo IP pubblico, può essere configurato un server web interno che utilizza la porta TCP 80 per servire il traffico web. Qualsiasi server aggiuntivo deve usare porte alternative come 8080. Se cinque indirizzi IP pubblici disponibili sono configurati come indirizzi IP virtuali, allora cinque server web interni che utilizzano la porta 80 possono essere configurati. Vedere *Indirizzi IP virtuali* per maggiori informazioni sugli indirizzi IP virtuali.

C'è una eccezione insolita ma a volte applicabile a questa regola. Se una particolare porta deve essere inoltrata a un host interno specifico solo per determinati indirizzi IP di origine, e la stessa porta può essere inoltrata a un host diverso per altri indirizzi IP di origine, ciò è possibile specificando l'indirizzo di origine nella porta di ingresso, come in figura Port Forward Esempio con diverse fonti.

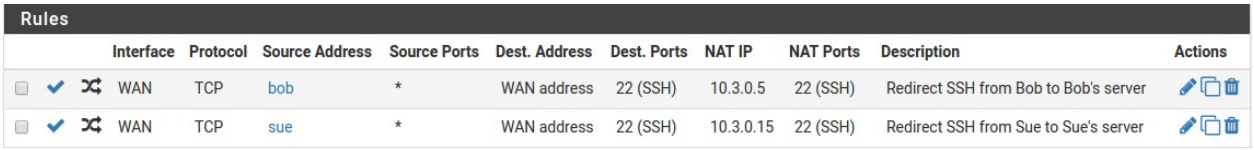


Fig. 4: Esempio di Port Forward con diverse fonti

Affinché le porte inoltrate sugli indirizzi WAN siano accessibili utilizzando i rispettivi indirizzi IP della WAN da interfacce interne, la Nat Reflection deve essere attivata, come descritto nella *Nat Reflection*. **Verificare sempre la porta faorward da un sistema su una connessione Internet diversa**, e non dall'interno della rete. Testare da un dispositivo mobile su 3G/ 4G è un modo semplice e veloce per confermare la connettività esterna.

13.1.7 Auto-configurazione del servizio con UPnP o NAT-PMP

Alcuni programmi supportano il Plug-and-Play universale (UPnP) o il protocollo di mappatura delle porte NAT (NAT-PMP) per configurare automaticamente le port forward del NAT e le regole del firewall. Ancora più preoccupazioni di sicurezza si applicano lì, ma nell'uso domestico i benefici spesso superano eventuali preoccupazioni potenziali. Vedere *UPnP & NAT-PMP* per maggiori informazioni sulla configurazione e l'utilizzo di UPnP e NAT-PMP.

13.1.8 Reindirizzamento del traffico con la Port Forward

Un altro uso di port forward è per reindirizzare in modo trasparente il traffico da una rete interna. Le port forward che specificano l'interfaccia LAN o un'altra interfaccia interna reindirizzeranno il traffico corrispondente alla destinazione specificata. Questo è più comunemente usato per instradare in modo trasparente il traffico HTTP su un server proxy, o reindirizzare tutti i DNS in uscita su un server.

Le voci NAT mostrate in Figura *Esempio di reindirizzamento con porte forward* sono un esempio di una configurazione che reindirizzerà tutto il traffico HTTP proveniente dall'interfaccia LAN a Squid (porta 3128) sull'host 10.3.0.10, ma non reindirizzerà il traffico proveniente dal proxy squid stesso. Le regole devono essere nell'ordine corretto nell'elenco delle port forward: la regola di negazione prima, poi il reindirizzamento.

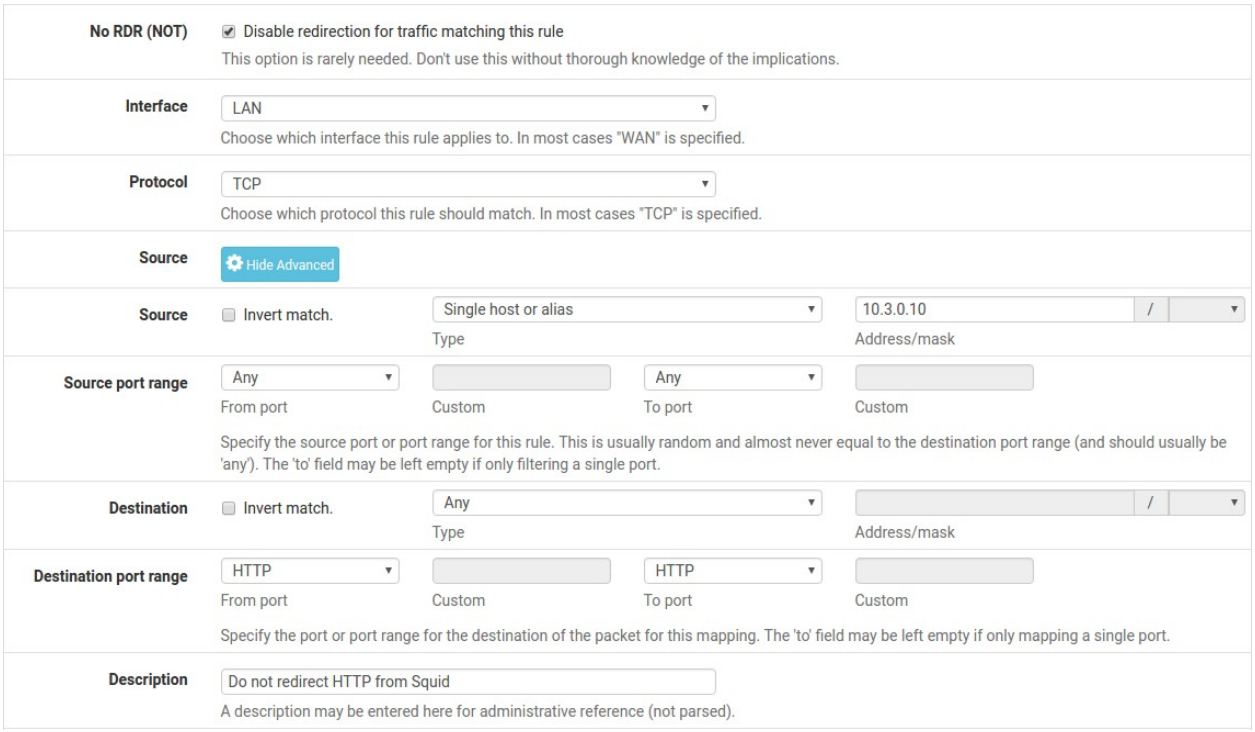


Fig. 5: Esempio di reindirizzamento con port forward (Negazione)

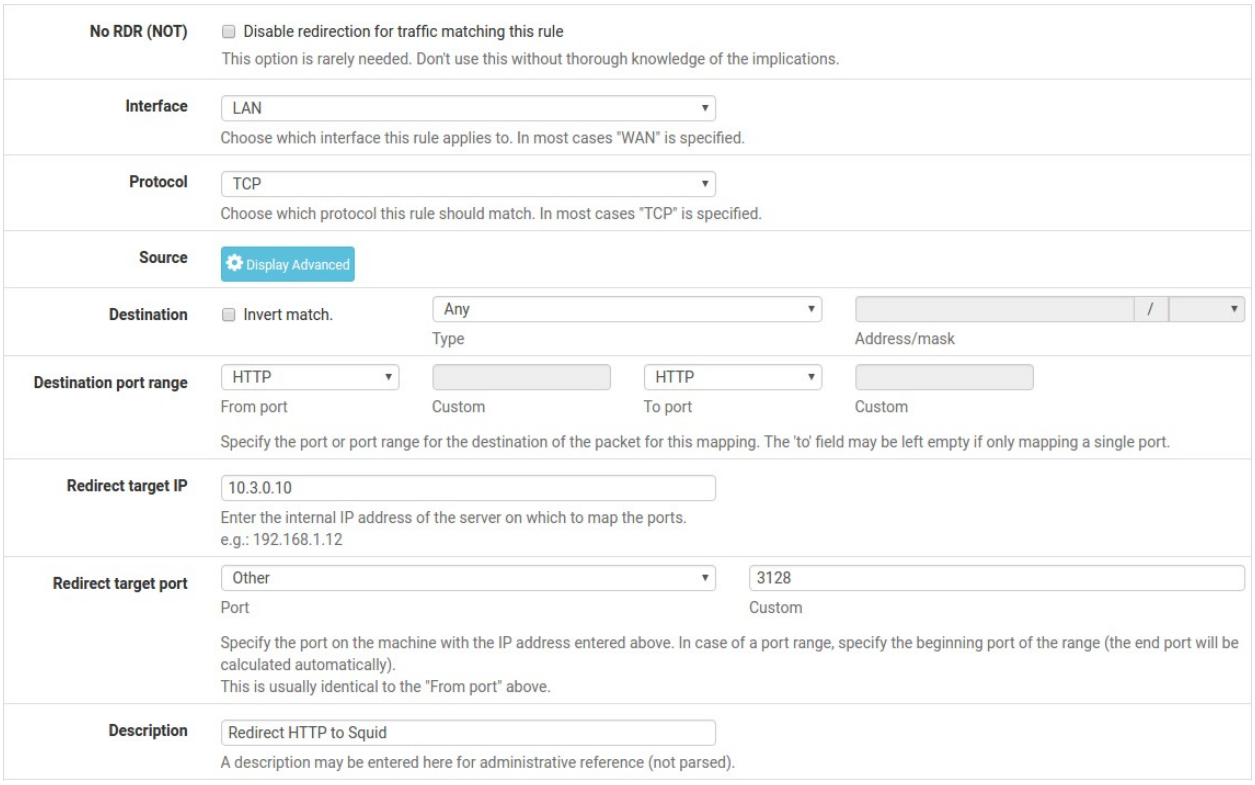


Fig. 6: Esempio di reindirizzamento con port forward

13.2 NAT 1:1

Il NAT (pronunciato «NAT uno a uno») mappa un indirizzo IPv4 esterno (di solito pubblico) a un indirizzo IPv4 interno (di solito privato). Tutto il traffico proveniente da tale indirizzo IPv4 privato che va a Internet sarà mappato dal NAT 1:1 all'indirizzo IPv4 pubblico definito nella voce, sovrascrivendo la configurazione NAT in uscita. Tutto il traffico avviato su Internet destinato all'indirizzo IPv4 pubblico specificato sulla mappatura sarà tradotto all'indirizzo IPv4 privato, quindi valutato in base alle regole del firewall della WAN. Se il traffico corrispondente è consentito dalle regole del firewall ad un target dell'indirizzo IPv4 privato, sarà passato all'host interno.

Il NAT 1:1 può anche tradurre intere sottoreti e singoli indirizzi, a condizione che siano della stessa dimensione e si allineino su adeguati confini della sottorete.

Le porte di una connessione rimangono costanti con il NAT 1:1; per le connessioni in uscita, le porte sorgente utilizzate dal sistema locale vengono mantenute, analogamente all'uso di **Porta Statica** sulle regole NAT in uscita.

13.2.1 Rischi del NAT 1:1

I rischi di NAT 1:1 sono in gran parte gli stessi delle port forward, se le regole WAN firewall consentono il traffico. Le norme temporali consentono il traffico e il traffico potenzialmente dannoso può essere ammesso nella rete locale. L'utilizzo del NAT 1:1 comporta un leggero rischio in quanto gli errori nelle regole del firewall possono avere conseguenze più disastrose. Con le entrate in avanti della porta, il traffico è limitato dai vincoli all'interno della regola NAT e della regola firewall. Se la porta TCP 80 è aperta da una regola port forward, allora una regola allow all on WAN autorizzerebbe comunque solo TCP 80 su quell'host interno. Se sono in vigore regole NAT 1:1 e esiste una regola allow all su WAN, tutto su quell'host interno sarà accessibile da Internet. Le misconfigurazioni sono sempre un rischio

potenziale, e questo di solito non dovrebbe essere considerato un motivo per evitare 1:1 NAT. Tieni a mente questo fatto quando configuri le regole del firewall, e come sempre, evita di permettere qualsiasi cosa che non sia necessaria.

13.2.2 Configurazione del NAT 1:1

Per configurare il NAT 1:1:

- Aggiungere un IP virtuale per l'indirizzo IP pubblico da utilizzare per la voce NAT 1:1 come descritto negli indirizzi IP virtuali
- Passare a **Firewall>NAT**, scheda **1:1**
- Fare clic su  **Aggiungere** per creare una nuova voce 1:1 in cima alla lista
- Configurare la voce NAT 1:1 come segue:

  Disabilitato Controlla se questa voce NAT 1:1 è attiva.

  Interfaccia L'interfaccia in cui avrà luogo la traduzione NAT 1:1, tipicamente un'interfaccia di tipo WAN.

  IP della sottorete esterna L'indirizzo IPv4 a cui l'indirizzo **IP interno** sarà tradotto mentre entra o esce dall'**interfaccia**. Questo è tipicamente un indirizzo IP virtuale IPv4 sull'**interfaccia**, o un indirizzo IP instradato al firewall tramite **interfaccia**.

  IP interno L'indirizzo IPv4 dietro il firewall che sarà tradotto all'indirizzo IP della sottorete esterna. Questo è tipicamente un indirizzo IPv4 dietro questo firewall. Il dispositivo con questo indirizzo deve usare questo firewall come gateway direttamente (collegato) o indirettamente (tramite un percorso statico). Specificando qui una maschera di sottorete, l'intera rete che corrisponde alla maschera di sottorete verrà tradotta. Per esempio usando x.x.x.0/24 tradurrete qualsiasi cosa in quella sottorete al suo equivalente nella sottorete esterna.

  Destinazione Facoltativo, una restrizione della rete che limita la voce NAT 1:1. Quando un valore è presente, il NAT 1:1 avrà effetto solo quando il traffico passa dall'indirizzo **IP interno** all'indirizzo di **destinazione** sull'uscita, o dall'indirizzo di **destinazione** all'indirizzo **IP della sottorete esterna** indirizzo sulla strada verso il firewall. Il campo Destinazione supporta l'uso di alias.

  Descrizione Testo di descrizione facoltativo che illustra lo scopo di questa voce.

  Nat Reflection Un override per le opzioni di Nat Reflection globale. *Usare il sistema predefinito* rispetterà le impostazioni di Nat Reflection globale, *abilitare* eseguirà sempre la Nat Reflection per questa voce, e *disabilitare* non farà mai eseguire la Nat Reflection per questa voce. Per maggiori informazioni sulla Nat Reflection, vedere *Nat Reflection*.

- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**

Esempio di configurazione 1:1 dell'indirizzo IP

Questa sezione mostra come configurare una voce NAT 1:1 con un unico indirizzo IP interno ed esterno. In questo esempio, 198.51.100.210 è un indirizzo IP virtuale sull'interfaccia WAN. Nella maggior parte delle distribuzioni, questo sistema sarà supportato da un indirizzo IP pubblico funzionante. Il server di posta in questa mappatura si trova su un segmento DMZ utilizzando l'indirizzo IP interno 10.3.1.15. La voce NAT 1:1 nella mappa 198.51.100.210-10.3.1.15 è riportata nella figura *Voce del NAT 1:1*.

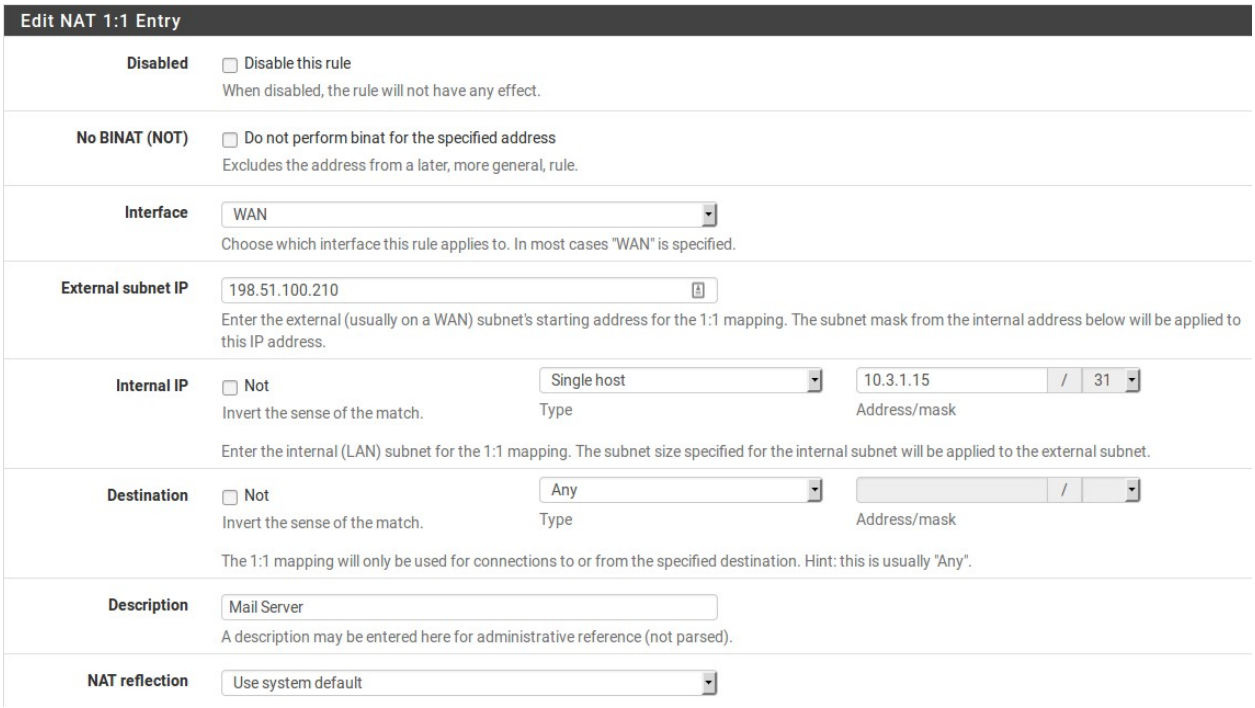


Fig. 7: Voce del NAT 1:1

Esempio di configurazione 1:1 nell'intervallo di indirizzo IP

Il NAT 1:1 può essere configurato per più indirizzi IP pubblici utilizzando intervalli CIDR. In questo esempio, il NAT 1:1 è configurato per un intervallo CIDR /30 di indirizzi IP.

Vedi anche:

Vedere *Sintesi del CIDR* per più informazioni sul riepilogo di reti o gruppi di indirizzi IP all'interno di una sottorete più grande utilizzando la notazione CIDR.

Tabella 1: Ottetto finale che corrisponde alla mappatura CIDR /30

IP esterno	IP interno
198.51.100.64/30	10.3.1.64/30
198.51.100.64	10.3.1.64
198.51.100.65	10.3.1.65
198.51.100.66	10.3.1.66
198.51.100.67	10.3.1.67

L'ultimo ottetto degli indirizzi IP non deve necessariamente essere lo stesso sia all'interno che all'esterno, ma in questo modo diventa logicamente più semplice da seguire. Ad esempio, la tabella *Ottetto finale che non corrisponde alla mappatura CIDR* /30 è anche valida.

Tabella 2: Ottetto finale che non corrisponde alla mappatura CIDR /30

IP esterno	IP interno
198.51.100.64/30	10.3.1.200/30
198.51.100.64	10.3.1.200
198.51.100.65	10.3.1.201
198.51.100.66	10.3.1.202

198.51.100.67	10.3.1.203	

Scegliere uno schema di indirizzamento in cui l'ultimo ottetto che corrisponde rende il layout più facile da capire e quindi da mantenere. La figura *Voce del NAT 1:1 per l'intervallo CIDR /30* mostra come configurare il NAT 1:1 per ottenere la mappatura indicata nella tabella *Ottetto finale che corrisponde alla mappatura CIDR /30*.

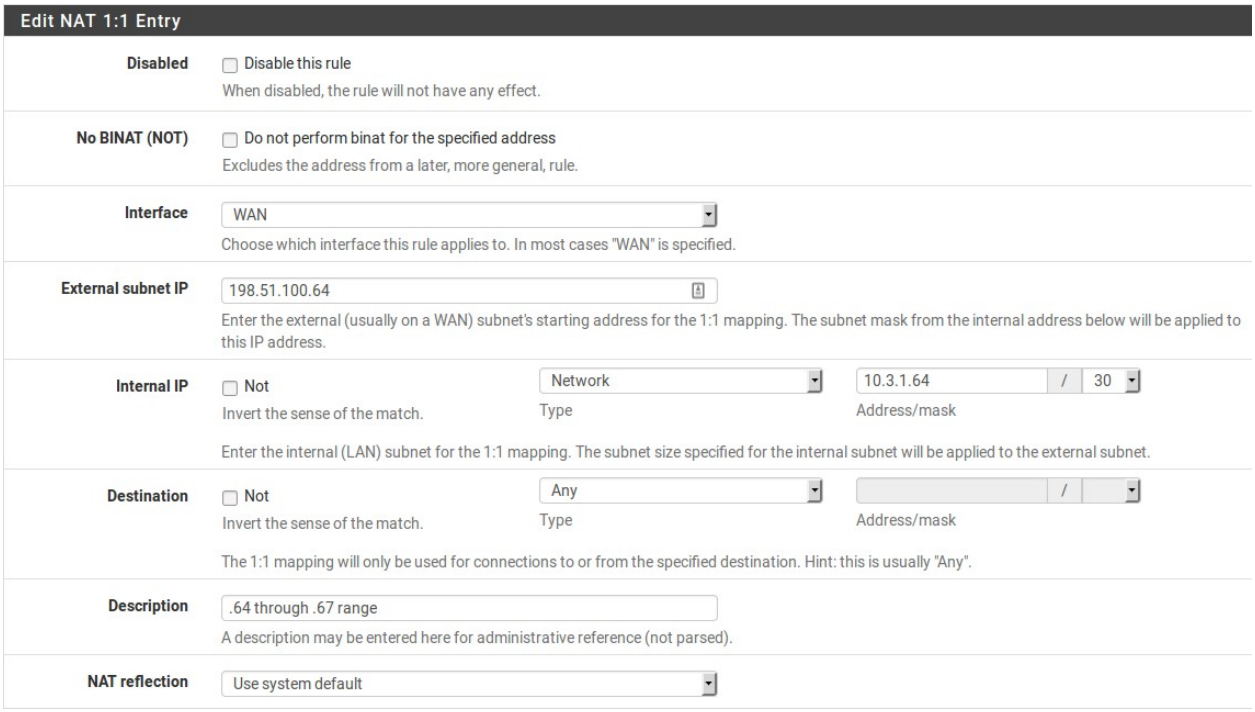


Fig. 8: Voce del NAT 1:1 per l'intervallo CIDR /30.

13.2.3 NAT 1:1 sull'IP della WAN IP, anche conosciuto come «DMZ» su Linksys

Alcuni router per consumatori come quelli di Cisco/Linksys hanno quella che chiamano una funzionalità «DMZ» che inoltrerà tutte le porte e i protocolli destinati all'indirizzo IP della WAN ad un sistema sulla LAN. In effetti, questo è il NAT 1:1 tra l'indirizzo IP della WAN e l'indirizzo IP del sistema interno. «DMZ» in tale contesto, tuttavia, non ha nulla a che fare con ciò che una rete DMZ reale è nella terminologia del networking vero e proprio. Anzi, è quasi il contrario. Un host in una vera DMZ si trova in una rete isolata, lontano dagli altri host LAN, al sicuro dagli host Internet e LAN. Al contrario, un host «DMZ» nel significato Linksys non è solo sulla stessa rete degli host LAN, ma è completamente esposto al traffico in entrata senza protezione.

In Firew4LL, il NAT 1:1 può essere attivo sull'indirizzo IP WAN, con l'avvertenza che lascerà tutti i servizi in esecuzione sul firewall stesso inaccessibili esternamente. Quindi il NAT 1:1 non può essere usato sull'indirizzo IP WAN nei casi in cui VPN di qualsiasi tipo sono abilitate, o altri servizi locali sul firewall devono essere accessibili esternamente. In alcuni casi, questa limitazione può essere attenuata da una Port Forward per i servizi ospitati localmente.

13.3 Ordine nei processi del NAT e del firewall

La comprensione dell'ordine in cui si verificano il firewalling e il NAT è importante quando si configurano le regole NAT e firewall. L'ordine logico di base è illustrato dalla figura *Ordine dei processi di NAT e Firewall*. La figura mostra anche dove tcpdump si lega, poiché il suo uso come strumento di risoluzione dei problemi è descritto più avanti in questo libro in *Cattura dei pacchetti*.

Ogni livello non è sempre colpito in configurazioni tipiche, ma l'uso di regole dinamiche o del NAT in uscita manuale o altre configurazioni più complicate possono colpire ogni livello in entrambe le direzioni. Il diagramma copre solo gli scenari di base per il traffico in entrata e in uscita.

Il traffico dalla LAN alla WAN è trattato come descritto nel seguente elenco più dettagliato. Se un tipo di regole non esiste o non corrisponde, queste vengono saltate.

- port forward o NAT 1:1 sull'interfaccia LAN (ad es. proxy o reindirizzamenti DNS)
- Regole del firewall per l'interfaccia LAN: Regole dinamiche **in ingresso** sulla LAN, poi regole per i gruppi di interfaccia, compresa l'interfaccia LAN, quindi regole sulla scheda LAN.
- NAT 1:1 o regole NAT in uscita su WAN
- Regole dinamiche che corrispondono a quelle **in uscita** su WAN

In questo caso, le regole del firewall della scheda WAN e le porte forward non si applicano.

Per il traffico iniziato sulla WAN, l'ordine è lo stesso ma la direzione è invertita:

- port forward o NAT 1:1 sull'interfaccia WAN (ad es. servizi pubblici)
- Regole del firewall per l'interfaccia WAN: Regole dinamiche **in ingresso** su WAN, poi regole per i gruppi di interfaccia tra cui l'interfaccia WAN, poi le regole della scheda WAN.
- NAT 1:1 o regole NAT in uscita sulla LAN
- Regole dinamiche che corrispondono a quelle **in uscita** sulla LAN

tcpdump è sempre la prima e l'ultima cosa a vedere il traffico, a seconda della direzione. In primo luogo, sull'interfaccia in entrata prima di qualsiasi elaborazione NAT e firewall, e per ultimo sull'interfaccia in uscita. Mostra cosa c'è nel cavo. (Vedere *Cattura dei pacchetti*)

Vedi anche:

Vedere *Ordine di elaborazione della regola* per maggiori informazioni sull'ordine di elaborazione della regola del firewall.

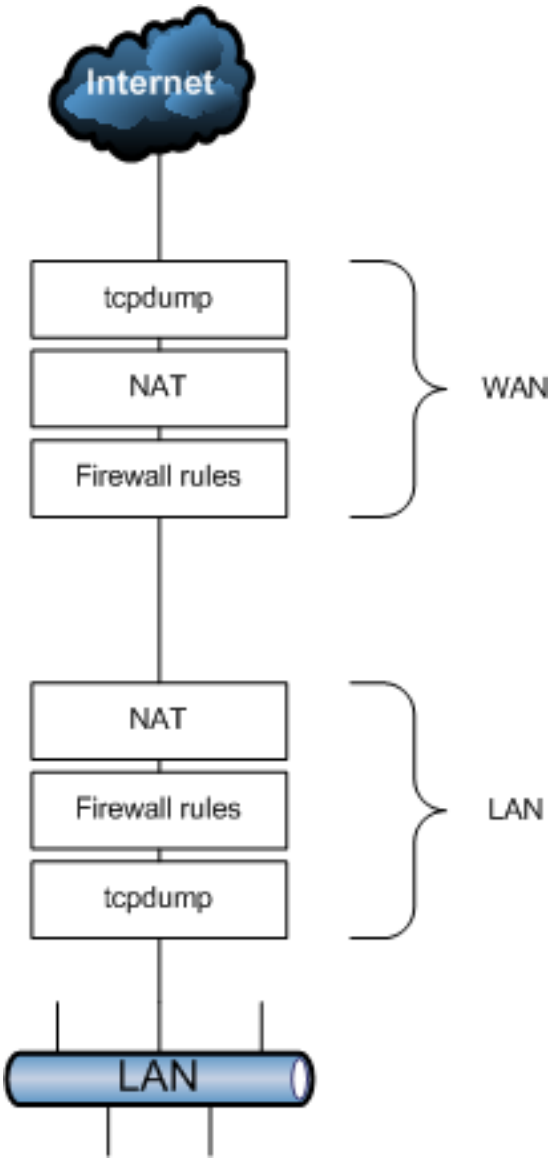


Fig. 9: Ordine dei processi di NAT e Firewall

13.3.1 Estrapolare le interfacce aggiuntive

Il diagramma e le liste precedenti illustrano solo una rete LAN a due interfacce di base e una distribuzione WAN. Quando si lavora con interfacce aggiuntive, si applicano le stesse regole. Il traffico tra due interfacce interne si comporta allo stesso modo del traffico LAN-WAN, anche se le regole NAT predefinite non traducono il traffico tra le interfacce interne in modo che il livello NAT non faccia nulla in questi casi. Se esistono regole NAT in uscita che corrispondono al traffico tra interfacce interne, si applicherà come indicato.

13.3.2 Regole per il NAT

Quando si entra in un'interfaccia, il NAT si applica prima delle regole del firewall, quindi se la destinazione viene tradotta lungo il percorso (ad es. port forward o NAT 1:1 su WAN), le regole del firewall devono corrispondere alla

destinazione tradotta. Nel caso tipico di una porta forward sulla WAN, ciò significa che la regola deve corrispondere alla destinazione dell'indirizzo IP privato di destinazione sulla LAN.

Ad esempio, con una porta in avanti per la porta 80 TCP su WAN con una regola firewall aggiunta automaticamente, la figura *Regola firewall per la Port Forward sull'host LAN* mostra la regola risultante del firewall su WAN. L'indirizzo IP interno della Port Forward è 10.3.0.15. Sia che si utilizzino port forward o NAT 1:1 o meno, le regole del firewall su tutte le interfacce WAN devono utilizzare l'indirizzo IP interno come destinazione. All'uscita da un'interfaccia, il NAT in uscita si applica prima delle regole del firewall, quindi ogni regola dinamica che corrisponde a un'interfaccia in uscita deve corrispondere alla sorgente dopo che è stata tradotta dal NAT in uscita o dal NAT 1:1

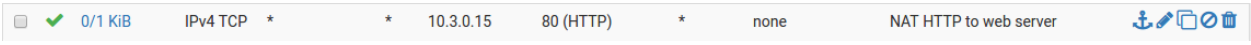


Fig. 10: Regola firewall per la Port Forward sull'host LAN

13.4 NAT Reflection

Il NAT Reflection si riferisce alla capacità di accedere a servizi esterni dalla rete interna utilizzando l'indirizzo esterno (di solito pubblico) IP, lo stesso come se il client fosse su Internet. Molti firewall commerciali e open source non supportano affatto questa funzionalità. Quando possibile, il DNS diviso (split) è il mezzo preferito per accedere alle risorse in modo che il firewall non sia coinvolto nell'accesso ai servizi interni dall'interno. Firew4LL ha un buon supporto per la Nat Reflection, anche se alcuni ambienti richiederanno un'infrastruttura DNS split per adattarsi a questa funzionalità. Il DNS diviso è coperto alla fine di questa sezione in *DNS diviso (split).*

13.4.1 Configurare NAT Reflection

Per abilitare la Nat Reflection a livello globale:

- Passare al **Sistema>Avanzate** su **Firewall e NAT**
- Individuare la sezione **Traduzione degli indirizzi di rete** della pagina
- Configurare le opzioni di Nat Reflection come segue:

  Modalità di Nat Reflection per le port forward Ci sono tre opzioni disponibili per la modalità di Nat Reflection per porte forward, sono:

  Disabilitare La Nat Reflection non sarà eseguita, ma può essere abilitata sulla base di una regola.

  NAT + Proxy Abilita la Nat Reflection usando un programma di aiuto per inviare i pacchetti alla destinazione della Port Forward. Ciò è utile nelle configurazioni in cui l'indirizzo IP dell'interfaccia e/o del gateway utilizzato per la comunicazione con l'obiettivo non possa essere determinato con precisione al momento del caricamento delle regole. Le regole di riflessione per l'uso con il proxy non sono create per intervalli che vanno oltre 500 porte e non sarà utilizzato per più di 1000 porte totali tra tutte le porte forward. Questa modalità non funziona con UDP, solo con TCP. Poiché questo è un proxy, l'indirizzo sorgente del traffico, visto dal server, è l'indirizzo IP del firewall più vicino al server.

  Puro NAT Abilita la Nat Reflection che usa solo le regole NAT in pf per indirizzare i pacchetti verso l'obiettivo della Port Forward. Ha una migliore scalabilità, ma deve essere possibile determinare con precisione l'interfaccia e l'indirizzo IP del gateway utilizzati per la comunicazione con il target al momento del caricamento delle regole. Non ci sono limiti inerenti al numero di porte oltre ai limiti dei protocolli. Tutti i protocolli disponibili per le porte forward sono supportati. Se i server sono nella stessa sottorete dei client, l'opzione **Abilitare NAT di uscita automatico per la riflessione** maschererà la fonte del traffico in modo che ritorni correttamente attraverso il firewall.

  Timeout di riflessione Questa opzione è rilevante solo per la modalità *NAT + Proxy*, e controlla per quanto tempo il demone proxy del NAT aspetterà prima di chiudere una connessione. Specificare il valore in secondi.

Abilitare la Nat Reflection per NAT 1:1 Questa opzione permette ai client sulle reti interne di raggiungere i servizi ospitati localmente collegandosi all'indirizzo IP esterno di una voce NAT 1:1. Per attivare completamente la funzione, controllare sia Abilitare la Nat Reflection per NAT 1:1 e Abilitare il NAT automatico in uscita per la riflessione. Quest'ultima opzione è necessaria solo se client e server sono nella stessa sottorete.

Abilitare NAT automatico in uscita per la riflessione Quando abilitata, questa opzione attiva ulteriori regole NAT per la Nat Reflection 1:1 e la modalità NAT puro per la riflessione per le port forward. Queste regole aggiuntive mascherano l'indirizzo sorgente del client per assicurare che il traffico di risposta ritorni attraverso il firewall. Senza questo, le connessioni tra il client e il server fallirà quando il server risponderà direttamente al client utilizzando il suo indirizzo IP interno. Il client eliminerà la connessione poiché si aspetta una risposta dall'indirizzo IP pubblico.

- Fare clic su **Salvare** per attivare le nuove opzioni di riflessione NAT

  Avvertenze sulla Nat Reflection

La Nat Reflection è un hack quando fa passare il traffico attraverso il firewall quando non è necessario. A causa delle opzioni limitate pf permette di ospitare questi scenari, ci sono alcune limitazioni nell'implementazione della Nat Reflection+Proxy di Firew4LL. Gli intervalli di porte più grandi di 500 porte non hanno NAT riflesso abilitato in modalità NAT+Proxy, e quella modalità è anche effettivamente limitata a lavorare solo con TCP. Le altre modalità richiedono ulteriori NAT se i client e i server sono collegati alla stessa interfaccia del firewall. Questo NAT aggiuntivo nasconde l'indirizzo sorgente del client, facendo sembrare che il traffico provenga dal firewall, in modo che la connessione possa essere stabilita correttamente.

Il DNS split è il mezzo migliore per ospitare grandi intervalli di porte e NAT 1:1. Mantenere un'infrastruttura DNS divisa è richiesto anche da molti firewall commerciali, e in genere non è un problema.

13.4.2 DNS suddiviso (Split)

Un'alternativa preferibile alla Nat Reflection è la distribuzione di un'infrastruttura DNS suddivisa. DNS split si riferisce ad una configurazione DNS in cui, per un dato hostname, il DNS pubblico di Internet si risolve all'indirizzo IP pubblico e il DNS della rete interna si risolve all'indirizzo IP interno privato. I mezzi per accogliere questo variano a seconda delle specifiche dell'infrastruttura DNS di un'organizzazione, ma il risultato finale è lo stesso. La Nat Reflection non è necessaria perché i nomi host risolvono gli indirizzi IP privati all'interno della rete e i client possono raggiungere i server direttamente.

Il DNS split permette ai server di vedere il vero indirizzo IP del client, e le connessioni tra server e client nella stessa sottorete si stabiliranno direttamente, piuttosto che coinvolgendo inutilmente il firewall.

L'unico caso che non funziona correttamente con il DNS diviso è quando i numeri di porta esterni e interni sono diversi. Con DNS diviso, il numero di porta deve essere lo stesso in entrambi i posti.

DNS Resolver/Forwarder Overrides

Se Firew4LL agisce come server DNS per host interni, allora la sovrascrittura degli host nel risolutore DNS o nel DNS forwarder possono fornire funzionalità di DNS split.

Per aggiungere un override al risolutore del DNS:

- Andare a **Servizi>Risolutore del DNS**
- Fare clic su  sotto **Override dell'host** per raggiungere la pagina delle opzioni dell'override dell'host
- Configurare l'override dell'host come necessario, usando l'indirizzo IP interno del server. Vedere *Override dell'host*. La figura *Aggiungere l'override del risolutore del DNS per esempio.com* mostra un esempio di un override del DNS per esempio.com e www.example.com.

- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**

Il DNS Forwarder funziona in modo identico a questo proposito. Se il Forwarder DNS è abilitato al posto del risolutore del DNS, aggiungere gli override lì.

È richiesto un override per ogni hostname in uso dietro il firewall.

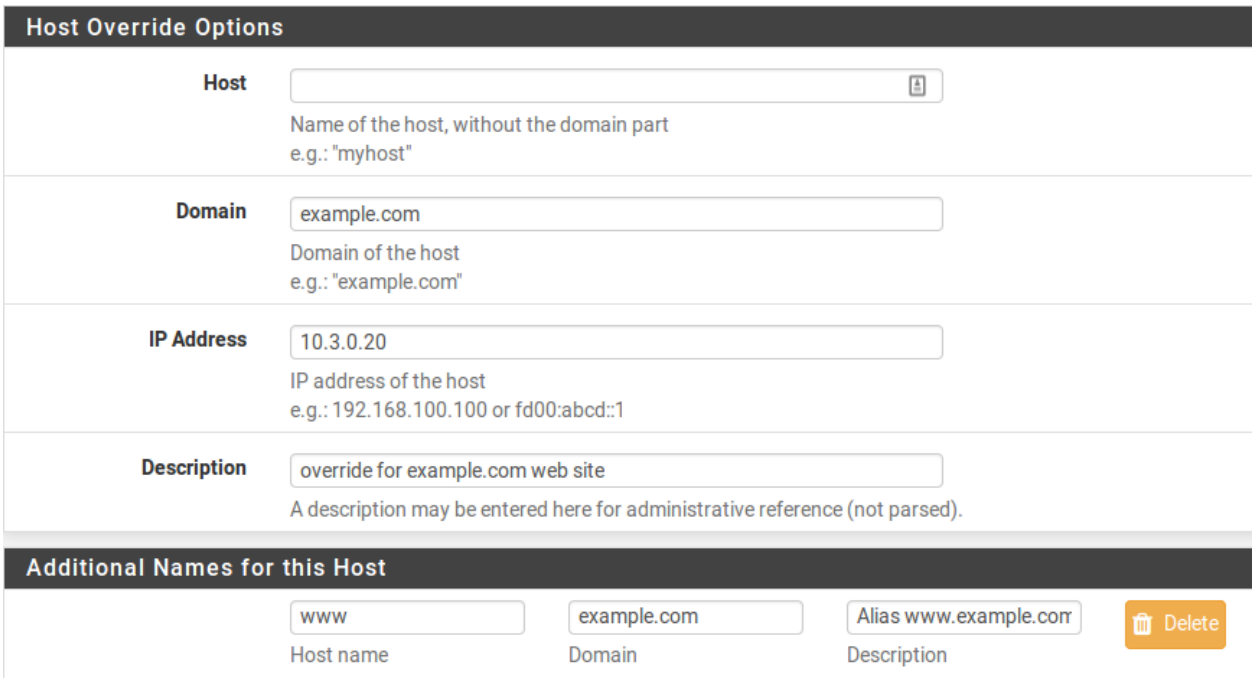


Fig. 11: Aggiungere l'override del risolutore del DNS per esempio.com

Server DNS interni

Quando si utilizza un server DNS seplit su una rete interna, come la directory attiva di Microsoft, le zone devono essere create dall'amministratore del server DNS per tutti i domini ospitati all'interno della rete, insieme a tutti gli altri record per quei domini (A, CNAME, MX, ecc).

In ambienti che eseguono il server DNS BIND dove il DNS pubblico è ospitato sullo stesso server come il DNS privato, la caratteristica vista di BIND viene utilizzata per risolvere il DNS in modo diverso per gli host interni da quelli esterni. Altri server DNS possono supportare funzionalità simili. Controllare la loro documentazione per informazioni.

13.5 NAT in uscita

Il NAT in uscita, noto anche come NAT di sorgente, controlla come Firew4LL tradurrà l'indirizzo sorgente e le porte del traffico che lasciano un'interfaccia. Per configurare il NAT in uscita, passare a **Firewall>NAT**, nella scheda **in uscita**.

Ci sono quattro possibili modalità per il NAT in uscita:

NAT automatico in uscita L'opzione predefinita, che esegue automaticamente il NAT dalle interfacce interne, come LAN, alle interfacce esterne, come WAN.

NAT ibrido in uscita Utilizza le regole manuali, ma anche le regole automatiche per il traffico che non corrisponde a regole inserite manualmente. Questa modalità è la più flessibile e facile da usare per gli

amministratori che hanno bisogno di un piccolo controllo extra ma non vogliono gestire l'intero elenco manualmente.

NAT manuale in uscita onora solo le regole inserite manualmente, e nient'altro. Offre il maggior controllo, ma può essere difficile da gestire e le modifiche apportate alle interfacce interne o WAN devono essere contabilizzate nelle regole a mano. Se l'elenco è vuoto quando si passa da automatico a manuale, l'elenco viene compilato con regole equivalenti al gruppo generato automaticamente.

Disabilitare il NAT in uscita Disabilita tutti i NAT in uscita. Utile se il firewall contiene solo annunci della route (ad es. indirizzi IP pubblici) su tutte le LAN e WAN.

Quando si modifica il valore della **modalità**, fare clic sul pulsante **Salvare** per memorizzare il nuovo valore.

Nelle reti con un unico indirizzo IP pubblico per WAN, di solito non c'è motivo di abilitare il NAT manuale in uscita. Se è necessario un controllo manuale, la modalità ibrida è la scelta migliore. In ambienti con molteplici indirizzi IP pubblici e requisiti NAT complessi, il NAT in uscita manuale offre un controllo più accurato su tutti gli aspetti della traduzione.

Per gli ambienti che utilizzano elevata disponibilità con il CARP, è importante per il traffico in uscita del NAT verso un indirizzo VIP del CARP, come discusso in *elevata disponibilità*. Questo può essere realizzato in modalità ibrida o manuale.

Come per le altre regole in Firew4LL, le regole del NAT in uscita sono considerate dall'alto della lista verso il basso, e viene usata la prima corrispondenza. Anche se le regole sono presenti nella schermata NAT in uscita, non saranno rispettate a meno che la **modalità** non sia impostata su **NAT ibrido in uscita** o **NAT manuale in uscita**.

Nota: Il NAT in uscita controlla solo ciò che accade al traffico *quando esce da un'interfaccia*. *Non* controlla l'interfaccia se il traffico esce dal firewall. Questo è gestito dalla tabella di routing (*Route statiche*) o dalla politica di routing (*Politica di routing*).

13.5.1 Regole NAT in uscita di default

Quando si imposta la modalità del **NAT automatico in uscita** di default, Firew4LL mantiene una serie di regole NAT per tradurre il traffico che lascia qualsiasi rete interna all'indirizzo IP dell'interfaccia WAN che il traffico lascia. Le reti con route statiche e le reti VPN di accesso remoto sono incluse anche nelle regole del NAT automatiche.

Quando il NAT in uscita è configurato per le modalità **Automatica** o **Ibrida**, le regole automatiche sono presentate nella sezione inferiore dello schermo etichettato come **regole automatiche**.

Se l'elenco delle regole del NAT in uscita è vuoto, il passaggio al **NAT manuale in uscita** e il salvataggio genereranno un insieme completo di regole equivalenti alle regole automatiche.

13.5.2 Porta statica

Per default, Firew4LL riscrive la porta sorgente su tutte le connessioni in uscita ad eccezione della porta UDP 500 (IKE per il traffico VPN). Alcuni sistemi operativi fanno un lavoro povero per la randomizzazione della porta di sorgente, se lo fanno a tutti. Questo rende lo spoofing degli indirizzi IP più facile e permette di rilevare le impronte digitali degli host dietro il firewall dal loro traffico in uscita. Riscrivere la porta sorgente elimina queste potenziali (ma improbabili) vulnerabilità di sicurezza. Le regole NAT in uscita, che comprendono le regole automatiche, appariranno  nella colonna della **porta statica** sulle regole impostate per randomizzare la porta sorgente.

La randomizzazione della porta sorgente rompe alcune applicazioni rare. Il NAT automatico predefinitoin uscita disabilita la randomizzazione della porta sorgente per UDP 500 perché sarà quasi sempre interrotta riscrivendo la porta sorgente. Le regole del NAT in uscita che conservano la porta sorgente originale sono chiamate regole della

porta statica e hanno  sulla regola nella colonna della **porta statica**. Tutti gli altri traffici hanno la porta sorgente riscritta di default.

Altri protocolli, come quelli usati dalle console di gioco, potrebbero non funzionare correttamente quando la porta sorgente viene riscritta. Per disabilitare questa funzionalità, utilizzare l'opzione **porta statica**.

Per aggiungere una regola per un dispositivo che richiede porte di origine statica:

- Passare a **Firewall>NAT**, scheda **in uscita**
- Selezionare la generazione di regole del **NAT ibrido in uscita**
- Fare clic su **Salvare**
- **Fare clic su**  **per aggiungere una nuova regola NAT in cima** alla lista
- **Configurare la regola in modo che corrisponda al traffico che** richiede una porta statica, come un indirizzo sorgente di un PBX o di una console di gioco (vedere *Lavorare con le regole del NAT manuale in uscita* sotto)
- **Selezionare Porta Statica nella sezione Traduzione della** pagina
- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**

Dopo aver apportato tale modifica, la porta sorgente sul traffico in uscita corrispondente alla regola sarà mantenuta. La migliore pratica è quella di usare regole severe quando si utilizza la porta statica per evitare conflitti potenziali se due host locali usano la stessa porta sorgente per parlare con lo stesso server remoto e la stessa porta che usano lo stesso indirizzo IP esterno.

13.5.3 Disattivare il NAT in uscita

Se vengono utilizzati indirizzi IP pubblici su interfacce locali, e quindi non è necessario il NAT per far passare il traffico attraverso il firewall, disabilitare il NAT per la sottorete della route. Ciò può essere realizzato in diversi modi:

- Se il NAT non è necessario per qualsiasi interfaccia, impostare la modalità NAT in uscita su **disattivare**
- Utilizzare il NAT ibrido in uscita, un insieme di regole con **Senza NAT** può disabilitare il NAT per il traffico corrispondente
- Utilizzare il NAT manuale in uscita, eliminare (o non creare) le regole NAT corrispondenti alle sottoreti della route

In uno dei casi di cui sopra, il NAT in uscita non sarà più attivo per gli indirizzi IP di sorgente e Firew4LL indirizzerà gli indirizzi IP pubblici senza traduzione.

13.5.4 Lavorare con le regole del NAT manuale in uscita

Le norme NAT in uscita sono molto flessibili e sono in grado di tradurre il traffico in molti modi.

Le regole NAT sono riportate in un'unica pagina e la colonna **Interfaccia** è fonte di confusione per alcuni; poiché il traffico lascia un'interfaccia, vengono consultate solo le regole NAT in uscita impostate per quella specifica **interfaccia**.

Fare clic su  dalla pagina del NAT in uscita per aggiungere una regola in **alto** alla lista. Fare clic su  per aggiungere una regola in basso. Posizionare le regole specifiche in alto, e le regole più generali in basso. Le regole vengono elaborate dal firewall che inizia in cima alla lista e lavora verso il basso, e viene usata la prima regola che corrisponde. Le regole possono essere riordinate nel modo desiderato.

Le opzioni per ciascuna regola NAT in uscita sono:

Disabilito commuta se questa regola è attiva o meno

Senza NAT Questa opzione fa sì che i pacchetti che corrispondono alla regola non abbiano NAT applicato quando escono. Ciò è necessario se il traffico è conforme ad una regola NAT, ma non deve essere applicato al NAT. Un uso comune per questo è quello di aggiungere un'eccezione alla regola in modo che gli indirizzi IP del firewall non abbiano il NAT applicato, soprattutto nel caso del CARP, dove tale NAT romperebbe la comunicazione Internet da un nodo secondario mentre è in modalità di backup.

Interfaccia L'interfaccia in cui si applicherà la regola NAT quando il traffico parte da questa interfaccia. In genere questa è WAN o una WAN OPT, ma in alcuni casi speciali potrebbe essere LAN o un'altra interfaccia interna.

Protocollo Nella maggior parte dei casi, il NAT in uscita si applicherà a qualsiasi protocollo, ma occasionalmente è necessario limitare il protocollo su cui il NAT agirà. Ad esempio, per eseguire solo il NAT sulla porta statica per il traffico UDP da una PBX.

Sorgente La sorgente è la rete locale che avrà il suo indirizzo tradotto mentre lascia l'**Interfaccia** selezionata. Questa è tipicamente una sottorete LAN, DMZ o VPN. La porta sorgente è quasi sempre lasciata vuoto per corrispondere a tutte le porte. Questo campo supporta l'uso di alias se il **Tipo** è impostato su *Rete*.

Nota:

Evitare di utilizzare un indirizzo sorgente come **qualsiasi** perché corrisponderà anche il traffico dal firewall stesso. Questo causerà problemi con il monitoraggio del gateway e altro traffico iniziato dal firewall.

Destinazione Nella maggior parte dei casi, la **destinazione** rimane impostata su *qualsiasi* in modo che il traffico in uscita da questa **interfaccia** sarà tradotto, ma la destinazione può essere limitata in base alle esigenze. Per esempio, per tradurre su una certa strada quando si va a una destinazione specifica, come ad esempio usare solo il NAT sulla porta statica versi indirizzi tronchi SIP. Questo campo supporta l'uso di alias se il **Tipo** è impostato su *Rete*.

Traduzione Il campo **Indirizzo** all'interno della sezione **Traduzione** controlla cosa succede all'indirizzo sorgente del traffico che corrisponde a questa regola. Più comunemente, questo è impostato su *indirizzo d'interfaccia* in modo che il traffico sia tradotto all'indirizzo IP di **Interfaccia**, ad es. l'indirizzo IP della WAN. Il menu a discesa degli **Indirizzi** contiene anche tutti gli indirizzi IP virtuali definiti, gli alias dell'host e *altre sottoreti* per inserire manualmente una sottorete per la traduzione.

Nota:

Un alias contenente sottoreti non può essere utilizzato per la traduzione. Possono essere utilizzati solo alias host o una singola sottorete inserita manualmente.

Utilizzando un alias host o una sottorete inserita manualmente, una regola NAT in uscita può essere tradotta per un pool di indirizzi. Questo può aiutare in grandi distribuzioni NAT o in aree in cui è richiesta una porta statica per diversi client. Quando si traduce in un alias host o in una sottorete, un menù a discesa delle **opzioni del pool** è disponibile con diverse opzioni. Solo i tipi *Round Robin* lavorano con gli alias dell'host. Qualsiasi tipo può essere utilizzato con una sottorete.

Default Non definisce alcun algoritmo specifico per selezionare un indirizzo di traduzione dal pool.

Round Robin Passa in rassegna ogni potenziale indirizzo di traduzione nell'alias o sottorete a turno.

Round Robin con indirizzi appiccicosi (sticky) Funziona come un *Round Robin*, ma mantiene lo stesso indirizzo di traduzione per un determinato indirizzo di sorgente, a condizione che esistano stati dall'host di sorgente.

Random Seleziona un indirizzo di traduzione da usare da una sottorete a caso.

Random con indirizzo Seleziona un indirizzo a caso, ma mantiene lo stesso indirizzo di traduzione per un dato indirizzo di sorgente, purché esistano stati dall'host di sorgente.

Hash di sorgente Utilizza un hash dell'indirizzo di sorgente per determinare l'indirizzo di traduzione, assicurando che l'indirizzo tradotto sia sempre lo stesso per un dato indirizzo IP di sorgente.

Maschera di bit Applica la maschera di sottorete e mantiene l'ultima porzione identica. Per esempio se l'indirizzo sorgente è 10.10.10.50 e la sottorete di traduzione è 192.2.0.0/24, la regola cambierà l'indirizzo in 192.2.0.50. Funziona in modo simile al NAT 1:1, ma solo nella direzione di uscita.

Porta Specifica una porta *sorgente* in particolare per la traduzione. Questo è quasi sempre lasciato vuoto, ma potrebbe essere richiesto se il client seleziona una porta sorgente casuale, ma il server richiede una porta sorgente specifica.

Porta statica Fa sì che la porta sorgente originale del traffico client sia mantenuta dopo che l'indirizzo IP sorgente è stato tradotto. Alcuni protocolli richiedono questo, come IPsec senza NAT-T, e alcuni protocolli si comportano meglio con questo, come SIP e RTP. La spunta di questa opzione disabilita la casella di voce **Porta**.

Nessuna sincronizzazione XML-RPC Questa opzione è rilevante solo se è in uso una configurazione di cluster HA, e dovrebbe essere saltata altrimenti. Quando si utilizza un cluster HA con sincronizzazione della configurazione, selezionare questa casella impedirà che la regola sia sincronizzata con gli altri membri di un cluster (vedere *Elevata disponibilità*). In genere tutte le regole dovrebbero sincronizzarsi, comunque. Questa opzione è efficace solo sui nodi master, non impedisce che una regola venga sovrascritta sui nodi slave.

Nota: Un riferimento di testo facoltativo per spiegare lo scopo della regola.

Queste regole possono ospitare la maggior parte di scenari NAT, grandi o piccoli.

13.5.5 Tracciare le regole del NAT in uscita

Come indicato nella figura *Timestamp delle regole del firewall*, un timestamp viene aggiunto ad una voce del NAT in uscita che indica quando è stato creato o modificato l'ultima volta. Questo timestamp mostra quale utente ha creato la regola, e l'ultima persona a modificare la regola. Quando si passa dalla modalità NAT automatico in uscita alla modalità NAT manuale in uscita, le regole create vengono contrassegnate come create da tale processo.

13.6 Scegliere la configurazione del NAT

La migliore configurazione NAT per una data distribuzione dipende principalmente dal numero di indirizzi IP pubblici disponibili e dal numero di servizi locali che richiedono l'accesso in entrata da Internet.

13.6.1 Indirizzo IP pubblico singolo per WAN

Quando è disponibile solo un singolo IP pubblico per WAN, le opzioni NAT sono limitate. Le regole del NAT 1:1 possono essere usate con gli indirizzi IP della WAN, ma ciò può avere degli svantaggi. In questo caso, si consiglia di usare solo le port forward.

13.6.2 Indirizzi IP pubblici multipli per WAN

Quando sono disponibili più indirizzi IP pubblici per WAN, sono disponibili numerose opzioni per la configurazione NAT in entrata e in uscita. Le port forward, il NAT 1:1, e il NAT ibrido o manuale in uscita possono essere tutti auspicabili, a seconda delle esigenze del sito.

13.7 NAT e protocolli compatibili

Alcuni protocolli non funzionano bene con il NAT e altri non funzioneranno affatto. I protocolli problematici incorporano indirizzi IP e/o numeri di porta all'interno dei pacchetti (ad es. SIP e FTP), alcuni non funzionano correttamente se la porta sorgente viene riscritta (SIP da PBX, IPsec), e alcuni sono difficili a causa delle limitazioni di pf (PPTP). Questa sezione riguarda un campionamento di protocolli che hanno difficoltà con il NAT in Firew4LL, e come lavorare su questi temi, ove possibile.

13.7.1 FTP

FTP pone problemi sia con il NAT e sia con il firewall a causa della progettazione del protocollo. La FTP è stata concepita inizialmente negli anni "70 e l'attuale norma che definisce le specifiche del protocollo è stata scritta nel 1985. Dal momento che FTP è stato creato più di un decennio prima del NAT, e molto prima che i firewall fossero comuni, agisce in modi che sono molto ostili verso NAT e firewall.

Firew4LL non include un proxy FTP di default, ma c'è un proxy del client disponibile come pacchetto aggiuntivo.

Limitazioni FTP

Poiché pf non ha la capacità di gestire correttamente il traffico FTP senza un proxy, e l'implementazione del pacchetto proxy FTP è un po" carente, ci sono alcune restrizioni sull'uso di FTP.

I server FTP dietro il NAT

Per i server FTP dietro il NAT, tutte le porte pertinenti devono essere inoltrate manualmente al server e consentite nelle regole del firewall. O nel caso di NAT 1:1, sono necessarie solo le regole del firewall. A seconda della modalità FTP, del software del server e del software del client, può essere necessaria anche una configurazione del server.

Modalità FTP

FTP può agire in diverse modalità che cambiano il comportamento del client e del server, e quale lato ascolta per le connessioni in arrivo. Le complicazioni delle regole NAT e firewall dipendono da queste modalità e se un client da remoto sta tentando di raggiungere un server dietro Firew4LL, o se un client dietro Firew4LL sta tentando di raggiungere un server remoto.

Modalità attiva

Con l'FTP in modalità attiva, quando viene richiesto un trasferimento di file, il client ascolta una porta locale e poi comunica al server l'indirizzo IP del client e la porta. Il server si ricollegherà a quell'indirizzo IP e alla porta per trasferire i dati. Questo è un problema per i firewall perché la porta è tipicamente casuale, anche se i moderni client consentono di limitare l'intervallo che viene utilizzato. Nel caso di un client dietro il NAT, l'indirizzo IP dato sarebbe un indirizzo locale, irraggiungibile dal server. Non solo questo, ma una regola firewall dovrebbe essere aggiunta insieme con una Port Forward che consente il traffico in questa porta.

Quando il pacchetto del proxy FTP è in uso e un client è dietro a Firew4LL che si connette ad un server remoto, il proxy tenta di fare tre cose principali: in primo luogo, riscriverà il comando di PORTA FTP in modo che l'indirizzo IP sia l'indirizzo IP della WAN del firewall, e una porta scelta a caso su quell'indirizzo IP. Successivamente, si aggiunge una Port Forward che collega l'indirizzo IP tradotto e la porta all'indirizzo IP originale e la porta specificata dal client FTP. Infine, permette al traffico del server FTP di connettersi a quella porta «pubblica». Con Multi-WAN, il proxy funzionerà solo sulla WAN contenente il gateway predefinito.

Quando tutto funziona correttamente, tutto questo avviene in modo trasparente. Il server non sa mai che sta parlando con un client dietro NAT, e il client non sa mai che il server non si connette direttamente.

Nel caso di un server dietro NAT, la modalità attiva di solito non è un problema in quanto il server sarà solo in ascolto per le connessioni sulle porte FTP standard e poi farà connessioni in uscita indietro ai client. Le regole del firewall in uscita devono permettere al server di effettuare connessioni in uscita arbitrarie, e le regole non devono instradare quelle connessioni con una WAN diversa da quella che ha accettato la connessione FTP in entrata.

Modalità passiva

La modalità passiva (PASV) agisce un po" al contrario. Per i client, è più amichevole al NAT e al firewall perché il server ascolta una porta quando viene richiesto un trasferimento di file, non il client. In genere, la modalità PASV funziona per i client FTP dietro NAT senza riservare alcun proxy o trattamento speciale a nessuno.

Analogamente alla situazione nella sezione precedente, quando un client richiede la modalità PASV il server fornirà al client il suo indirizzo IP e una porta casuale a cui il client può tentare di connettersi. Poiché il server è su una rete privata, l'indirizzo IP e la porta dovranno essere tradotti e permessi attraverso il firewall. Vedere sotto *Server FTP e port forward* per i requisiti delle regole. Il server FTP deve fornire l'indirizzo IP pubblico a cui i client si connettono, ma alcuni client come Filezilla sono abbastanza intelligenti da ignorare un dato indirizzo IP se è privato, e si connetterà all'indirizzo IP del server originale.

Modalità passiva estesa

La Modalità passiva estesa (EPSV) funziona in modo simile alla Modalità PASV, ma rende possibile l'utilizzo su IPv6. Quando un client richiede un trasferimento, il server risponderà con la porta a cui il client dovrebbe connettersi. Le stesse avvertenze per i server in modalità PASV si applicano qui.

I server FTP e il port forward

Per i server FTP che forniscono modalità passiva ai client, la configurazione del server FTP deve definire un intervallo di porte passive e deve anche impostare l'indirizzo NAT esterno, solitamente l'indirizzo IP della WAN del firewall. I mezzi per impostare questi valori variano a seconda dell'implementazione del software del server FTP. Consultare la documentazione del server FTP per ulteriori informazioni. Sul firewall, l'intervallo delle porte passive deve essere inoltrato insieme alla porta 21 del TCP.

Per i server FTP che forniscono la modalità attiva ai client, una porta forward è necessaria solo per la porta 21 del TCP.

I server FTP e NAT 1:1

Con il NAT 1:1, le regole del firewall devono consentire la porta 21 e l'intervallo di porte passive.

13.7.2 TFTP

Il traffico standard TCP e UDP avvia le connessioni a host remoti utilizzando una porta sorgente casuale nell'intervallo delle porte effimere, che varia a seconda del sistema operativo ma rientra entro 1024-65535, e la porta di destinazione del protocollo in uso.

Le risposte dal server al client invertono ciò: La porta di sorgente è la porta di destinazione client, e la porta di destinazione è la porta di sorgente del client. Questo è il modo in cui pf associa il traffico di risposta con connessioni avviate dall'interno di una rete.

Il TFTP (Protocollo di trasferimento dei file banali, Trivial File Transfer Protocol) non segue tuttavia questa convenzione. La definizione standard TFTP, RFC 1350, specifica che la risposta dal server TFTP al client verrà fornita da un

numero di porta pseudo-casuale. Il client TFTP può scegliere una porta sorgente di 10325 (come esempio) e utilizzare la porta di destinazione per TFTP, porta 69. Il server per altri protocolli dovrebbe poi inviare la risposta utilizzando la porta sorgente 69 e la porta di destinazione 10325. Poiché TFTP utilizza invece una porta sorgente pseudo-casuale, il traffico di risposta non corrisponderà allo stato che pf ha creato per questo traffico. Pertanto le risposte saranno bloccate perché sembrano essere traffico non richiesto da Internet.

Il TFTP non è un protocollo comunemente utilizzato su Internet. L'unica situazione che occasionalmente si presenta in cui questo è un problema è con alcuni telefoni IP che si connettono a fornitori VoIP esterni su Internet utilizzando TFTP per estrarre la configurazione e altre informazioni. La maggior parte dei fornitori VoIP non richiedono questo.

Se il traffico TFTP deve passare attraverso il firewall, è disponibile un proxy TFTP configurato in **Sistema>Aanzate** nella scheda **Firewall e NAT**. Vedere *Proxy TFTP* per maggiori informazioni.

13.7.3 PPTP/GRE

Le limitazioni con PPTP in Firew4LL sono causate da limitazioni nella capacità di pf legate al protocollo GRE del NAT. In quanto tali, le limitazioni si applicano a qualsiasi uso del protocollo GRE, tuttavia PPTP è stato l'uso più comune di GRE in natura.

Il codice di tracciamento di stato in pf per il protocollo GRE può tracciare solo una singola sessione per indirizzo IP pubblico per server esterno. Questo significa che se esiste una connessione VPN PPTP, solo una macchina interna può connettersi contemporaneamente allo stesso server PPTP su Internet. Un migliaio di macchine possono connettersi simultaneamente ad un migliaio di server PPTP diversi, ma solo uno simultaneamente ad un singolo server. Un singolo client può anche connettersi a un numero illimitato di server PPTP esterni.

L'unico metodo possibile è quello di utilizzare più indirizzi IP pubblici sul firewall, uno per client tramite Outbound o NAT 1:1, o di utilizzare più indirizzi IP pubblici sul server PPTP esterno. Questo non è un problema con altri tipi di connessioni VPN.

A causa della sicurezza estremamente difettosa in PPTP (Vedere *Avvertenze su PPTP*), compreso un compromesso completo dell'intero protocollo, il suo utilizzo dovrebbe essere interrotto il più presto possibile, quindi questo problema non è rilevante dati gli attuali standard di sicurezza.

13.7.4 Giochi online

I giochi sono tipicamente NAT amichevole a parte un paio di avvertimenti. Questa sezione si riferisce sia ai giochi per PC e sistemi di gioco per console con funzionalità online. Questa sezione fornisce una panoramica delle esperienze di numerosi utenti Firew4LL. Visitate il campo da gioco sul forum Firew4LL per maggiori informazioni.

Porta statica

Alcuni giochi non funzionano correttamente a meno che la porta statica sia abilitata sulle regole NAT in uscita. Se un gioco ha problemi a stabilire una connessione, la cosa migliore da provare per prima è abilitare la porta statica per il traffico proveniente dalla console. Vedere *Porta Statica* per maggiori informazioni.

Più giocatori o dispositivi dietro un dispositivo NAT

Alcuni giochi hanno temi in cui più giocatori o dispositivi sono dietro un singolo dispositivo NAT. Questi temi sembrano essere specifici per il NAT, non per il Firew4LL, ma anche gli utenti che hanno provato altri firewall sperimentano gli stessi problemi con loro.

Cercare la scheda di gioco sul forum Firew4LL del gioco o il sistema per trovare informazioni da altri con esperienze simili.

Superare i problemi NAT con UPnP

Molti moderni sistemi di gioco supportano l'UPnP (Universal Plug-and-Play) per configurare automaticamente qualsiasi Port Forward NAT richiesta e le regole del firewall. Abilitare UPnP su Firew4LL permetterà ai giochi di funzionare con un intervento minimo o nullo. Vedere *UPnP & NAT-PMP* per maggiori informazioni sulla configurazione e sull'utilizzo di UPnP e per informazioni su potenziali problemi di sicurezza.

13.8 Traduzione dei prefissi di rete IPv6 (NPt)

La traduzione di prefisso di rete, o NPt in breve, funziona in modo simile a NAT 1:1, ma opera su indirizzi IPv6. NPt può essere trovato sotto **Firewall>NAT** nella scheda **NPt**.

Npt prende un prefisso e lo traduce in un altro. Così 2001:db8:1111:2222:::/64 diventa 2001:db8:3333:4444::/64 e se il prefisso cambia, il resto dell'indirizzo sarà identico per un dato host su quella sottorete.

Ci sono alcuni scopi per NPt, ma molti mettono in dubbio la sua effettiva utilità. Con NPt, lo spazio «privato» IPv6 (fc00::/7) può essere utilizzato su una LAN e può essere tradotto da NPt in un prefisso pubblico, instradato, IPv6 perché arriva e passa attraverso una WAN. L'utilità di tutto ciò è discutibile. Un uso è quello di evitare di rinumerare la LAN in caso di cambiamento dei fornitori esterni, tuttavia dal momento che tutto ciò che è esterno e ha cercato il vecchio prefisso deve anche essere regolato, l'utilità di ciò che può andare in entrambi i modi, soprattutto quando la configurazione deve tenerne conto per evitare collisioni nello spazio fc00::/7 per i tunnel VPN.

NPt ha perfettamente senso per le distribuzioni Multi-WAN con IPv6 SOHO. La probabilità che un utente finale di una casa o di una piccola impresa abbia un proprio spazio IPv6 indipendente dal fornitore e un feed BGP è molto ridotta. In questi casi, il firewall può utilizzare un prefisso instradato da WAN multiple per funzionare in modo simile a Multi-WAN su IPv4. Poiché il traffico lascia la seconda WAN proveniente dalla sottorete LAN, NPt la tradurrà nell'indirizzo IP equivalente nella sottorete instradata per quella WAN. La LAN può usare uno dei prefissi instradati ed eseguire l'Npt sugli altri WAN, oppure usare gli indirizzi in fc00::/7 ed esegure l'NPt su tutte le WAN. Si consiglia di evitare l'uso dello spazio fc00::/7 per questo compito. Per maggiori informazioni sulle Multi-WAN con IPv6, vedere *Multi-WAN per IPv6*.

Quando si aggiunge una voce NPt, ci sono poche opzioni da considerare in quanto NPt è abbastanza semplice:

Disabilitato Commuta se questa regola è usata attivamente.

Interfaccia Seleziona l'interfaccia in cui questa regola NPt ha effetto all'uscita del traffico.

Prefisso interno IPv6 La sottorete IPv6 locale (ad es. LAN) e la lunghezza del prefisso, tipicamente il /64 sulla LAN o altra rete interna.

Prefisso di destinazione IPv6 La sottorete esterna di IPv6 e la lunghezza del prefisso a cui sarà tradotto il prefisso interno IPv6. Questo **NON** è il prefisso della WAN stessa. Deve essere una rete indirizzata a questo firewall tramite **Interfaccia**

Descrizione Breve descrizione dello scopo di questa voce.

La figura *Esempio di NPt* mostra una regola NPt in cui la sottorete LAN con IPv6 2001:db8:1111:2222:::/64 sarà tradotta come 2001:db8:3333:4444::/64 mentre lascia l'interfaccia HENETV6DSL.

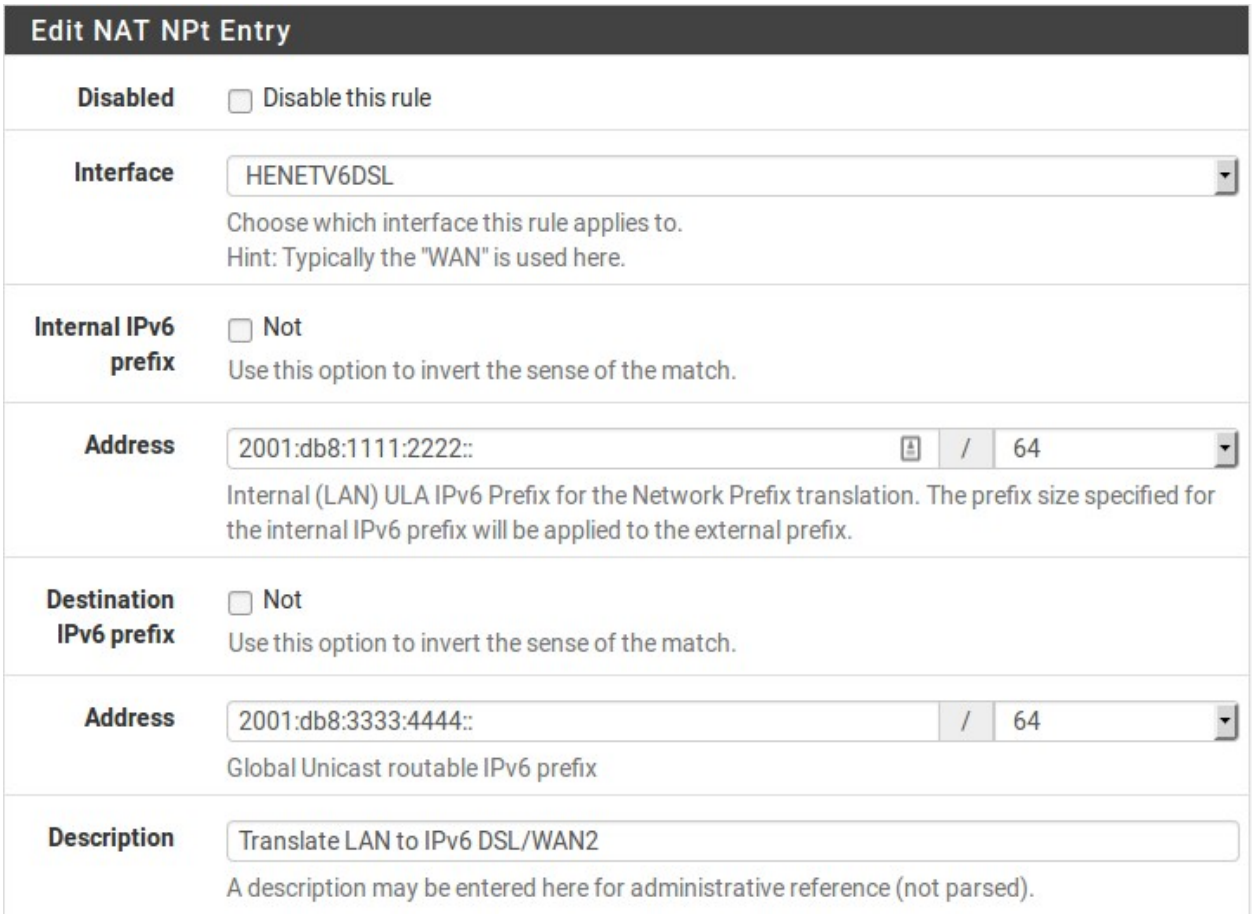


Fig. 12: Esempio di NPT

13.9 Risoluzione dei problemi

Il NAT può essere un animale complesso e in tutti gli ambienti, tranne i più basilari sono destinati a presentare problemi per ottenere una buona configurazione di lavoro. Questa sezione tratterà alcuni problemi comuni e suggerimenti su come essi possono essere potenzialmente risolti.

13.9.1 Risoluzione dei problemi con le port forward

Le port forward in particolare possono essere difficili, dal momento che ci sono molte cose che possono andare storto, molte delle quali potrebbero essere la configurazione del client e non di Firew4LL. La maggior parte dei problemi incontrati dagli utenti sono stati risolti da uno o più dei seguenti suggerimenti.

Voce del Port Forward scorretta

Prima di qualsiasi altra attività di risoluzione dei problemi, verificare le impostazioni per la Port Forward. Ricontrollare il processo in *Aggiungere le port forward*, e verificare due volte che i valori siano corretti. Ricordare, se l'indirizzo IP del NAT o le porte sono cambiate, la regola del firewall potrebbe anche aver bisogno di essere regolata se non è stata scelta una regola del firewall collegato.

Cose comuni da controllare per:

- Interfaccia corretta: Di solito WAN, o da dove il traffico entrerà nel firewall.
- Corretto IP del NAT: L'indirizzo IP deve essere raggiungibile da un'interfaccia sul firewall.
- Intervallo di porte corrette: Deve corrispondere al servizio inoltrato.
- Porta sorgente e sorgente dovrebbero quasi sempre essere impostate su *qualsiasi*.

Regola firewall mancante o non corretta

Dopo aver controllato le impostazioni della Port Forward, controllare due volte che la regola del firewall abbia le impostazioni corrette. Una regola errata del firewall sarebbe evidente anche visualizzando i registri del firewall (*Visualizzazione dei registri del firewall*). Bisogna ricordare che la destinazione per la regola del firewall è l'indirizzo IP interno del sistema di destinazione e non l'indirizzo dell'interfaccia che contiene la Port Forward. Vedere *Regole per il NAT* per maggiori dettagli.

Un firewall è attivato sul computer di destinazione

Un'altra cosa da considerare è che Firew4LL potrebbe inoltrare correttamente la porta, ma un firewall sulla macchina di destinazione potrebbe bloccare il traffico. Se c'è un firewall sul sistema di destinazione, controllare i registri e le impostazioni per confermare se il traffico è bloccato in quel punto.

Firew4LL non è il gateway del sistema di destinazione

Affinché Firew4LL possa inoltrare correttamente una porta per un sistema locale, Firew4LL deve essere il gateway predefinito per il sistema di destinazione. Se Firew4LL non è il gateway, il sistema di destinazione tenterà di inviare risposte al traffico della Port Forward qualunque sia il sistema di gateway, e allora accadrà una di queste due cose: a quel punto verrà eliminato poiché non ci sarebbe alcuno stato corrispondente di connessione su quel router o gli verrebbe applicato il NAT da quel router per poi essere abbandonato dal sistema che ha originato la domanda, poiché la risposta proviene da un indirizzo IP diverso da quello al quale la domanda è stata inizialmente inviata.

Sistema di destinazione non ha gateway o non può utilizzare Firew4LL come gateway

Un sottoinsieme del problema più grande del gateway della macchina di destinazione si ha quando il dispositivo non ha gateway, o è incapace di avere un gateway. In questi casi, si può aggirare il problema passando al NAT in uscita ibrido o manuale e la creazione di una regola sulla LAN o altra interfaccia interna di fronte al dispositivo locale. Questa regola tradurrebbe il traffico da qualsiasi fonte che va al sistema di destinazione sulla porta di destinazione.

Ad esempio, se c'è un file server che non supporta un gateway situato a 10.3.0.6, passare al NAT ibrido in uscita e creare una regola come nella figura *Regola del NAT in uscita manuale per il dispositivo LAN con gateway mancante* per raggiungerlo dall'esterno della rete. Il file server vedrà l'indirizzo IP della LAN del firewall come la fonte del traffico, e dal momento che è «locale» al server, risponderà correttamente.

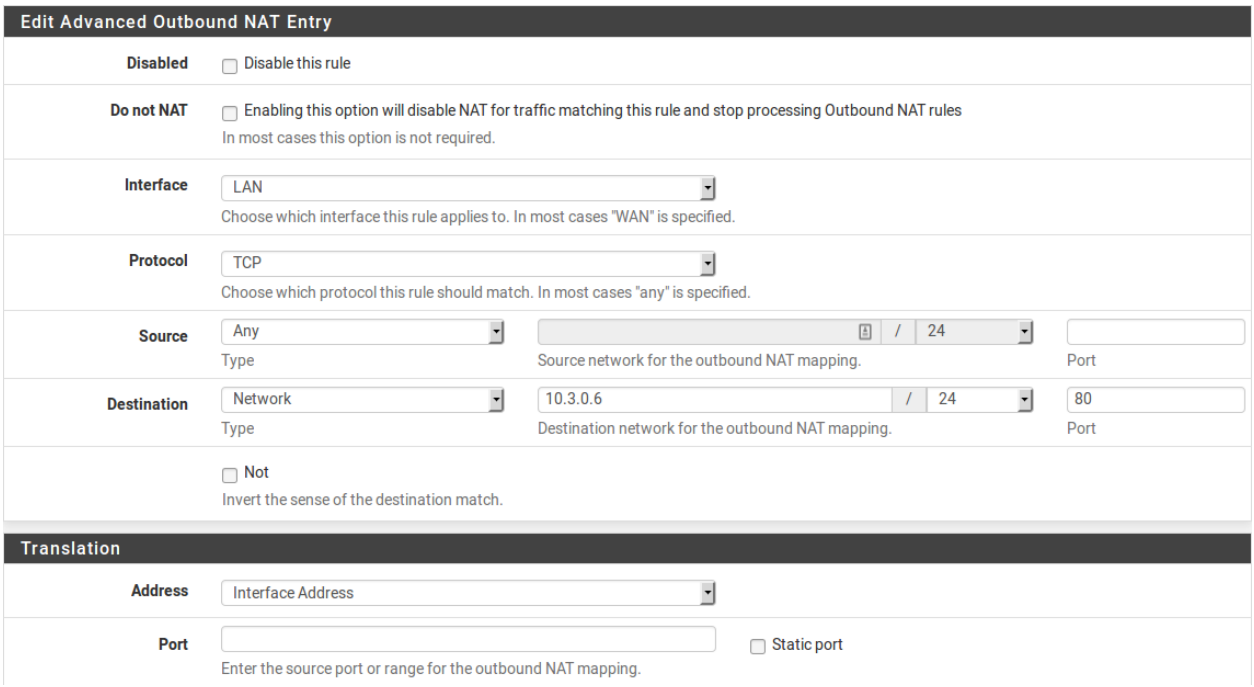


Fig. 13: Regola del NAT in uscita manuale per il dispositivo LAN con gateway mancante

La macchina di destinazione non è in ascolto sulla porta inoltrata

Se la richiesta viene respinta invece di essere programmata quando la connessione viene testata, con ogni probabilità Firew4LL sta inoltrando la connessione correttamente e la connessione viene respinta dal sistema di destinazione. Questo può accadere quando il sistema di destinazione non ha un servizio di ascolto sulla porta in questione, o se la porta in fase di inoltro non corrisponde alla porta su cui il sistema di destinazione è in ascolto.

Per esempio, se il sistema di destinazione è supposto in ascolto delle connessioni SSH, ma la Port Forward è stata inserita per la porta 23 invece di 22, la richiesta molto probabilmente sarebbe respinta dal server. La differenza può essere rilevata tipicamente cercando di connettersi alla porta in questione utilizzando netcat o telnet. Un messaggio come «Connessione rifiutata» indica qualcosa, spesso l'host interno, sta attivamente rifiutando la connessione. Utilizzare **Diagnostica>Porta di prova** può anche aiutare, vedere *Provare una porta TCP*.

ISP blocca la porta

Alcuni ISP filtrano il traffico in entrata verso porte ben note. Controllare i Termini di servizio (ToS) dall'ISP per vedere se c'è una clausola sul funzionamento dei server. Tali restrizioni sono più comuni sulle connessioni residenziali rispetto alle connessioni commerciali. In caso di dubbio, una chiamata all'ISP può chiarire la questione.

Se le porte vengono filtrate dall'ISP, spostare i servizi in una porta diversa può funzionare per aggirare la restrizione. Per esempio, se l'ISP non consente un server sulla porta 80, provare 8080 o 18080.

Prima di tentare di aggirare un filtro, consultare il ToS dell'ISP per garantire che l'esecuzione di un server non sia una violazione delle loro regole.

Testare dall'interno la rete invece che al di fuori

Per impostazione predefinita, le port forward funzioneranno solo quando le connessioni vengono effettuate dall'esterno della rete locale. Questo è un errore molto comune quando si provano port forward.

Se le poret forward non sono necessarie per funzionare internamente, vedere *Nat Reflection*. Tuttavia, il DNS split (*Split DNS*) è una soluzione più corretta ed elegante a questo problema senza bisogno di fare affidamento sulla Nat Reflection o sulla Port Forward, e sarebbe valsa la pena invece di implementarlo.

Anche con la Nat Reflection, testare dall'interno della rete non è necessariamente indicativo del buon funzionamento da Internet. Le restrizioni ISP, restrizioni sui dispositivi di upstream dal firewall, tra le altre possibilità si può non vedere quando si esegue il test dall'interno della rete.

Indirizzo IP virtuale errato o mancante

Quando si utilizzano indirizzi IP che non sono gli indirizzi IP effettivi assegnati ad un'interfaccia, è necessario utilizzare un indirizzo IP virtuale (VIPs, vedere *Indirizzi IP virtuali*). Se una Port Forward su un indirizzo IP alternativo non funziona, può essere richiesto un tipo diverso di VIP. Per esempio, un tipo di Proxy ARP può essere necessario invece di un VIP di «Altro» tipo.

Durante il test, anche assicurarsi che il client si connette al VIP corretto.

Firew4LL non è il router perimetrale

In alcuni scenari Firew4LL è un router interno e ci sono altri router in mezzo e Internet sta anche eseguendo il NAT. In tal caso, una porta forward deve essere inserita sul router di bordo inoltrando la porta a Firew4LL, che utilizzerà un'altra Port Forward per portarla al sistema locale.

Inoltro porte ad un sistema dietro il captive portale

L'inoltro di porte ad un host dietro un captive portal richiede una particolare attenzione. Consultare *port forward per gli host dietro il portale solo quando il sistema di destinazione è collegato* per i dettagli.

Necessità di ulteriori prove

Se nessuna di queste soluzioni funziona, consultare *Stati del firewall* per cercare gli stati NAT che indicano che la connessione ha attraversato il firewall, o *Catturare il pacchetto* per informazioni sull'utilizzo di pacchetti per diagnosticare problemi di inoltro delle porte.

13.9.2 Risoluzione dei problemi del Nat Reflection

La Nat Reflection (*Nat Reflection*) è complessa, e come tale potrebbe non funzionare in alcuni scenari avanzati. Si consiglia di utilizzare il DNS split (vedere *DNS split*) nella maggior parte dei casi. Tuttavia, la Nat Reflection sula versione attuale di Firew4LL funziona ragionevolmente bene per quasi tutti gli scenari, e tutti i problemi sono legati ad un errore di configurazione. Assicurarsi che sia stata intrapresa la strada giusta, e assicurarsi che una vasta gamma di porte non venga inoltrata inutilmente.

Le regole di Nat Reflection sono duplicate anche per ogni interfaccia presente nel sistema, quindi se molte port forward e interfacce sono in uso, il numero di riflettori può facilmente superare i limiti del sistema. Se questo accade, una voce viene stampata nei registri di sistema. Controllare i registri di sistema per eventuali errori o informazioni.

Accesso Web non funzionante con il Nat Reflection abilitato

Se una Port Forward del NAT specificata in modo improprio è presente sul firewall, può causare problemi quando la Nat Reflection è abilitata. Il modo più comune in cui questo problema si presenta è con un server web locale, e la porta 80 inoltrata lì con un **indirizzo esterno** specificato impropriamente.

Se la Nat Reflection è abilitata e l'**indirizzo esterno** è impostato su *qualsiasi*, qualsiasi connessione effettuata sul firewall viene fuori come il server web locale. Per risolvere questo problema, modificare la Port Forward per la porta che offende, e modificare invece l'**indirizzo esterno** nell'*indirizzo dell'interfacc*.

Se è richiesto un indirizzo esterno su *qualsiasi*, allora la Nat Reflection non funzionerà, e il DNS split deve invece essere utilizzato.

13.9.3 Risoluzione dei problemi del NAT in uscita

Quando il NAT in uscita manuale è abilitato e vi sono più sottoreti locali, per ciascuna di esse è richiesta una voce del NAT in uscita. Questo vale soprattutto se il traffico deve uscire con il NAT dopo essere entrato nel router Firew4LL tramite una connessione VPN come OpenVPN.

Una indicazione di una regola NAT in uscita mancante sarebbe vedere i pacchetti lasciare l'interfaccia WAN con un indirizzo sorgente di una rete privata. Per ulteriori dettagli sull'ottenimento e l'interpretazione delle catture dei pacchetti, vedere *Cattura dei pacchetti*.

Nel suo uso più comune, la traduzione degli indirizzi di rete (NAT) permette a più computer che utilizzano IPv4 di essere collegati a Internet utilizzando un unico indirizzo IPv4 pubblico. Firew4LL consente queste semplici implementazioni, ma anche configurazioni NAT molto più avanzate e complesse richieste in reti con più indirizzi IP pubblici.

Il NAT è configurato in due direzioni: in entrata e in uscita. Il NAT in uscita definisce come viene tradotto il traffico che lascia una rete locale destinata a una rete remota, come Internet. Il NAT in entrata si riferisce al traffico che entra in una rete da una rete remota. Il tipo più comune di NAT in entrata è la Port Forward, che è anche il tipo con cui molti amministratori hanno più familiarità.

Nota: In generale, ad eccezione della Traduzione del prefisso di rete (NPt), il NAT su IPv6 non è supportato in Firew4LL. Vi è una ulteriore discussione sull'argomento in *IPv6 e NAT*. Se non diversamente indicato, questo capitolo sta discutendo di NAT con IPv4

Vedi anche:

Per ulteriori informazioni, è possibile accedere all'archivio di Hangout per visualizzare l'Hangout di maggio 2016 sul NAT con Firew4LL 2.3 e il precedente Hangout di agosto 2014 sulla Traduzione degli indirizzi di rete.

13.10 Configurazione predefinita del NAT

Questa sezione descrive la configurazione NAT di default presente su Firew4LL. La configurazione NAT più appropriata che può essere determinata viene generata automaticamente. In alcuni ambienti, questa configurazione potrebbe non essere adatta, e Firew4LL permette di cambiarla completamente dall'interfaccia web. Questo è un contrasto che si crea in molte altre distribuzioni di firewall open source, che non consentono le capacità comunemente richieste in tutte le reti ma piccole e semplici.

13.10.1 Configurazione predefinita del NAT in ucita

In una tipica configurazione Firew4LL a due interfacce con LAN e WAN, la configurazione NAT di default traduce automaticamente il traffico connesso a Internet all'indirizzo IP della WAN. Quando si configurano più interfacce WAN, il traffico che lascia qualsiasi interfaccia WAN viene automaticamente tradotto all'indirizzo dell'interfaccia WAN utilizzata.

La porta statica è configurata automaticamente per IKE (parte di IPsec). La porta statica è trattata più dettagliatamente in *NAT in uscita* sul NAT in uscita.

Per rilevare interfacce di tipo WAN da utilizzare con NAT, Firew4LL ricerca la presenza di un gateway selezionato nella configurazione dell'interfaccia se ha un indirizzo IP statico, o Firew4LL assume che l'interfaccia sia WAN se si tratta di un tipo dinamico come PPPoE o DHCP.

13.10.2 Configurazione predefinita del NAT in entrata

Per impostazione predefinita, non è permesso far entrare nulla da Internet sull'interfaccia WAN. Se il traffico avviato su Internet deve poter raggiungere un host sulla rete interna, è necessaria la porta forward o il NAT 1:1. Questo aspetto è trattato nelle prossime sezioni.

CAPITOLO 14

Routing

14.1 Gateway

I gateway sono la chiave dell'instradamento; sono sistemi attraverso i quali altre reti possono essere raggiunte. Il tipo di gateway con cui la maggior parte delle persone ha familiarità è un gateway predefinito, ovvero il router attraverso il quale un sistema si connetterà a Internet o ad altre reti che non ha un percorso più specifico da raggiungere. I gateway sono utilizzati anche per il routing statico, dove altre reti devono essere raggiunte attraverso specifici router locali. Nella maggior parte delle reti normali, i gateway si trovano sempre nella stessa sottorete di una delle interfacce di un sistema. Per esempio, se un firewall ha un indirizzo IP come 192.168. 22.5/24, allora un gateway ad un'altra rete dovrebbe essere da qualche parte all'interno di 192.168.22.x se l'altra rete è raggiungibile attraverso quell'interfaccia. Una notevole eccezione a questo sono le interfacce point-to-point come quelle utilizzate nei protocolli basati su PPP, che spesso hanno indirizzi IP di gateway in un'altra sottorete perché non sono utilizzati nello stesso modo.

14.1.1 Famiglie degli indirizzi gateway (IPv4 e IPv6)

Quando si lavora con l'instradamento e i gateway, la funzionalità e le procedure sono le stesse sia per gli indirizzi IPv4 e IPv6, tuttavia tutti gli indirizzi per una data rotta devono coinvolgere gli indirizzi della stessa famiglia. Ad esempio, una rete IPv6 deve essere instradata utilizzando un gateway/router IPv6. Non è possibile creare un percorso per una rete IPv6 utilizzando un indirizzo di gateway IPv4. Quando si lavora con gruppi di gateway, si applica la stessa restrizione; tutti i gateway di un gruppo gateway devono essere della stessa famiglia di indirizzi.

14.1.2 Gestione del gateway

Prima che un gateway possa essere utilizzato per qualsiasi scopo, deve essere aggiunto alla configurazione del firewall.

Se viene utilizzato un gateway per un'interfaccia di tipo WAN, può essere aggiunto nella pagina di configurazione di tale interfaccia (vedere *Basi di configurazione dell'interfaccia*), oppure può essere aggiunto manualmente e quindi selezionato dall'elenco a discesa sulla configurazione dell'interfaccia.

I tipi di interfaccia dinamica come DHCP e PPPoE ricevono un gateway automatico noto come **Dinamico (Dynamic)** nell'elenco dei gateway. I parametri per questi gateway possono essere regolati allo stesso modo dei parametri per un gateway statico, ma un gateway dinamico non può essere eliminato.

Per aggiungere o gestire i gateway:

- Passare a **Sistema>Routing**
- Fare clic sulla scheda di **Gateway**
- Fare clic su  **Aggiungere** in cima o in fondo alla lista per creare un nuovo gateway
- Fare clic su  accanto ad una voce per modificare un gateway esistente
- Fare clic su  accanto ad una voce per eliminare un gateway
- Fare clic su  per disattivare un gateway attivo
- Fare clic su  per attivare un gateway disabilitato

Le singole opzioni per i gateway sono discusse in dettaglio nella prossima sezione.

14.2 Impostazioni del gateway

Quando si aggiunge o si modifica un gateway, viene presentata una schermata che elenca tutte le opzioni per controllare il comportamento del gateway. Le uniche impostazioni richieste sono l'**interfaccia**, il **nome** e il **gateway** (indirizzo IP).

14.2.1 Interfaccia

L'interfaccia attraverso la quale viene raggiunto il gateway. Ad esempio, se si tratta di un gateway locale sulla sottorete LAN, scegliere qui l'interfaccia *LAN*.

14.2.2 Famiglia dell'indirizzo

IPv4 o *IPv6*, a seconda del tipo di indirizzo per questo gateway.

14.2.3 Nome

Il **nome** per il gateway, come riportato nell'elenco del gateway, e vari menu a discesa e altri selettori per i gateway. Può contenere solo caratteri alfanumerici, o un underscore, ma non spazi. Per esempio: WANGW, GW_WAN e WANGATE sono validi ma WAN GW non è permesso.

14.2.4 Gateway

L'indirizzo IP del gateway. Come detto in precedenza, questo deve risiedere in una sottorete direttamente configurato sull'Interfaccia selezionata.

14.2.5 Gateway predefinito

Se selezionato, questo gateway è trattato come gateway predefinito per il sistema. Il gateway predefinito è il gateway dell'ultima risorsa. Viene usato quando non ci sono altre rotte specifiche. Il firewall può avere un gateway predefinito IPv4 e un gateway predefinito IPv6.

14.2.6 Disabilitare il monitoraggio del gateway

Per default, il sistema esegue un ping ad ogni gateway una volta al secondo per monitorare la latenza e la perdita di pacchetti per il traffico all'indirizzo IP monitorato. Questi dati vengono utilizzati per le informazioni sullo stato del gateway e anche per disegnare il grafico della qualità RRD. Se questo monitoraggio è indesiderabile per qualsiasi motivo, può essere disabilitato selezionando **Disabilitare il monitoraggio del gateway**. Notare che se lo stato del gateway non è monitorato, allora le Multi-WAN non funzioneranno correttamente in quanto non sono in grado di rilevare guasti.

14.2.7 IP da monitorare

L'opzione indirizzo **IP da monitorare** configura l'indirizzo IP utilizzato per determinare lo stato del gateway. Per impostazione predefinita il sistema eseguirà un ping sull'indirizzo IP del gateway. Questo non è sempre auspicabile, specialmente nel caso in cui l'indirizzo IP del gateway sia locale, come su un modem via cavo o su CPE DSL. In casi come questo ha più senso per effettuare un ping su qualcosa di più upstream, come un server DNS ISP o un server su Internet. Un altro caso è quando un ISP è incline a guasti upstream, quindi effettuare un ping su un host di Internet è un test più accurato per determinare se una WAN è utilizzabile piuttosto che testare il collegamento stesso. Alcune scelte popolari includono i server DNS pubblici di Google, o siti web popolari come Google o Yahoo. Se l'indirizzo IP specificato in questa casella non è direttamente connesso, viene aggiunto un percorso statico per assicurare che il traffico verso l'indirizzo IP da monitorare parta attraverso il gateway previsto. Ogni gateway deve avere un unico indirizzo IP da monitorare.

Lo stato di un gateway percepito dal firewall può essere controllato visitando **Stato>Gateway** o utilizzando il widget del **gateway** sulla dashboard. Se il gateway mostra **Online**, l'indirizzo IP da monitorare restituisce correttamente i ping.

14.2.8 Stato da forzare

Quando **Gateway down** è selezionato, il gateway sarà sempre considerato down, anche quando i ping vengono restituiti dall'indirizzo IP da monitorare. Ciò è utile nei casi in cui una WAN si stia comportando in modo incoerente e le transizioni del gateway stiano causando problemi. Il gateway può essere forzato in stato *down* in modo che altri gateway possano essere preferiti fino a quando si stabilizza.

14.2.9 Descrizione

Una **descrizione** facoltativa della voce gateway per riferimento. Una breve nota sul perché il gateway o l'interfaccia è usato può essere utile, o può essere lasciata in bianco.

14.2.10 Avanzate

Diversi parametri possono essere modificati per controllare come un gateway viene monitorato o trattato in uno scenario Multi-WAN. La maggior parte degli utenti non avrà bisogno di modificare questi valori. Per accedere alle opzioni

avanzate, fare clic sul pulsante  **Visualizzare avanzate**. Se una delle opzioni avanzate è impostata, questa sezione viene espansa automaticamente. Per maggiori informazioni sull'utilizzo di connessioni WAN multiple, vedere *Connessioni WAN multiple*.

Peso

Quando si utilizza le Multi-WAN, se due WAN hanno quantità di banda diverse, il parametro Peso regola la razione alla quale vengono utilizzate le WAN. Per esempio, se WAN1 ha 5Mbit/s e WAN2 ha 10Mbit/s, il peso della WAN1 sarà *1* e della WAN2 *2*. Poi per ogni tre connessioni che escono, una userà WAN1 e due useranno WAN2. Utilizzando questo metodo, le connessioni sono distribuite nel modo più probabile per utilizzare meglio la larghezza di banda disponibile. Si può scegliere un peso da *1* a *30*.

Carico dei dati

Per conservare la larghezza di banda, il demone dpinger invia un ping con una dimensione del carico utile di 0 per default in modo che nessun dato sia contenuto nella richiesta di eco ICMP. Tuttavia, in rare circostanze un CPE, un router ISP o un luppolo intermedio possono rilasciare o rifiutare pacchetti ICMP senza un carico utile. In questi casi, impostare la dimensione del carico utile sopra 0. Di solito una dimensione di 1 è sufficiente per soddisfare apparecchiature colpite.

Soglie di latenza

I campi delle **Soglie di Latenza** controllano la quantità di latenza considerata normale per questo gateway. Questo valore è espresso in millisecondi (ms). Il valore nel campo **Da** è il limite inferiore sotto il quale il gateway sarebbe considerato in uno stato di avvertimento, ma non down. Se la latenza supera il valore nel campo **A**, è considerata verso down e rimossa dal servizio. I valori corretti in questi campi possono variare a seconda del tipo di connessione in uso, e quali ISP o apparecchiature sono tra il firewall e l'indirizzo IP da monitorare. I valori predefiniti sono **Da** 300 e **A** 500.

Alcune altre situazioni comuni possono richiedere la regolazione di questi valori. Per esempio, alcune linee DSL funzionano bene anche con una latenza più alta, quindi aumentare il parametro **A** a 700 o più ridurrebbe il numero di volte in cui il gateway sarebbe considerato down quando, in effetti, stava funzionando in modo accettabile. Un altro esempio è un tunnel GIF per un provider come he.net per IPv6. A causa della natura dei tunnel GIF e del carico sui server dei tunnel, il tunnel potrebbe funzionare in modo accettabile anche con latenza fino a 900 ms come riportato dalle risposte del ping di ICMP.

Soglie della perdita di pacchetti

Analogamente alle **soglie di latenza**, le **soglie di perdita dei pacchetti** controllano la quantità di perdite di pacchetti in un indirizzo IP da monitorare prima che sia considerato inutilizzabile. Questo valore è espresso in percentuale, 0 in perdita e 100 in perdita totale. Il valore nel campo **Da** è il limite inferiore sotto il quale il gateway sarebbe considerato in uno stato di avvertimento, ma non down. Se la quantità di perdita dei pacchetto supera il valore nel campo **A**, è considerato down e rimosso dal servizio. I valori corretti in questi campi possono variare a seconda del tipo di connessione in uso, e quali ISP o apparecchiature sono tra il firewall e l'indirizzo IP da monitorare. I valori predefiniti sono **Da** 10 e **A** 20.

Poiché con latenza, le connessioni possono essere inclini a diverse quantità di perdita di pacchetti e ancora funzionare in modo utilizzabile, soprattutto se il percorso di un indirizzo IP da monitorare cali o ritardi ICMP a favore di altro traffico. Abbiamo osservato connessioni inutilizzabili con piccole quantità di perdita, e alcuni che sono utilizzabili anche quando si mostra il 45% di perdita. Se si verificano allarmi di perdita su un gateway WAN normalmente funzionante, immettere valori più alti nei campi **Da** e **A** fino a quando un buon equilibrio per il circuito è raggiunto.

Intervallo da sondare

Il valore nel campo **Intervallo da sondare** controlla la frequenza di invio di un ping all'indirizzo IP da monitorare, in *millisecondi*. Il valore predefinito è effettuare un ping due volte al secondo (500 ms). In alcune situazioni, come i collegamenti che hanno bisogno di essere monitorati, ma hanno elevati oneri di dati, anche un piccolo ping ogni secondo può creare problemi. Questo valore può essere aumentato in modo sicuro a condizione che sia inferiore o uguale all'**intervallo di allerta** e non violi il vincolo sul **periodo di tempo** indicato sotto. Valori più bassi effettueranno un oing più spesso e saranno più precisi, ma consumeranno più risorse. Valori più alti saranno meno sensibili al comportamento erratico e consumano meno risorse, al costo della precisione.

Nota: Il grafico di qualità è mediato su secondi, non intervalli, così come l'**intervallo di prova** aumenta la precisione del grafico di qualità diminuisce.

Intervallo di perdita

Tempo in millisecondi prima che i pacchetti siano trattati come persi. Il valore predefinito è 2000 ms (2 secondi). Deve essere superiore o uguale alla **soglia di latenza elevata**.

Se un circuito è noto per avere alta latenza durante il funzionamento normale, questo può essere aumentato per compensare.

Periodo di tempo

La quantità di tempo, in millisecondi, su cui i risultati del ping sono mediati. Il valore predefinito è 60000 (60 secondi, un minuto). Un **periodo di tempo** più lungo richiederà più tempo per la latenza o la perdita per attivare un allarme, ma è meno incline ad essere influenzato dal comportamento erratico nei risultati di ping.

Il **periodo di tempo** deve essere superiore al **doppio** della somma dell'**intervallo da sondare** e dell'**intervallo da sondare**, altrimenti non ci può essere almeno un sondaggio completato.

Intervallo di allerta

L'intervallo di tempo, in millisecondi, nel quale il demone controlla la presenza di una condizione di avviso. Il valore predefinito è 1000 (1 secondo). Questo valore deve essere maggiore o uguale all'**Intervallo da sondare**, perché un allarme non può verificarsi tra i sondaggi.

Usare i gateway non locali

L'opzione **Usare i gateway non locali tramite una rotta specifica dell'interfaccia** consente una configurazione non standard in cui esiste un indirizzo IP del gateway al di fuori di una sottorete dell'interfaccia. Alcuni fornitori che cercano di raschiare il fondo del barile dell'IPv4 hanno fatto ricorso a ciò al fine di non mettere un gateway in ogni sottorete del cliente. Non attivare questa opzione se non richiesto dal fornitore upstream.

14.3 Gruppi di gateway

I gruppi di gateway definiscono insiemi di gateway da utilizzare per il failover o il bilanciamento del carico. I gruppi di gateway possono anche essere usati come valori di **interfaccia** in alcune aree della GUI per il failover del servizio, come OpenVPN, IPsec, e DNS dinamico.

Per informazioni sull'impostazione di tali funzioni, vedere *Connessioni delle WAN multiple*.

14.4 Rotte statiche

Si utilizzano percorsi statici quando gli host o le reti sono raggiungibili attraverso un router diverso dal gateway predefinito. Firew4LL è a conoscenza delle reti ad esso direttamente collegate e raggiunge tutte le altre reti come indicato dalla sua tabella di routing. Nelle reti in cui un router interno collega sottoreti interne supplementari, deve essere definito un percorso statico affinché tale rete sia raggiungibile. I router attraverso i quali queste altre reti sono raggiunte devono prima essere aggiunti come il gateway. Vedere *Gateway* per informazioni sull'aggiunta di gateway.

Rotte statiche si trovano nella sezione **Sistema>Routing** nella scheda **Rotte**.

14.4.1 Gestione rotte statiche

Per aggiungere una rotta:

- Passare a **Sistema>Routing** nella scheda **Rotte**
- Fare clic su **Aggiungere** per creare un nuovo percorso statico
- Compilare la configurazione come segue:

  Rete di destinazione Specifica la maschera di rete e di sottorete raggiungibile utilizzando questo percorso.

  Gateway Definisce il router attraverso il quale si raggiunge questa rete.

  Disabilitato Verifica se il percorso statico non deve essere utilizzato, solo definito.

  Descrizione Testo per descrivere la rotte, il suo scopo, ecc.
- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**

Per gestire le rotte esistenti:

- Passare a **Sistema>Routing** nella scheda rotte
- Fare clic su accanto a una voce per modificare un percorso esistente
- Fare clic su accanto a una voce per eliminare un percorso
- Fare clic su per disattivare un percorso attivo
- Fare clic su per attivare un percorso disabilitato
- Fare clic su **Applicare modifiche**

Esempio di rotta statica

La figura *Rotte statiche* illustra uno scenario in cui è richiesto un percorso statico.

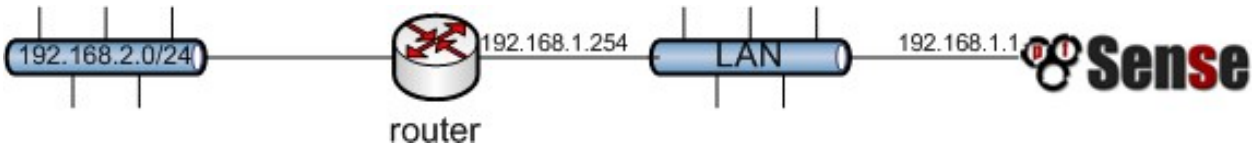


Fig. 1: Rotte statiche

Poiché la rete 192.168.2.0/24 nella figura *Rotte statiche* non si trova su un'interfaccia direttamente collegata a Firew4LL, è necessario un percorso statico in modo che il firewall sappia come raggiungere quella rete. La figura *Configurazione della rotta statica* mostra il percorso statico appropriato per il diagramma di cui sopra. Come accennato in precedenza, prima che un percorso statico possa essere aggiunto a un gateway deve prima essere definito.

Possono essere necessari anche aggiustamenti delle regole del firewall. Se si utilizzano regole LAN personalizzate, esse devono consentire il passaggio del traffico da una fonte delle reti raggiungibili tramite percorsi statici su LAN.

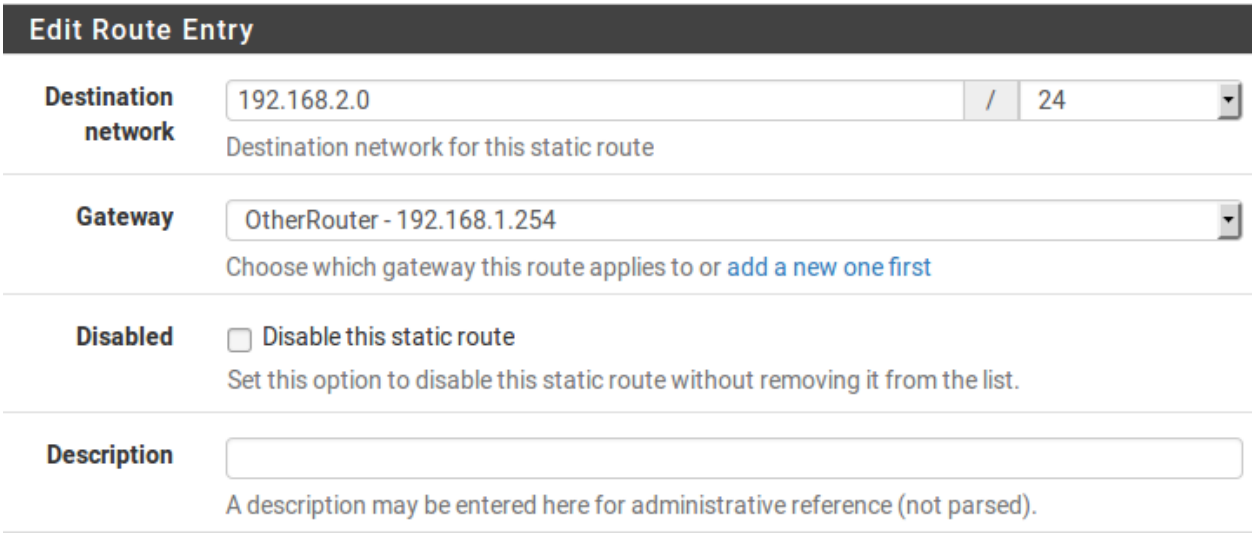


Fig. 2: Configurazione della rotta statica

14.4.2 Bypassare le regole del firewall per il traffico sulla stessa interfaccia

In molte situazioni, quando si utilizzano rotte statiche, il traffico finisce per essere instradato in modo asimmetrico. Ciò significa che il traffico seguirà un percorso diverso in una direzione rispetto al traffico che scorre nella direzione opposta. Prendere la figura *Routing asimmetrico* come esempio.

Il traffico da PC1 a PC2 passerà attraverso Firew4LL poiché è il gateway predefinito per PC1, ma il traffico nella direzione opposta andrà direttamente dal router al PC1. Dal momento che Firew4LL è un firewall stateful, deve vedere il traffico affinché l'intera connessione sia in grado di filtrare il traffico correttamente. Con un routing asimmetrico come questo esempio, qualsiasi firewall stateful farà cadere il traffico legittimo perché non può mantenere correttamente lo stato senza vedere il traffico in entrambe le direzioni. Questo generalmente riguarda solo il TCP, poiché altri protocolli non hanno un handshake della connessione formale che il firewall può riconoscere per l'uso nel routing di stato.

Negli scenari di routing asimmetrico, vi è un'opzione che può essere utilizzato per impedire al traffico legittimo di cadere. L'opzione aggiunge regole del firewall che permettono tutto il traffico tra le reti definite nelle rotte statiche che usano un insieme più permissivo di regole e gestione dello stato. Per attivare questa opzione:

- Cliccare su **Sistema>Avanzate**
- Fare clic sulla scheda **Firewall/NAT**
- Selezionare **Bypassare le regole del firewall per il traffico sulla stessa interfaccia**
- Fare clic su **Salvare**

In alternativa, le regole del firewall possono essere aggiunte manualmente per consentire un traffico simile. Sono necessarie due regole, una nella scheda dell'interfaccia in cui il traffico entra (ad es. LAN) e un'altra nella scheda di **Floating**:

- Passare a **Firewall>Regole**

- Fare clic sulla scheda per l'interfaccia in cui il traffico entrerà (ad es. **LAN**)
- Fare clic su **Aggiungere** per aggiungere una nuova regola in cima alla lista
- Usare le seguenti impostazioni:

  Protocollo *TCP*

  Sorgente I sistemi locali che utilizzano la rotta statica (ad es. *rete LAN*)

  Destinazione La rete all'altra estremità del percorso

  Flag TCP Selezionare **Qualsiasi Flag** (in **Funzionalità avanzate**)

  Tipo di stato *Stato Sloppy* (in **Caratteristiche avanzate**)
- Fare clic su **Salvare**
- Fare clic sulla scheda **Floating**
- Fare clic su **Aggiungere** per aggiungere una nuova regola in cima alla lista
- Usare le seguenti impostazioni:

  Interfaccia L'interfaccia dove il traffico ha avuto origine (ad es. **LAN**)

  Direzione *Out*

  Protocollo *TCP*

  Sorgente I sistemi locali che utilizzano la rotta statica (ad es. *rete LAN*)

  Destinazione La rete all'altra estremità del percorso

  Flag TCP selezionare **Qualsiasi flag** (in **Funzionalità avanzate**)

  Tipo di stato Stato Sloppy (in **Caratteristiche avanzate**)
- Fare clic su **Salvare**

Se il traffico aggiuntivo proveniente da altre fonti o destinazioni è indicato come bloccato nei registri del firewall con flag TCP come «TCP:SA» o «TCP:PA», le regole possono essere modificate o copiate per corrispondere a tale traffico.

Nota: Se è richiesto il filtraggio del traffico tra sottoreti indirizzate in modo statico, deve essere fatto sul router e non il firewall in quanto il firewall non è in una posizione sulla rete in cui può controllare efficacemente il traffico.

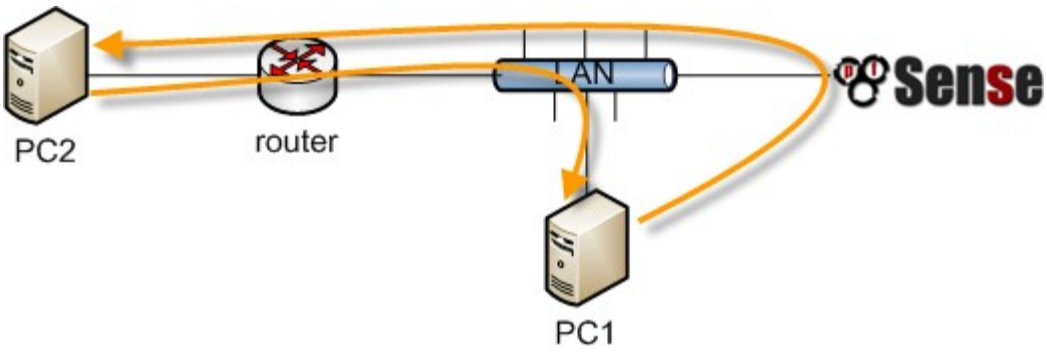


Fig. 3: Routing asimmetrico

14.4.3 Reindirizzamenti ICMP

Quando un dispositivo invia un pacchetto al suo gateway predefinito, e il gateway sa che il mittente può raggiungere la rete di destinazione tramite un percorso più diretto, invierà un messaggio di reindirizzamento ICMP in risposta e inoltrerà il pacchetto come configurato. Il reindirizzamento ICMP fa sì che un percorso per tale destinazione venga temporaneamente aggiunto alla tabella di routing del dispositivo d'invio, e il dispositivo utilizzerà successivamente quel percorso più diretto per raggiungere quella destinazione.

Questo funzionerà solo se il sistema operativo del client è configurato per consentire i reindirizzamenti ICMP, che è di solito il caso dell'impostazione predefinita.

I reindirizzamenti ICMP sono comuni quando sono presenti percorsi statici che puntano a un router sulla stessa interfaccia dei PC client e di altri dispositivi di rete. Il diagramma del routing asimmetrico della sezione precedente ne è un esempio.

I reindirizzamenti ICMP hanno una cattiva reputazione per lo più immeritata da parte di alcuni nella comunità di sicurezza perché consentono la modifica di una tabella di routing del client. Tuttavia non rappresentano il rischio che alcuni implicano, perché per essere accettati, il messaggio di reindirizzamento ICMP debba includere i primi 8 byte di dati dal datagramma originale. Un host in grado di vedere che i dati e quindi in grado di forgiare con successo illeciti reindirizzamenti ICPM è in grado di realizzare lo stesso risultato finale in molti altri modi.

14.5 Instradamento degli indirizzi IP pubblici

Questa sezione riguarda l'instradamento di indirizzi IP pubblici in cui una sottorete IP pubblica è assegnata a un'interfaccia interna su un'unica distribuzione di firewall.

Se un cluster ad elevata disponibilità è in uso, vedere *Fornire ridondanza senza NAT*.

14.5.1 Assegnazioni degli IP

L'ISP deve assegnare almeno due sottoreti IP pubbliche. Una è per la WAN del firewall e una per l'interfaccia interna. Questa è comunemente una sottorete /30 per la WAN, con una seconda sottorete assegnata per l'interfaccia interna. Questo esempio userà un /30 sulla WAN come mostrato nella tabella *Blocco degli IP della WAN* e una sottorete pubblica /29 su un'interfaccia interna OPT come mostrato nella tabella *Blocco degli IP interni*.

Tabella 1: Blocco degli IP della WAN

+====================+===-+ | 198.51.100.64/30 | +====================+===-+ | Indirizzo IP | Assegnato a | +====================+===-+ | 198.51.100.65 | router ISP (Firew4LL di default gateway)| +====================+===-+ | 198.51.100.66 | indirizzo di interfaccia Firew4LL IP WAN| +====================+===+

Tabella 2: Blocco degli IP interni

+==================+============================-+ | 192.0.2.128/29 | +==================+============================-+ | Indirizzo IP | Assegnato a | +==================+============================-+ | 192.0.2.129 | Interfaccia Firew4LL OPT| +==================+============================-+ | 192.0.2.130 | host interni | +==================+============================-+ | 192.0.2.131 | | +==================+============================-+ | 192.0.2.132 | | +==================+============================-+ | 192.0.2.133 | | +==================+============================-+ | 192.0.2.134 | | +==================+============================-+

14.5.2 Configurazione dell'interfaccia

In primo luogo configurare le interfacce WAN e OPT. L'interfaccia LAN può essere utilizzata anche per gli indirizzi IP pubblici, se desiderato. In questo esempio, la LAN è una sottorete con IP privato e OPT1 è la sottorete con IP pubblico.

Configurazione della WAN

Aggiungere l'indirizzo IP e il gateway di conseguenza. La figura *Configurazione del gateway e dell'IP della WAN* mostrano la WAN configurata come mostrato nella tabella *blocco di IP della WAN*.

Fig. 4: Configurazione del gateway e dell'IP della WAN

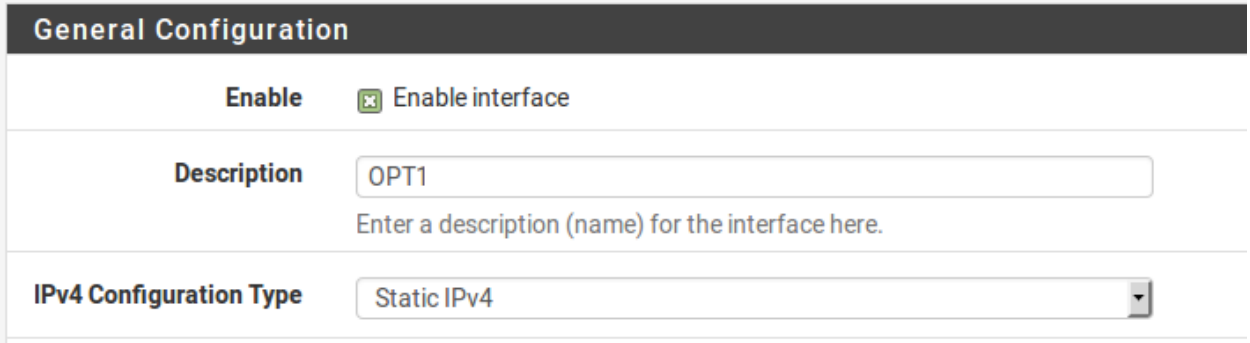


Fig. 5: Configurazione dell'interfaccia OPT1 per il routing

Configurare OPT1

Ora abilitare l'OPT1, eventualmente cambiare il suo nome, e configurare l'indirizzo IP e la maschera di sottorete. La figura *Configurazione dell'interfaccia OPT1 per il routing* mostra l'OPT1 configurata come mostrato nella tabella *blocco degli IP interni*.

Fig. 6: Configurazione dell'indirizzo IP della OPT1 per il routing

14.5.3 Configurazione del NAT

L'impostazione predefinita per tradurre il traffico interno all'IP della WAN deve essere ignorata quando si utilizzano indirizzi IP pubblici su un'interfaccia interna.

- Arrivare su **Firewall>NAT**
- Fare clic sulla scheda **In uscita**
- Selezionare la generazione di regole del NAT ibrido in uscita
- Fare clic su Salvare
- Fare clic su  per aggiungere una nuova regola in cima alla lista con le seguenti impostazioni:

  Nessun NAT Selezionare, in modo che NAT verrà disabilitato

  Interfaccia *WAN*

  Protocollo *Qualsiasi*

  Sorgete Rete, inserire la sottorete pubblica dell'IP, 192.0.2.128/29

  Destinazione *Qualsiasi*

- Fare clic su **Salvare**

Questo sovrascriverà le regole automatiche di default che traducono tutto il traffico dalle interfacce locali lasciando l'interfaccia WAN sull'indirizzo IP della WAN. Il traffico proveniente dalla rete OPT1 192.0.2.128/29 non viene tradotto a causa della regola aggiunta manualmente che lo esclude dal NAT. Questa configurazione mantiene il comportamento automatico per altre interfacce interne, in modo da non perdere i vantaggi delle regole automatiche del NAT in uscita. Questa configurazione è mostrata in figura *Configurazione del NAT in uscita*.

Se vengono utilizzati indirizzi IP pubblici su **tutte** le interfacce locali, impostare **Disabilitare il NAT in uscita** invece di usare la modalità ibrida.

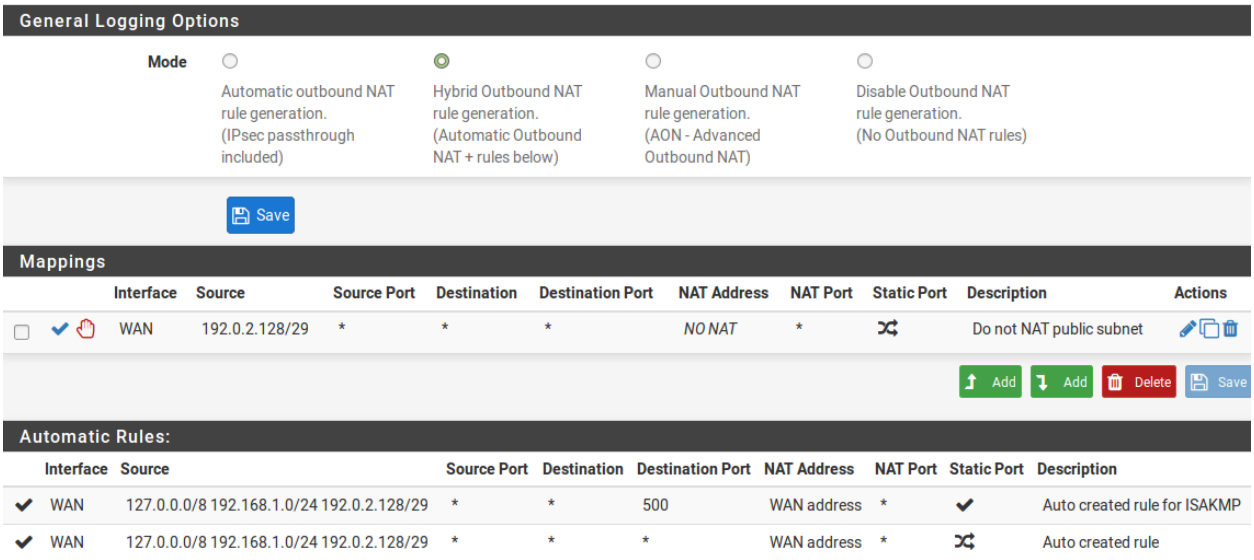


Fig. 7: Configurazione del NAT in uscita

14.5.4 Configurazione della regola del firewall

La configurazione degli indirizzi NAT e IP è ora completa. Le regole del firewall dovranno essere aggiunte per consentire il traffico in uscita e in arrivo. La figura *Regole del firewall per la OPT1* mostra una configurazione simile a DMZ, dove tutto il traffico destinato alla sottorete LAN viene respinto, il DNS e i ping all'indirizzo IP dell'interfaccia OPT1 sono permessi, e HTTP è permesso in uscita.

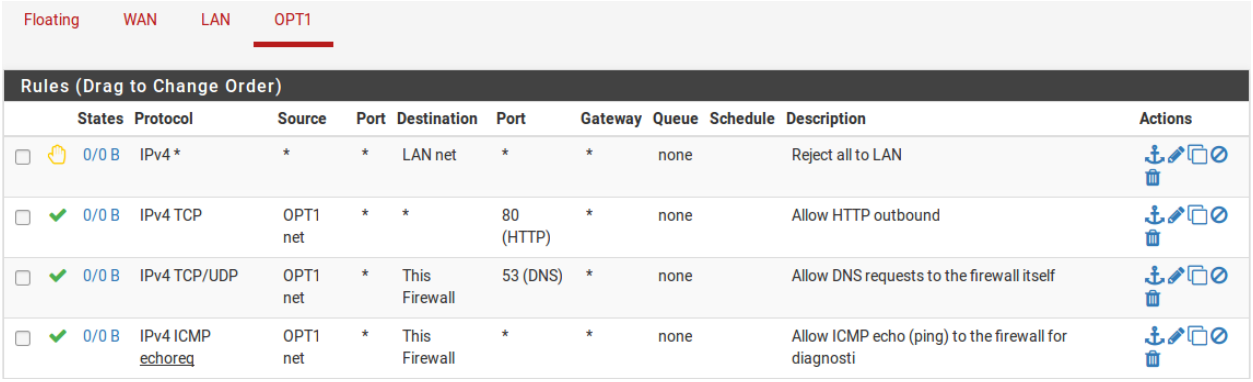


Fig. 8: Regole del firewall per la OPT1

Per consentire il traffico da Internet agli indirizzi IP pubblici su un'interfaccia interna, aggiungere regole sulla WAN utilizzando gli indirizzi IP pubblici come destinazione. La figura *Regole del firewall per la WAN* mostra una regola che consente l'HTTP su 192.0.2.130, uno degli indirizzi IP pubblici sull'interfaccia interna, come mostrato nella tabella *Blocco degli IP interni*.

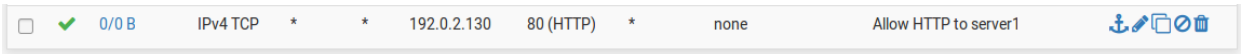


Fig. 9: Regole del firewall per la WAN Dopo aver configurato le regole del firewall come desiderato, l'impostazione è completa.

Nota: Il traffico scorrerà dalla LAN a questa sottorete pubblica di default senza NAT. Se questo comportamento non è desiderato, regolare il firewall della LAN e le regole NAT di conseguenza. Inoltre, potrebbe essere necessario bypassare la politica di routing per consentire il passaggio dalla LAN a questa interfaccia.

14.6 Protocolli di routing

Al momento, tre protocolli di routing sono supportati da Firew4LL:

- PIR (Protocollo sulle informazioni del routing)
- BGP (Protocollo sulle porte di gateway)
- OSf4l (Prima percorso aperto più breve).

Questa sezione fa luce sui dettagli, e presume la comprensione dei protocolli di routing come prerequisito. Una discussione approfondita sui protocolli di routing non rientra nell'ambito di questo libro.

14.6.1 RIP

RIP fa parte del pacchetto instradato. Per installarlo:

- Passare a **Sistema>Gestione dei pacchetti**
- Fare clic su **Pacchetti disponibili**
- Individuare l'"**instradamento** nell'elenco o ricercarlo
- Fare clic su  Installare a destra della voce del pacchetto **instradato**.

- Fare clic su  **Confermare**
- Attendere il completamento dell'installazione
- Navigare verso **Servizi>RIP**

Per configurare il RIP:

- Selezionare la casella **Abilitare RIP**
- Scegliere le **interfacce** RIP su cui si ascolteranno e invieranno gli aggiornamenti di routing
- Selezionare la **versione RIP**
- Inserire una **password per RIPv2** se RIPv2 è in uso e richiede una password sulla rete.
- Fare clic su **Salvare**

RIP avvierà immediatamente e inizierà ad inviare e ricevere aggiornamenti di routing sulle interfacce specificate.

14.6.2 BGP

È disponibile un pacchetto BGP che utilizza OpenBGPD da OpenBSD. Per installarlo:

- Passare a **Sistema>Gestione di pacchetti**
- Fare clic su **Pacchetti disponibili**
- Individuare **OpenBGPD** nella lista, o cercarlo
- Fare clic su  **Installare** a destra della voce del pacchetto **OpenBGPD**.
- Fare clic su  Confermare
- Attendere il completamento dell'installazione
- Andare a **Servizi>OpenBGPD**

  BGP è una bestia complessa, e descriverla in dettaglio è al di fuori dell'ambito di questo libro. La configurazione di OpenBGPD su Firew4LL è immediata per chi conosce BGP. Durante lo sviluppo di questo pacchetto, abbiamo fatto affidamento sul libro su BGP di O'Reilly e lo consigliamo a chiunque cerchi di implementare BGP.

  La forma generale della configurazione per il pacchetto OpenBGPD è:

- Configurare un gruppo nella scheda **Gruppo** con l'AS remoto
- Configura uno o più vicini nella scheda **Vicini** come membri del **gruppo** definito
- Configurare la scheda **Impostazioni** come desiderato per l'AS locale e le reti da annunciare.

14.6.3 OSf4l

È disponibile anche un pacchetto OSf4l che utilizza il demone per il routing di Quagga. Come per BGP, per installarlo:

- Passare a **Sistema>Gestione dei pacchetti**
- Fare clic su **pacchetti disponibili**
- Individuare **Quagga_OSf4l** nell'elenco o cercarlo
- Fare clic su  Installare a destra della voce del pacchetto **Quagga_OSf4l**.

- Fare clic su **Confermare**
- Attendere il completamento dell'installazione
- Andare a **Servizi>Quagga OSf4l**

L'OSf4l è anche un protocollo di instradamento piuttosto complesso, anche se non così complesso da configurare come BGP. I dettagli della configurazione di OSf4lD sono anche al di fuori dello scopo di questo libro, anche se per qualcuno abituato a OSf4l le opzioni di configurazione presenti nella GUI saranno familiari.

La forma generale di configurazione per il pacchetto Quagga OSf4l è:

- **Aggiungere le interfacce necessarie, con le sottoreti di interfaccia** locale contrassegnate come passive, e quelle rivolte verso altri router OSf4l come attive.
- **Configurare le impostazioni generali come necessario con il router** dell'ID, ID dell'area, e così via.

Site-to-Site dell'OpenVPN con Multi-WAN e OSf4l contiene un esempio di configurazione di OSf4l.

14.7 Risoluzione dei problemi con le rotte

Quando si diagnosticano problemi di flusso di traffico, una delle prime cose da verificare sono i percorsi noti per Firew4LL.

14.7.1 Visualizzazione delle rotte

Ci sono due modi per visualizzare i percorsi: tramite la WebGUI, e tramite la riga di comando.

Per visualizzare i percorsi nella WebGUI, navigare fino a **Diagnostica>Rotte** e l'output è mostrato in maniera simile a lla figura *Visualizzazione della rotte*.

IPv4 Routes

Destination	Gateway	Flags	Use	Mtu	Netif	Expire
default	198.51.100.1	UGS	1797	1500	igb1	
10.2.0.0/24	link#2	U	0	1500	igb0	
10.2.0.1	link#2	UHS	0	16384	lo0	
127.0.0.1	link#11	UH	204	16384	lo0	
198.51.100.0/24	link#3	U	907	1500	igb1	
198.51.100.1	00:08:a2:09:95:b6	UHS	2519	1500	igb1	
198.51.100.2	link#3	UHS	0	16384	lo0	

Fig. 10: Visualizzazione della rotte

L'uscita dalla linea di comando è simile a quello visto nella WebGUI:

```
# netstat -rWn
```

Routing tables Internet: Destination Gateway Flags Use Mtu Netif Expire default 198.51.100.1 UGS 1822 1500 igb1 10.2.0.0/24 link#2 U 0 1500 igb0 10.2.0.1 link#2 UHS 0 16384 lo0 127.0.0.1 link#11 UH 204 16384 lo0 198.51.100.0/24 link#3 U 1181 1500 igb1 198.51.100.1 00:08:a2:09:95:b6 UHS 2789 1500 igb1 198.51.100.2 link#3 UHS 0 16384 lo0

Le colonne visualizzate su questi schermi indicano varie proprietà dei percorsi, e sono spiegati in seguito in questa sezione.

Destinazione

Questa colonna contiene l'host o la rete di destinazione. Il percorso predefinito per il sistema è semplicemente elencato come predefinito. In caso contrario, gli host sono elencati come per indirizzo IP, e le reti sono elencati con un indirizzo IP e una maschera di sottorete CIDR.

Gateway

UUn gateway è il router attraverso il quale i pacchetti che vanno verso una destinazione specifica vengono inviati. Se questa colonna mostra un collegamento, come link#1, allora quella rete è direttamente raggiungibile da quell'interfaccia e non è necessario un instradamento speciale. Se un host è visibile con un indirizzo MAC, allora è un host raggiungibile localmente con una voce nella tabella ARP, e i pacchetti vengono inviati direttamente.

Flag

Ci sono un bel paio di flag, che sono tutte coperte nella pagina principale di FreeBSD per *netstat(1)*, riprodotti nella tabella

Tabella delle flag e dei significati delle rotte con alcune modifiche.

Tabella 3: Tabella delle flag e dei significati delle rotte

Lettera	Flag	Significato
1	RTF_PROTO1	Specifico protocollo di routing flag#1
2	RTF_PROTO2	Specifico protocollo di routing flag#2
3	RTF_PROTO3	Specifico protocollo di routing flag#3
B	RTF_BLACKHOLE	Pacchetti da eliminare durante gli aggiornamenti
B	RTF_BROADCAST	Rappresenta un indirizzo di broadcast
D	RTF_DYNAMIC	Creato dinamicamente dal reindirizzamento
sol	RTF_GATEWAY	Destinazione richiede l'inoltro dall'intermediario
H	RTF_HOST	Voce dell'host (altrimenti rete)
L	RTF_LLINFO	Protocollo valido per la traduzione degli indirizzi di collegamento
M	RTF_MODIFIED	Modificato in modo dinamico (dal reindirizzamento)
R	RTF_REJECT	Host o rete non raggiungibile
S	RTF_STATIC	Aggiunto manualmente
U	RTF_UP	rotte utilizzabile
X	RTF_XRESOLVE	daemon esterno traduce il proto per l'indirizzo del link

Ad esempio, un percorso contrassegnato come UGS è un percorso utilizzabile, i pacchetti vengono inviati tramite il gateway elencati, ed è un itinerario statico.

Ref

In questa colonna conta il numero corrente di utilizzi attivi di un determinato percorso.

Uso

Questo contatore è il numero totale di pacchetti inviati tramite questo percorso. Questo è utile per determinare se un percorso è effettivamente utilizzato, in quanto aumenterà continuamente perché i pacchetti utilizzano il percorso.

Netif

L'interfaccia di rete utilizzata per questa rotta.

Scadenza

Per le voci dinamiche, questo campo mostra quanto tempo ci vuole prima che questa rotta scada se non viene usata di nuovo.

14.7.2 Utilizzare traceroute

Traceroute è uno strumento utile per testare e verificare percorsi e funzionalità multi-WAN, tra gli altri usi. Mostra ogni «salto» lungo il percorso di un pacchetto che viaggia da un capo all'altro, insieme alla latenza incontrata nel raggiungere quel punto intermedio. Su Firew4LL, un traceroute può essere eseguito navigando fino a **Diagnostica>Traceroute**, o utilizzando traceroute alla riga di comando. Per i client che eseguono Windows, il programma è disponibile con il nome Tracert.

Ogni pacchetto IP contiene un valore di tempo di vita (time-to-live **TTL**). Quando un router passa un pacchetto, decrementa il TTL di uno. Quando un router riceve un pacchetto con un TTL di 1 e la destinazione non è una rete collegata localmente, il router restituisce un messaggio di errore ICMP «Tempo di vita superato» e lascia cadere il pacchetto. Questo serve a limitare l'impatto dei cicli di instradamento, che altrimenti causerebbero un ciclo indefinito per ciascun pacchetto.

Traceroute utilizza questo TTL a proprio vantaggio per mappare il percorso verso una destinazione di rete specifica. Inizia inviando il primo pacchetto con un TTL di 1. Il primo router (di solito il gateway predefinito) restituirà un errore di tempo di vita superato di ICMP. Il tempo tra l'invio del pacchetto e la ricezione dell'errore ICMP è l'orario visualizzato, elencato insieme all'indirizzo IP che ha inviato l'errore e il suo DNS inverso, se qualsiasi. Dopo aver inviato tre pacchetti con un TTL di 1 e aver visualizzato i loro tempi di risposta, incrementerà il TTL a 2 e invierà altri tre pacchetti, notando le stesse informazioni per il secondo salto. Traceroute incrementa il TTL e ripete il processo fino a raggiungere la destinazione specificata o supera il numero massimo di salti.

Traceroute funziona in modo leggermente diverso sui sistemi operativi Windows e Unix-like (BSD, Linux, Mac OS X, Unix, ecc.). Windows usa i pacchetti di richiesta dell'echo di ICMP (ping) mentre i sistemi come Unix usano i pacchetti UDP per impostazione predefinita. ICMP e UDP sono protocolli di livello 4, e traceroute è fatto a livello 3, quindi il protocollo utilizzato è in gran parte irrilevante, tranne quando si considera una politica di configurazione di routing. Traceroute da client Windows sarà sulla politica della rotta basata su quale regola permette le richieste echo di ICMP, mentre i client come Unix saranno instradati dalla regola corrispondente alle porte UDP in uso.

In questo esempio, traceroute viene utilizzato per visualizzare il percorso a www.google.com:

```
# traceroute www.google.com
```

traceroute: Warning: www.google.com has multiple addresses; using 74.125.95.99 traceroute to www.l.google.com (74.125.95.99), 64 hops max, 40 byte packets 1 core (172.17.23.1) 1.450 ms 1.901 ms 2.213 ms 2 172.17.25.21 (172.17.25.21) 4.852 ms 3.698 ms 3.120 ms 3 bb1-g4-0-2.ipltin.ameritech.net (151.164.42.156) 3.275 ms 3.210 ms 3.215 ms 4 151.164.93.49 (151.164.93.49) 8.791 ms 8.593 ms 8.891 ms 5 74.125.48.117 (74.125.48.117) 8.460 ms 39.941 ms 8.551 ms 6 209.85.254.120 (209.85.254.120) 10.376 ms 8.904 ms 8.765 ms 7 209.85.241.22 (209.85.241.22) 19.479 ms 20.058 ms 19.550 ms 8 209.85.241.29 (209.85.241.29) 20.547 ms 19.761 ms 209.85.241.27 (209.85.241.27) 20.131 ms 9 209.85.240.49 (209.85.240.49) 30.184 ms 72.14.239.189 (72.14.239.189) 21.337 ms 21.756 ms 10 iw-in-f99.google.com (74.125.95.99) 19.793 ms 19.665 ms 20.603 ms

L'uscita mostra che ci sono voluti 10 salti per arrivare lì, e la latenza generalmente aumentat con ogni luppolo, che si prevede.

Nota: Quando si utilizza la politica del routing, come con Multi-WAN, il firewall stesso potrebbe non apparire come un salto nel traceroute. Quando viene utilizzata la politia di routing, f4l non decrementa il TTL durante l'inoltro dei pacchetti, quindi traceroute non può rilevarlo come router intermedio.

14.7.3 Rotte e VPN

A seconda della VPN utilizzata, una rotta potrebbe non essere visualizzata nella tabella per il lato lontano. IPsec non usa la tabella di routing, è invece gestito internamente nel kernel usando le voci del database della politica della sicurezza di IPsec (SPD). Le rotte statiche non faranno mai in modo che il traffico sia diretto attraverso una connessione IPsec. OpenVPN utilizza la tabella di routing di sistema e come tali voci sono presenti per le reti raggiungibili tramite un tunnel OpenVPN, come nel seguente esempio:

```
#netstat -rWn
```

Routing tables Internet: Destination Gateway Flags Use Mtu Netif Expire default 198.51.100.1 UGS 92421 1500 em0 10.6.0.0/16 10.6.203.1 UGS 0 1500 ovpnc2 10.6.203.0/24 10.6.203.2 UGS 0 1500 ovpnc2 10.6.203.1 link#9 UH 0 1500 ovpnc2 10.6.203.2 link#9 UHS 0 16384 lo0 10.7.0.0/24 link#2 U 1260771 1500 em1 10.7.0.1 link#2 UHS 0 16384 lo0 127.0.0.1 link#7 UH 866 16384 lo0 198.51.100.0/24 link#1 U 1251477 1500 em0 198.51.100.7 link#1 UHS 0 16384 lo0

L'interfaccia OpenVPN è 10.6.203.2, con un gateway di 10.6.203.1 e l'interfaccia è ovpnc2. La rete raggiungibile che utilizza OpenVPN in questo esempio è 10.6.0.0/16.

Con IPsec, traceroute non è così utile come con configurazioni routing come OpenVPN, perché il tunnel IPsec per sé non ha gli indirizzi IP. Durante l'esecuzione di traceroute verso una destinazione attraverso IPsec, una scadenza verrà mostrata per il salto che è il tunnel IPsec.

Una delle funzioni principali di un firewall è l'instradamento del traffico. Questo capitolo tratta diversi argomenti relativi all'instradamento, inclusi gateway, percorsi statici, protocolli di instradamento, instradamento di indirizzi IP pubblici e visualizzazione di informazioni sul routing.

CAPITOLO 15

Bridging

Creare un bridge (bridge)

In Firew4LL, i bridge vengono aggiunti e rimossi in **Interfacce>(assegna)** nella scheda **bridge**. Utilizzando i bridge, un numero illimitato di porte può essere facilmente unito. Ogni bridge creato nella GUI creerà anche una nuova interfaccia bridge nel sistema operativo, denominata bridgex dove X inizia a 0 e aumenta di un0 per ogni nuovo bridge. Queste interfacce possono essere assegnate e utilizzate come la maggior parte delle altre interfacce, che vengono discusse più avanti in questo capitolo.

Per creare un bridge:

- Passare a **Interfacce>(assegnare)** nella scheda **bridge**.
- Fare clic su **Aggiungere** per creare un nuovo bridge.
- Seleziona almeno una voce da **Interfacce dei membri**. Selezionare quante ne servono usando Ctrl-click.
- Aggiungere una **descrizione** se desiderato.
- Fare clic su **Mostrare opzioni avanzate** per rivedere i parametri di configurazione rimanenti come necessario. Per la maggior parte dei casi non sono necessari.
- Fare clic su **Salvare** per completare il bridge.

Nota: Un bridge può consistere in un'unica interfaccia membro, che può aiutare a migrare in una configurazione con un bridge assegnato, o per fare una semplice porta span/mirror.

15.1 Opzioni avanzate del bridge

Ci sono numerose opzioni avanzate per un bridge e i suoi membri. Alcune di queste impostazioni sono abbastanza coinvolte, quindi vengono discusse singolarmente in questa sezione.

15.1.1 Spanning Tree Options (Rapido)

L'albero di spanning (spanning tree) è un protocollo che aiuta switch e dispositivi a determinare se c'è un ciclo (loop) e a tagliarlo come necessario per evitare che il ciclo danneggi la rete. Ci sono parecchie opzioni che controllano il comportamento dello spanning tree che permettono di fare certe ipotesi su porte specifiche o di garantire che alcuni bridge abbiano la priorità nel caso di un ciclo o di collegamenti ridondanti. Maggiori informazioni su STP possono essere trovate nella pagina principale di FreeBSD ifconfig(8), e su Wikipedia.

Protocollo

L'impostazione del **protocollo** stabilisce se il bridge utilizzerà il protocollo dello Spanning Tree (*STP*) dell'ID o il protocollo dello Spanning Tree rapido (*RSTP*) IEEE 802.1w. RSTP è un protocollo più recente, e come il nome suggerisce opera molto più veloce di STP, ma è retrocompatibile. Il nuovo standard IEEE 802.1D-2004 è basato su RSTP e rende STP obsoleto.

Selezionare STP solo quando è in uso una vecchia versione che non si comporta bene con RSTP.

Interfacce STP

L'elenco delle **interfacce STP** riflette i membri del bridge su cui è abilitato STP. Utilizzare Ctrl-click per selezionare i membri del bridge da utilizzare con STP.

Tempo di validità

Impostare il **tempo di validità** per una configurazione del protocollo dell'albero di spanning. Il valore predefinito è 20 secondi. Il minimo è 6 secondi e il massimo è 40 secondi.

Tempo di forward

L'opzione **Tempo di forward** imposta il tempo che deve passare prima che un'interfaccia inizi a inoltrare i pacchetti quando l'albero di spanning è abilitato. Il valore predefinito è 15 secondi. Il minimo è 4 secondi e il massimo è 30 secondi.

Nota: Un ritardo più lungo sarà notato dai client direttamente connessi in quanto non saranno in grado di passare il traffico, anche per ottenere un indirizzo IP tramite DHCP, fino a quando la loro interfaccia entra in modalità di inoltro.

Hello Time

L'opzione **Hello Time** imposta il tempo tra la trasmissione dei messaggi di configurazione del protocollo di Spanning Tree. Il **hello time** può essere modificato solo quando si opera in modalità STP. Il valore predefinito è 2 secondi. Il minimo è 1 secondo e il massimo è 2 secondi.

Priorità del bridge

La **priorità del bridge** dell'albero di Spanning controlla se questo bridge sarà selezionato per primo per il blocco in caso di rilevamento di un ciclo. Il valore predefinito è 32768. Il minimo è 0 e il massimo è 61440. I valori devono essere un multiplo di 4096. Priorità inferiori hanno la precedenza, e valori inferiori a 32768 indicano l'ammissibilità per diventare un bridge di root.

Tenere il conto (Hold count)

La trasmissione **Hold Count** per l'albero di spanning è il numero di pacchetti trasmessi prima di vare un tasso limitato. Il valore predefinito è 6. Il minimo è 1 e il massimo è 10.

Priorità delle porte

I campi **Priorità** definiscono la priorità dell'albero di spanning per ogni interfaccia membro del bridge. Alle priorità più basse viene data preferenza quando si decide quali porte bloccare e quali inoltrare. La priorità predefinita è 128, e deve essere compresa tra 0 e 240.

Path Costs

I campi **Path Costs** impostano il path costs dell'albero di spanning per ogni membro del bridge. Il valore predefinito è calcolato dalla velocità del collegamento. Per cambiare un path costs precedentemente selezionato indietro all'automatico, impostare il costo a 0. Il minimo è 1 e il massimo è 200000000. I path costs più bassi sono preferiti quando si prende una decisione su quali porte bloccare e quali lasciare come forward.

15.1.2 Impostazioni della cache

La **dimensione della cache** imposta la dimensione massima della cache dell'indirizzo del bridge, simile alla tabella MAC o CAM di uno switch. Il valore predefinito è 100 voci. Se ci sarà un gran numero di dispositivi che comunicano attraverso il bridge, impostarlo come più alto.

Tempo di scadenza della voce della cache controlla il timeout delle voci della cache dell'indirizzo in secondi. Se impostata su 0, le voci della cache dell'indirizzo non saranno scadute. Il valore predefinito è 240 secondi (quattro minuti)

15.1.3 Porta Span

Selezionando un'interfaccia come **porta Span** sul bridge trasmetteremo una copia di ogni fotogramma ricevuto dal bridge all'interfaccia selezionata. Questo è molto utile per lo snooping di una rete bridge passivamente su un altro host collegato alle porte span del bridge con qualcosa come Snort, tcpdump, ecc. La porta span selezionata potrebbe non essere una porta membro sul bridge.

15.1.4 Porte di EDGE/Porte automatiche di edge

Se un'interfaccia è impostata come una **porta Edge**, si presume sempre che sia collegata ad un dispositivo di fine, e mai ad uno switch; si assume che la porta non possa mai creare un loop di livello 2. Impostare questo solo su una porta quando non sarà mai collegato a un altro switch. Le porte di default rilevano automaticamente lo stato edge, e possono essere selezionate sotto le porte di **edge automatico** per *disabilitare* questo comportamento automatico di rilevamento edge.

15.1.5 Porte PTP/porte automatico PTP

Se un'interfaccia è impostata come **porta PTP**, si presume sempre che sia collegata ad uno switch, e non ad un dispositivo utente finale; si presume che la porta possa potenzialmente creare un loop di livello 2. Dovrebbe essere abilitato solo sulle porte collegate ad altri switch abilitati RSTP. Le porte di default rilevano automaticamente lo stato PTP, e possono essere selezionate sotto le **porte PTP** automatiche per *disabilitare* questo comportamento automatico di rilevamento PTP.

15.1.6 Porte Sticky

Un'interfaccia selezionata in **porte Sticky** avrà i suoi indirizzi dinamicamente imparati memorizzati come se fossero statici una volta che entrano nella cache. Le voci sticky non vengono mai rimosse dalla cache degli indirizzi, anche se appaiono su un'interfaccia diversa. Questo potrebbe essere utilizzato come una misura di sicurezza per garantire che i dispositivi non possano muoversi tra le porte arbitrariamente.

15.1.7 Porte private

Un'interfaccia contrassegnata come una **porta privata** non comunica con qualsiasi altra porta contrassegnata come una **porta privata**. Questo può essere usato per isolare gli utenti finali o sezioni di una rete tra loro se sono collegati alle porte di bridge separati contrassegnate in questo modo. Funziona in modo analogo alle "VLAN private" o all'isolamento dei client su un punto di accesso wireless.

15.2 Bridging e interfacce

Un'interfaccia di bridge (ad es. *bridge0*) può essere assegnata come interfaccia. Questo permette al bridge di agire come un'interfaccia normale e avere un indirizzo IP posto su di esso piuttosto che un'interfaccia membro.

La configurazione dell'indirizzo IP sul bridge stesso è la migliore in quasi tutti i casi. La ragione principale è dovuta al fatto che i bridge dipendono dallo stato dell'interfaccia su cui è assegnato l'indirizzo IP. Se l'indirizzo IP del bridge è configurato su un'interfaccia membro e l'interfaccia è disattivata, l'intero bridge sarà disattivato e non passerà più il traffico. Il caso più comune per questo è un'interfaccia wireless collegata a un NIC della LAN Ethernet. Se il NIC LAN è scollegato, il wireless sarebbe morto a meno che l'indirizzo IP sia stato configurato sull'interfaccia bridge e non LAN. Un'altra ragione è che se i limitatori devono essere usati per controllare il traffico, allora ci deve essere un indirizzo IP sull'interfaccia del bridge per farli funzionare correttamente. Allo stesso modo, affinché il portale Captive o un proxy trasparente funzioni su un bridge interno, l'indirizzo IP deve essere configurato sul bridge assegnato e non su un'interfaccia membro.

15.2.1 Scambiare le assegnazioni dell'interfaccia

Prima di spingersi troppo oltre nel parlare di scambi delle assegnazioni di interfaccia bridge, si deve notare che queste modifiche dovrebbero essere fatte da una porta che non è coinvolta nel bridge. Ad esempio, se si collega WLAN a LAN, effettuare la modifica da WAN o da un'altra porta OPT. In alternativa, scaricare un backup di config.xml e manualmente apportare le modifiche. Il tentativo di apportare modifiche ad una porta durante la gestione del firewall da quella porta molto probabilmente comporterà la perdita di accesso alla GUI, lasciando il firewall irraggiungibile.

Metodo semplice: spostare le impostazioni alla nuova interfaccia

Il percorso più semplice, anche se non il più veloce, nella GUI è quello di rimuovere le impostazioni dall'interfaccia LAN individualmente (indirizzo IP, DHCP, ecc) e quindi attivarle sull'interfaccia bridge appena assegnata.

Metodo rapido ma complicato: riassegnare il bridge come LAN

Anche se questo metodo è un po" più complicato che spostare le impostazioni, può essere molto più veloce soprattutto nei casi in cui ci iano un sacco di regole firewall su LAN o una complessa configurazione DHCP. In questo metodo, è richiesto un po" di hoop-jumping, ma alla fine il bridge finisce come interfaccia LAN, e mantiene l'indirizzo IP della LAN, tutte le regole del precedente firewall, DHCP, e altre configurazioni di interfaccia.

- Assegnare e configurare i membri del bridge che non sono stati ancora gestiti. Riesaminare le fasi che seguono per garantire che le impostazioni dell'interfaccia siano corrette anche se le interfacce sono già state assegnate e configurate.
  - Passare a **Interfacce>(assegnare)**
  - Scegliere l'interfaccia dall'elenco delle **porte di rete disponibili**
  - Fare clic su **Aggiungere**
  - Passare alla nuova pagina di configurazione dell'interfaccia, ad es. **Interfacce>OPT2**
  - Selezionare **Abilitare**
  - Inserire una **descrizione** come WiredLAN2
  - Impostare sia il **tipo di configurazione IPv4** sia il **tipo di configurazione IPv6** su *Nessuno*
  - Deselezionare il **Blocco delle reti private** e il **Blocco delle reti bogon** se selezionate
  - Fare clic su **Salvare**
  - Fare clic su **Applicare modifiche**
  - Ripetere la procedura per ulteriori futuri membri del bridge non assegnati
- Creare il nuovo bridge
  - Passare a **Interfacce>(assegnare)** nella scheda **bridge**
  - Fare clic su **Aggiungere** per creare un nuovo bridge
  - Inserire una **descrizione**, ad esempio bridge LAN
  - Selezionare tutti i nuovi membri del bridge **ECCETTO**l'interfaccia LAN nell'elenco delle **interfacce membri**
  - Fare clic su **Salvare**
- Modificare il **regolabile di sistema** del filtraggio del bridge per disabilitare il filtro dell'interfaccia membro
  - Passare a **Sistema>Avanzate**, scheda **Regolabili di sistema**
  - Individuare la voce per **net.link.bridge.pfil_member** o creare una nuova voce se non esiste, utilizzando tale nome per il **sintonizzabile**
  - Fare clic su  per modificare una voce esistente
  - Digitare 0 nel campo **Valore**
  - Fare clic su **Salvare**
- Passare a **Interfacce>(assegnare)**
- Cambiare l'assegnazione della **LAN** a bridge0
- Fare clic su **Salvare**
- Assegnare e configurare la vecchia interfaccia LAN come descritto in precedenza, impostando i tipi di configurazione IP su *Nessuno* e nominandola WiredLAN
- Modificare il bridge e selezionare il nuovo WiredLAN assegnato come membro del bridge
- Modificare il **sintonizzabile di sistema** del filtraggio del bridge per abilitare il filtraggio dell'interfaccia bridge
  - Usare la procedura descritta in precedenza, ma impostare net.link.bridge.pfil_bridge su 1

Ora l'interfaccia LAN precedente, insieme con i nuovi membri bridge, sono tutti su un livello 2 comune con il bridge assegnato come LAN insieme con l'altra configurazione.

Metodo più veloce ma più difficile: Modifica config.xml manualmente

La modifica manuale config.xml può essere molto veloce per chi ha familiarità con il formato di configurazione in XML. Questo metodo è facile da sbagliare, tuttavia, in modo da essere sicuri bisogna avere un backup e installare i media nelle vicinanze nel caso in cui sia fatto un errore.

Quando si modifica a mano config.xml per eseguire questa operazione, fare come segue:

- Assegnare i membri aggiuntivi del bridge e impostare i loro tipi di configurazione IP su *Nessuno*
- Creare il bridge, compresi *LAN* e *LAN2* e altri membri del bridge
- Assegnare il bridge (ad es. come OPT2) e abilitarlo, anche con un tipo di configurazione IP come *Nessuno*
- Scaricare un backup di config.xml da **Diagnostica>Backup/Ripristino**
- Aprire config.xml in un editor di testo che comprende la fine della riga di UNIX
- Cambiare l'assegnazione *LAN* a bridge0
- Modificare l'assegnazione *LAN* precedente a quello che era il bridge (ad es. *OPT2*)
- Modificare la definizione del bridge per riferirsi all'*OPT2* e non alla *LAN*
- Salvare le modifiche
- Ripristinare config.xml modificato da **Diagnostica>Backup/Ripristino**

Il firewall si riavvierà con l'impostazione desiderata. Monitorare la console per garantire che le impostazioni sono state applicate correttamente e non si verificano errori durante la sequenza di avvio.

15.2.2 MAC assegnato agli indirizzo dei bridge e Windows

L'indirizzo MAC per un bridge è determinato casualmente quando il bridge viene creato, sia al momento dell'avvio o quando viene creato un nuovo bridge. Ciò significa che ad ogni riavvio, l'indirizzo MAC può cambiare. In molti casi questo non importa, ma Windows Vista, 7, 8, e 10 utilizzano l'indirizzo MAC del gateway per determinare se sono su una rete specifica. Se il MAC cambia, l'identità di rete cambierà e il suo status come pubblico, privato, ecc. potrebbe dover essere corretto. Per aggirare questo problema, immettete un indirizzo MAC sull'interfaccia bridge assegnata per effettuare lo spoof. Quindi i client vedranno sempre lo stesso MAC per l'indirizzo IP del gateway.

15.3 Bridging e firewall

Il filtraggio con interfacce bridge funziona in modo simile alle interfacce instradate, ma ci sono alcune scelte di configurazione per modificare esattamente il comportamento del filtraggio. Per impostazione predefinita, le regole del firewall sono applicate su ogni interfaccia membro del bridge sulla base dell'entrata, come qualsiasi altra interfaccia instradata.

È possibile decidere se il filtraggio avviene sulle interfacce degli elementi del bridge o sull'interfaccia del bridge stesso. Questo è controllato da due valori in **Sistema>Avanzate** nella scheda **Regolazioni di sistema**, come visto della figura *Filtri bridge regolabili*. Il net.link.bridge.pfil_member controlla se le regole saranno rispettate o meno sulle interfacce dei membri del bridge. Di default, questo è su attivo come (1). Il sintonizzabile **net.link.bridge.pfil_bridge** controlla se le regole saranno rispettate sull'interfaccia del bridge stesso. Di default, questo è spento come (0). Almeno uno di questi valori deve essere impostato su 1.

net.link.bridge.pfil_member	Packet filter on the member interface	1	
net.link.bridge.pfil_bridge	Packet filter on the bridge interface	0	

Fig. 1: Filtri bridge regolabili

Quando si filtra sull'interfaccia bridge stessa, il traffico colpirà le regole appena entra in qualsiasi interfaccia membro. Le regole sono ancora considerate "in entrata" come tutte le altre regole di interfaccia, ma funzionano più come un gruppo di interfaccia poiché le stesse regole si applicano ad ogni interfaccia membro.

15.3.1 Macro delle regole del firewall

Solo un'interfaccia bridge avrà un indirizzo IP impostato, le altre non ne avranno. Per queste interfacce, le loro macro del firewall come l'*indirizzo OPT1* e la *rete OPT1* sono indefinite perché l'interfaccia non ha nessun indirizzo e quindi nessuna sottorete.

Se il filtraggio viene eseguito sui membri del bridge, tenere presente questo fatto durante la creazione di regole ed elencare esplicitamente la sottorete o utilizzare le macro per l'interfaccia in cui risiede l'indirizzo IP.

15.4 Bridging di due reti interne

Quando si collegano due reti interne come descritto in *bridge interni* ci sono alcune considerazioni speciali da prendere per alcuni servizi sul firewall.

Nota: Ci sono ulteriori requisiti e restrizioni quando si collegano le interfacce wireless perché la via 802.11 funzioni. Vedere *Bridging e wireless* per maggiori informazioni.

15.4.1 DHCP e bridge interni

Quando si collega una rete interna ad un'altra, si devono fare due cose. In primo luogo, assicurarsi che il DHCP sia in esecuzione solo sull'interfaccia contenente l'indirizzo IP e non i membri del bridge senza un indirizzo. In secondo luogo, una regola firewall aggiuntiva può essere necessaria in cima alle regole sulle interfacce membro per consentire il traffico DHCP.

Nota: Questo vale solo per il filtraggio effettuato sulle interfacce dei membri, non per il filtraggio eseguito sul bridge.

Quando si crea una regola per consentire il traffico su un'interfaccia, normalmente la sorgente è specificata in modo simile alla *sottorete OPT1* in modo che solo il traffico da quella sottorete sia consentito fuori da quel segmento. Con DHCP, questo non è sufficiente. Poiché un client non ha ancora un indirizzo IP, una richiesta DHCP viene eseguita come una trasmissione. Per soddisfare queste richieste, creare una regola sulle interfacce degli elementi del bridge con le seguenti impostazioni:

- Passare a **Firewall>Regole** nella scheda per il membro del bridge
- Fare clic su  **Aggiungere** per aggiungere una nuova regola in cima all'elenco
- **Protocollo:** *UDP*
- **Fonte:** 0.0.0.0
- **Porta sorgente:** 68
- **Destinazione:** 255.255.255.255
- **Porta di destinazione:** 67
- **Descrizione** che indica permettere DHCP

- Fare clic su **Salvare** e **applicare modifiche**

La regola apparirà come nella figura *Regola del firewall per consentire DHCP*.

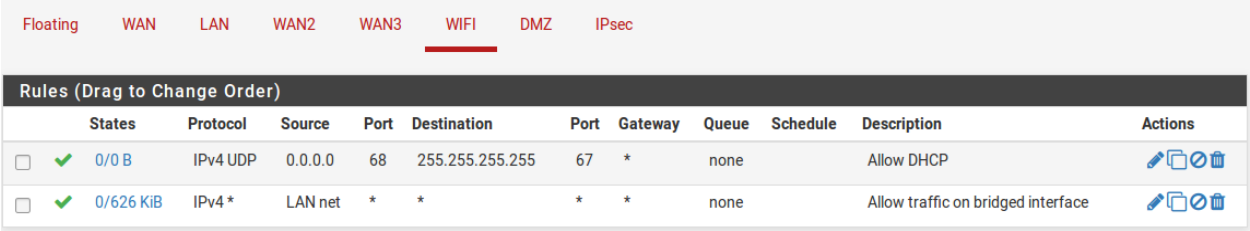


Fig. 2: Regola del firewall per consentire DHCP

Dopo aver aggiunto la regola, i client nel segmento del bridge saranno in grado di effettuare con successo richieste al demone DHCP in ascolto sull'interfaccia a cui è collegato.

Dhcpv6 è un po" più complicato da permettere poiché comunica da e verso gli indirizzi Ipv6 locali e multicast. Vedere la figura Regola del firewall per consentire sia DHCP che Dhcpv6 per l'elenco delle regole richieste. Questi possono essere semplificati con alias in una o due regole contenenti la rete di sorgente corretta, la rete di destinazione e le porte.

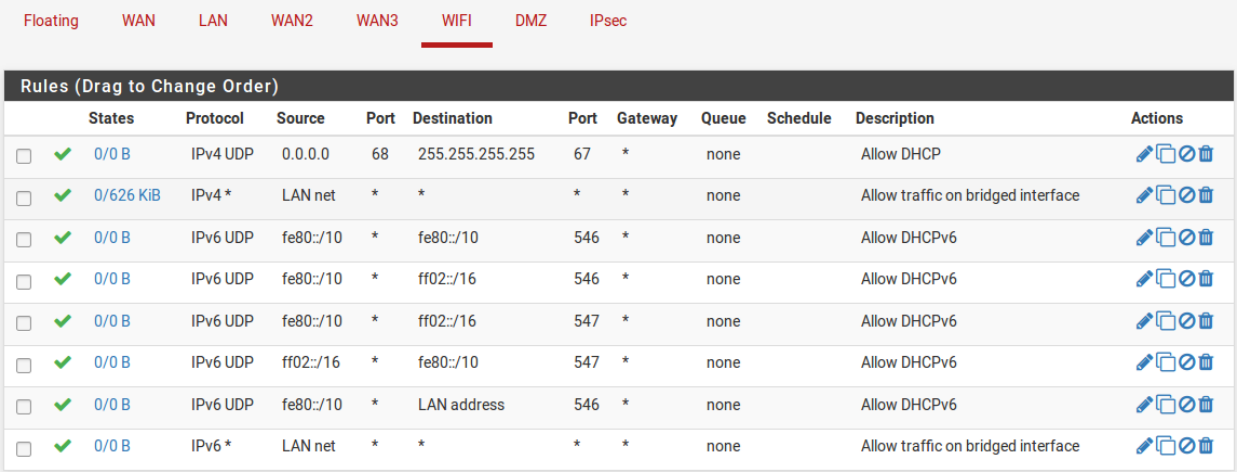


Fig. 3: Regola del firewall per consentire sia DHCP che Dhcpv6

15.5 Interoperabilità della creazione del bridge

Le interfacce bridge sono diverse dalle normali interfacce per alcuni aspetti, quindi ci sono alcune caratteristiche che sono incompatibile con il bridging, e altre in cui devono essere fatte considerazioni aggiuntive per accogliere il bridging. Questa sezione copre funzionalità che funzionano in modo diverso con il bridge rispetto alle interfacce senza bridge.

15.5.1 Il captive portal

Il captive portal (*Captive Portal*) non è compatibile con il bridging trasparente perché richiede un IP sull'interfaccia per il bridge, utilizzato per servire i contenuti del portale, e quell'IP deve essere il gateway per i client. Ciò significa che non è possibile, ad esempio, collegare LAN e WAN e sperare di catturare i client con il portale.

Questo può funzionare quando si collegano più interfacce *locali* a tutti i percorsi attraverso Firew4LL (ad es. LAN1, LAN2, LAN3, ecc.). Funzionerà se l'interfaccia bridge è assegnata, l'interfaccia bridge ha un indirizzo IP e quel-

l'indirizzo IP è usato come gateway dai client sul bridge. Vedere *Assegnazioni dell'interfaccia da scambiare* per la procedura per posizionare l'indirizzo IP su un'interfaccia bridge assegnata.

15.5.2 HA - Elevata disponibilità

L" HA (*elevata disponibilità*) non è raccomandata con il bridging in questo momento. Alcuni hanno avuto successo con la combinazione dei due in passato, ma bisogna fare molta attenzione a gestire i loop di livello 2, che sono inevitabili in uno scenario HA+bridge. Quando due segmenti di rete sono collegati con un bridge, sono in effetti fusi in una rete più grande, come discusso in precedenza in questo capitolo. Quando HA viene aggiunto nel mix, ciò significa che ci saranno due percorsi tra gli switch per ogni rispettiva interfaccia, creando un loop.

Gli switch gestiti possono gestire questo con il protocollo dell'albero di Spanning (STP), ma gli switch non gestiti non hanno difese contro la creazione di loop. Lasciato libero, un loop metterà in ginocchio una rete e renderà impossibile far passare qualsiasi traffico. STP può essere configurato sui bridge per aiutare, anche se ci possono ancora essere risultati imprevisti.

15.5.3 Multi-WAN

Il bridging trasparente per sua natura è incompatibile con il multi-WAN in molti dei suoi usi. Quando si utilizza un bridge tra una WAN e un'interfaccia LAN/OPT, di solito qualcosa di diverso da Firew4LL sarà il gateway predefinito per gli host sull'interfaccia per il bridge, e quel router è l'unico dispositivo che può dirigere il traffico da quegli host. Questo non impedisce che il multi-WAN venga utilizzato con altre interfacce sullo stesso firewall che non sono integrate, ma influisce solo sugli host sulle interfacce bridge dove usano qualcosa di diverso da Firew4LL come gateway predefinito. Se più interfacce interne sono unite insieme e Firew4LL è il gateway predefinito per gli host sulle interfacce del bridge, allora si può usare multi-WAN come con le interfacce senza bridge.

15.5.4 Limitatori

Affinché i limitatori funzionino con il bridging, il bridge stesso deve essere assegnato e l'interfaccia bridge deve avere l'indirizzo IP e non un'interfaccia membro.

15.5.5 NAT nella LAN e Proxy Trasparente

Per le porte forward sulla LAN, o proxy trasparenti che utilizzano porte forward sulla LAN per catturare il traffico, per funzionare in uno scenario bridge, la situazione è la stessa del captive portal: funzionerà solo per bridge LAN e non bridge WAN/LAN, l'indirizzo IP deve trovarsi sull'interfaccia bridge assegnata e tale indirizzo IP deve essere utilizzato come gateway per i client locali.

Ciò significa che un pacchetto come Squid non può funzionare in uno scenario di firewall trasparente dove la LAN è collegata a una WAN.

Normalmente ogni interfaccia su Firew4LL rappresenta il proprio dominio broadcast con una sottorete IP unica. In alcune circostanze è auspicabile o necessario combinare più interfacce su un singolo dominio di trasmissione, dove due porte sul firewall agiranno come se fossero sullo stesso switch, ad eccezione del traffico tra le interfacce che può essere controllato con le regole del firewall. In genere questo viene fatto in modo che più interfacce agiscano come se fossero sulla stessa rete piatta utilizzando la stessa sottorete IP e in modo che tutti i client condividano il traffico broadcast e multicast.

Alcune applicazioni e dispositivi si basano su trasmissioni per funzionare, ma questi si trovano più comunemente in ambienti domestici che ambienti aziendali. Per una discussione pratica, vedere *Bridging e wireless*.

Per i servizi in esecuzione sul firewall, il bridging può essere problematico. Caratteristiche come i limitatori, il captive portal e i proxy trasparenti richiedono una configurazione e una gestione speciali per lavorare su reti a bridge. In particolare, il bridge stesso deve essere assegnato e l'unica interfaccia sul bridge con un indirizzo IP deve essere il bridge assegnato. Inoltre, affinché queste funzioni funzionino, l'indirizzo IP sul bridge deve essere l'indirizzo utilizzato dai client come gateway. Questi temi sono discussi in modo più approfondito nel l'ambito del l'*interoperabilità della creazione del bridge*.

15.6 Tipi di bridge

Esistono due tipi distinti di bridge: bridge interni e bridge interni/esterni. I bridge interni collegano due interfacce locali come due interfacce LAN o un'interfaccia LAN e un'interfaccia wireless. I bridge interni/esterni collegano una LAN ad una WAN dando luogo a quello che viene comunemente chiamato un firewall trasparente..

15.6.1 Bridge Interni

Con un bridge di tipo interno, le porte sul firewall sono collegate in modo tale da comportarsi in modo simile alle porte switch, anche se con la possibilità di filtrare il traffico sulle porte o sul bridge e con prestazioni molto più basse di uno switch. Il firewall stesso è ancora visibile ai client collegati locali e agisce come gateway, e forse DNS e server DHCP. I client sui segmenti bridge potrebbero anche non sapere che c'è un firewall tra di loro.

Questo tipo di configurazione è comunemente scelto dagli amministratori per isolare e controllare una parte della rete, come un segmento wireless, o per utilizzare porte aggiuntive sul firewall al posto di uno switch corretto in cui l'installazione di uno switch sarebbe impraticabile. Anche se non è raccomandato, questo tipo di bridge può essere utilizzato anche per unire due reti remote su alcuni tipi di connessioni VPN.

Per ulteriori informazioni, è possibile accedere all'archivio degli Hangouts per visualizzare l'hangout di Maggio 2015 sui punti di accesso wireless che comprendeva esempi pratici di bridge di tipo interno.

15.6.2 Bridge Interni/Esterni

Un bridge di tipo Interno/Esterno, noto anche come firewall trasparente «, viene utilizzato per inserire un firewall tra due segmenti senza alterare gli altri dispositivi. Più comunemente questo viene usato per collegare una WAN a una rete interna in modo che la sottorete WAN possa essere usata «all'interno del firewall o internamente tra segmenti locali come filtro in linea. Un altro uso comune è per i dispositivi dietro il firewall per ottenere indirizzi IP tramite DHCP da un server upstream sulla WAN.

In una configurazione firewall trasparente il firewall non riceve il traffico direttamente o agisce come un gateway, si limita a ispezionare il traffico come passa attraverso il firewall.

Nota: I dispositivi sul lato interno di questo bridge devono continuare ad usare il gateway upstream come proprio gateway. Non impostare alcun indirizzo IP sul firewall come gateway per i dispositivi su un bridge trasparente.

Il NAT non è possibile con questo stile di bridge perché il NAT richiede che il traffico sia indirizzato direttamente all'indirizzo MAC del firewall per avere effetto. Dal momento che il firewall non è il gateway, questo non accade. In quanto tali, le regole per catturare il traffico come quelle utilizzate da un proxy trasparente non funzionano.

15.7 Bridging e loop di Livello 2

Quando si effettua il bridging, occorre evitare i loop di livello 2, oppure deve essere presente una configurazione di switch che gestisca i loop. Un loop di livello 2 si ha quando, direttamente o indirettamente, lo switch ha una

connessione a se stesso. Se un firewall che esegue Firew4LL ha interfacce unite insieme, e due interfacce sono collegate nello stesso switch sulla stessa VLAN, è stato creato un loop di livello 2. Il collegamento di due cavi di connessione tra due switch fa anche questo.

Gli switch gestiti utilizzano il protocollo dell'albero di spanning (STP) per gestire situazioni come questa, perché è spesso desiderabile avere collegamenti multipli tra gli switch, e la rete non dovrebbe essere esposta a una fusione completa da parte di qualcuno che collega una porta di rete a un'altra porta di rete. STP non è abilitato per default su tutti gli switch gestiti, e non è quasi mai disponibile con gli switch non gestiti. Senza STP, il risultato di un loop di livello 2 è che i frame sulla rete circoleranno all'infinito e la rete cesserà completamente di funzionare finché il loop non verrà rimosso. Controllare la configurazione dello switch per garantire che la funzione sia abilitata e configurata correttamente.

Firew4LL abilita STP sulle interfacce bridge per aiutare con i loop, ma può ancora portare a situazioni impreviste. Ad esempio, una delle porte bridge si spegne per fermare il loop, ciò potrebbe causare che il traffico smetta di fluire inaspettatamente o bypassi il firewall del tutto.

In poche parole, il bridging ha il potenziale per fondere completamente la rete a meno che chiunque colleghi i dispositivi nello switch non sia attento.

CAPITOLO 16

VLAN (LAN Virtuale)

16.1 Terminologia

Questa sezione definisce la terminologia necessaria per implementare correttamente le VLAN.

Tronco (Trunking) Trunking si riferisce a un mezzo di trasporto di più VLAN sulla stessa porta switch fisica. I frame che escono da una porta trunk sono contrassegnati con un contrassegno (tag) 802.1Q nell'intestazione, consentendo al dispositivo collegato di distinguere tra più VLAN. Le porte trunk sono utilizzate per collegare più switch e per collegare qualsiasi dispositivo in grado di contrassegnare come 802.1Q e richiedono l'accesso a più VLAN. Questo è comunemente limitato al firewall o al router che forniscono connettività tra le VLAN, in questo caso, Firew4LL, così come a qualsiasi connessione ad altri switch contenenti più VLAN.

ID delle VLAN Ogni VLAN ha un numero identificativo (ID) per distinguere il traffico contrassegnato. Questo è un numero tra *1* e *4094*. La VLAN predefinita sugli switch è la VLAN *1*, e questa VLAN non deve essere utilizzata quando si distribuisce il trunking delle VLAN. Questo è discusso ulteriormente in *Vlan e sicurezza*. A parte evitare l'uso di VLAN 1, i numeri delle VLAN possono essere scelti a piacimento. Alcuni progetti iniziano con VLAN 2 e si incrementano di uno fino a raggiungere il numero richiesto di VLAN. Un altro disegno comune è quello di utilizzare il terzo ottetto nella sottorete della VLAN come ID della VLAN. Ad esempio, se si usano 10.0.10.0/24, 10.0.20.0/24 e 10.0.30.0/24, è logico usare le VLAN 10, 20 e 30 rispettivamente. Scegliere uno schema di assegnazione ID della VLAN che abbia senso per un determinato progetto di rete.

Interfaccia principale L'interfaccia fisica in cui risiede una VLAN è nota come interfaccia principale. Ad esempio, *igb0* o *em0*. Quando le VLAN sono configurate su Firew4LL, ad ognuna viene assegnata un'interfaccia virtuale. Il nome dell'interfaccia virtuale è creato combinando il nome dell'interfaccia principale più l'ID della VLAN. Ad esempio, per VLAN 20 su *igb0*, il nome dell'interfaccia è igb0_vlan20.

Nota:

L'unica funzione dell'interfaccia principale è, idealmente, quella di essere il genitore per le VLAN definite e non essere utilizzata direttamente. In alcune situazioni questo funzionerà, ma può causare difficoltà con la configurazione dello switch, e richiede l'uso della VLAN predefinita sulla porta del trunk, che è meglio evitare come discusso ulteriormente in *Vlan e Sicurezza*.

Porta di accesso Una porta di accesso si riferisce a una porta switch che fornisce l'accesso a una singola VLAN, dove i frame non sono contrassegnati con un'intestazione 802.1Q. I normali dispositivi di tipo client sono collegati alle porte di accesso, I quali comprenderanno la maggior parte delle porte switch. I dispositivi sulle porte di accesso non hanno bisogno di conoscere le VLAN o I contrassegni. Vedono la rete sulla loro porta come farebbe uno switch senza VLAN.

Doppi contrassegni (Qinq) *Qinq* si riferisce ai doppi tag del traffico, utilizzando sia un tag 802.1Q esterno sia interno. Questo può essere utile in ambienti ISP di grandi dimensioni, con altre reti molto grandi, o reti che devono trasportare più VLAN attraverso un link che supporta solo un singolo tag della VLAN. È possibile anche il triplo contrassegno. Firew4LL supporta Qinq, anche se non è una caratteristica molto comune. Questi tipi di ambienti hanno generalmente bisogno del tipo di alimentazione del routing che solo un router ASIC di fascia alta può supportare, e Qinq aggiunge un livello di complessità che non è necessario nella maggior parte degli ambienti. Per ulteriori informazioni sulla configurazione di Qinq su Firew4LL, vedere *Configurazione di Qinq su |firew4ll|*.

VLAN privata (PVLAN) PVLAN, talvolta chiamato **Isolamento della porta**, si riferisce alle funzionalità di alcuni switch per segmentare gli host all'interno di una singola VLAN. Normalmente gli host all'interno di una singola funzione VLAN sono gli stessi degli host su un singolo switch senza VLAN configurato. PVLAN fornisce un mezzo per impedire agli host di una VLAN di comunicare con qualsiasi altro host su tale VLAN, consentendo solo la comunicazione tra tale host e il suo gateway predefinito. Questo non è direttamente rilevante per Firew4LL, ma è una domanda comune. Cambiare funzionalità come questa è l'unico modo per impedire la comunicazione tra host nella stessa sottorete. Senza una funzione come PVLAN, nessun firewall di rete può controllare il traffico all'interno di una sottorete perché non tocca mai il gateway predefinito.

16.2 VLAN e Sicurezza

Le VLAN sono un ottimo modo per segmentare una rete e isolare le sottoreti, ma ci sono problemi di sicurezza che devono essere presi in considerazione quando si progetta e si implementa una soluzione che coinvolge le VLAN. Le Vlan non sono intrinsecamente insicure, ma un'errata configurazione può rendere vulnerabile una rete. Ci sono stati anche problemi di sicurezza in passato con le implementazione dei venditori dello switch delle VLAN.

16.2.1 Segregare le zone di fiducia (Trust)

A causa della possibilità di errori di configurazione, le reti di livelli di fiducia notevolmente diversi dovrebbero essere su switch fisici separati. Ad esempio, mentre lo stesso switch potrebbe essere tecnicamente utilizzato con le VLAN per tutte le reti interne e la rete al di fuori dei firewall, ciò dovrebbe essere evitato perché un semplice errore di configurazione dello switch potrebbe portare a traffico Internet non filtrato che entra nella rete interna. Almeno usare due switch in questi scenari: uno per l'esterno del firewall e uno per l'interno del firewall. In molti ambienti, i segmenti DMZ vengono trattati separatamente, su un terzo switch oltre agli switch WAN e LAN. In altri, il lato WAN è sul proprio switch, mentre tutte le reti dietro il firewall sono sullo stesso switch che utilizza VLAN. Lo scenario più appropriato per una determinata rete dipende dalle circostanze specifiche, dal livello di rischio e dai problemi di sicurezza.

16.2.2 Utilizzare la VLAN1 predefinita

Poiché la VLAN 1 è la VLAN predefinita ("nativa"), può essere usata in modo inaspettato dallo switch. È simile all'uso di una politica di permesso predefinito sulle regole del firewall invece di negazione di default e selezionare ciò che è necessario. L'utilizzo di una VLAN diversa è sempre meglio, e garantisce che solo le porte selezionate devono essere su tale VLAN, per limitare l'accesso. Gli switch invieranno protocolli interni come STP (Prtocollo dell'albero di spanning), VTP (Protocollo del trunking delle VLAN, VLAN Trunking Protocol), e CDP (Protocollo di ricerca

Cisco, Cisco Discover Protocol) non contrassegnato sulla VLAN nativa, dove gli switch utilizzano questi protocolli. È generalmente meglio mantenere il traffico interno isolato dal traffico di dati.

Se la VLAN 1 deve essere utilizzata, fare molta attenzione ad assegnare ogni singola porta su ogni switch a una VLAN diversa tranne quelli che devono essere in VLAN 1, e non creare un'interfaccia di gestione per lo switch sulla VLAN 1. La VLAN nativa del gruppo switch dovrebbe anche essere cambiata in un altra, inutilizzata, VLAN. Alcuni switch potrebbero non supportare nessuna di queste soluzioni, e quindi è in genere più facile spostare i dati su una VLAN diversa invece di preoccuparsi di rendere disponibile la VLAN 1. Con l'ID della VLAN 2 attraverso 4094 tra cui scegliere, è senza dubbio meglio ignorare la VLAN 1 quando si progetta un nuovo schema della VLAN.

16.2.3 Utilizzare la VLAN predefinita di una porta trunk

Quando il traffico contrassegnato VLAN viene inviato su un tronco sulla VLAN nativa, i tag nei pacchetti che corrispondono alla VLAN nativa possono essere rimossi dallo switch per preservare la compatibilità con le reti più vecchie. Peggio ancora, i pacchetti con doppio tag con la VLAN nativa e una VLAN diversa avranno solo il tag della VLAN nativa rimosso quando si effettua il trunking per questa via e quando verranno elaborati in seguito, quel traffico può finire su una VLAN diversa. Questa è anche chiamato "VLAN saltellante (hopping)".

Come indicato nella sezione precedente, qualsiasi traffico non bloccato su una porta trunk sarà assunto come la VLAN nativa, che potrebbe anche sovrapporsi con un'interfaccia VLAN assegnata. A seconda di come lo switch gestisce tale traffico e come è visto da Firew4LL, utilizzare l'interfaccia direttamente potrebbe portare a due interfacce che sono sulla stessa VLAN.

16.2.4 Limitare l'accesso alle porte trunk

Poiché una porta trunk può comunicare con qualsiasi VLAN in un gruppo di switch del tronco, forse anche quelle non presenti sullo switch corrente possono a seconda delle configurazioni dello switch, quindi è importante proteggere fisicamente le porte del trunk. Assicurarsi anche che non ci siano porte configurate per il trunking che siano scollegate e abilitate dove qualcuno potrebbe collegarsi ad una, accidentalmente o in altro modo. A seconda dello switch, si può supportare la negoziazione dinamica del trunking. Assicurarsi che questa funzionalità sia disabilitata o correttamente limitata.

16.2.5 Altri problemi con gli switch

Nel corso degli anni ci sono state segnalazioni di rari casi in cui gli switch basati sulle VLAN hanno fatto trapelare traffico attraverso le VLAN, mentre in presenza di carichi pesanti, o se un indirizzo MAC di un PC su una VLAN è visto su un'altra VLAN. Questi problemi tendono a trovarsi in switch anziani con firmware non aggiornato, o switch gestiti con una estremamente bassa qualità. Questi tipi di problemi sono stati in gran parte risolti molti anni fa, quando tali problemi di sicurezza erano comuni. Non importa quale switch, di quale marca, è utilizzato per una rete, bisogna cercare di vedere se ha subito un alcun tipo di test di sicurezza, e garantire che il firmware più recente sia caricato sullo switch. Anche se questi problemi riguardano l'interruttore, e non Firew4LL, fanno parte della sicurezza complessiva di una rete.

Molti articoli qui sono specifici per particolari marche e modelli di switch. Le considerazioni sulla sicurezza variano in base allo switch utilizzato su una rete. Consultare la relativa documentazione per le raccomandazioni in materia di sicurezza della VLAN.

16.3 Configurazione della VLAN di Firew4LL

Questa sezione illustra come configurare le VLAN di Firew4LL.

16.3.1 Configurazione della VLAN dalla console

Le VLAN possono essere configurate sulla console utilizzando la funzione *Assegnare le interfacce*. L'esempio seguente mostra come configurare due VLAN, ID 10 e 20, con *igb0* come interfaccia principale. Le interfacce VLAN sono assegnate come OPT1 e OPT2:

|image24|

Valid interfaces are:

igb0 00:08:a2:09:95:b5 (up) Intel(R) PRO/1000 Network Connection, Version - igb1 00:08:a2:09:95:b6 (up) Intel(R) PRO/1000 Network Connection, Version - igb2 00:08:a2:09:95:b1 (down) Intel(R) PRO/1000 Network Connection, Version - igb3 00:08:a2:09:95:b2 (down) Intel(R) PRO/1000 Network Connection, Version - igb4 00:08:a2:09:95:b3 (down) Intel(R) PRO/1000 Network Connection, Version - igb5 00:08:a2:09:95:b3 (down) Intel(R) PRO/1000 Network Connection, Version -

Do VLANs need to be set up first? If VLANs will not be used, or only for optional interfaces, it is typical to say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? y

WARNING: all existing VLANs will be cleared if you proceed!

Do you want to proceed [y|n]? y

VLAN Capable interfaces:

igb0 00:08:a2:09:95:b5 (up) igb1 00:08:a2:09:95:b6 (up) igb2 00:08:a2:09:95:b1 igb3 00:08:a2:09:95:b2 igb4 00:08:a2:09:95:b3 (up) igb5 00:08:a2:09:95:b3 (up)

Enter the parent interface name for the new VLAN (or nothing if finished): igb2 Enter the VLAN tag (1-4094): 10

VLAN Capable interfaces:

igb0 00:08:a2:09:95:b5 (up) igb1 00:08:a2:09:95:b6 (up) igb2 00:08:a2:09:95:b1 igb3 00:08:a2:09:95:b2 igb4 00:08:a2:09:95:b3 (up) igb5 00:08:a2:09:95:b3 (up)

Enter the parent interface name for the new VLAN (or nothing if finished): igb2 Enter the VLAN tag (1-4094): 20

VLAN Capable interfaces:

igb0 00:08:a2:09:95:b5 (up) igb1 00:08:a2:09:95:b6 (up) igb2 00:08:a2:09:95:b1 igb3 00:08:a2:09:95:b2 igb4 00:08:a2:09:95:b3 (up) igb5 00:08:a2:09:95:b3 (up)

Enter the parent interface name for the new VLAN (or nothing if finished): <enter>

VLAN interfaces:

igb2_vlan10 VLAN tag 10, parent interface igb2 igb2_vlan20 VLAN tag 20, parent interface igb2

If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing "a" to begin the process.

Enter the WAN interface name or "a" for auto-detection (igb0 igb1 igb2 igb3 igb4 igb5 igb2_vlan10 igb2_vlan20 or a): igb1

Enter the LAN interface name or "a" for auto-detection NOTE: this enables full Firewalling/NAT mode. (igb0 igb2 igb3 igb4 igb5 igb2_vlan10 igb2_vlan20 a or nothing if finished): igb0

Enter the Optional 1 interface name or "a" for auto-detection (igb2 igb3 igb4 igb5 igb2_vlan10 igb2_vlan20 a or nothing if finished): igb2_vlan10

Enter the Optional 2 interface name or "a" for auto-detection (igb2 igb3 igb4 igb5 igb2_vlan20 a or nothing if finished): igb2_vlan20

Enter the Optional 3 interface name or "a" for auto-detection (igb2 igb3 igb4 igb5 a or nothing if finished):<enter>

The interfaces will be assigned as follows:

WAN -> igb1 LAN -> igb0 OPT1 -> igb2_vlan10 OPT2 -> igb2_vlan20

Do you want to proceed [y|n]? y

Writing configuration...done. One moment while the settings are reloading... done!

Dopo pochi secondi, le impostazioni del firewall verranno ricaricate e il menu della console verrà ricaricato.

16.3.2 Configurazione della VLAN dell'interfaccia Web

Nel sistema usato per questo esempio, WAN e LAN sono assegnate rispettivamente come *igb1* e *igb0*. C'è anche un'interfaccia *igb2* che verrà utilizzata come interfaccia principale della VLAN.

Per configurare le VLAN nell'interfaccia web di Firew4LL:

- **Passare a Interfacce>(assegnare) per visualizzare l'elenco delle** interfacce.
- Fare clic sulla scheda **Vlan**.
- Fare clic su **Aggiungere** per aggiungere una nuova VLAN
- Configurare la VLAN come mostrato nella figura *Modificare la VLAN*.

  Interfaccia principale L'interfaccia fisica su cui verrà utilizzato questo tag della VLAN. In questo caso, *igb2*

  Tag della VLAN Il numero ID della VLAN, in questo caso, 10

  Priorità della VLAN Lasciare al valore predefinito, vuoto

  Descrizione Testo per identificare lo scopo della VLAN, come DMZ

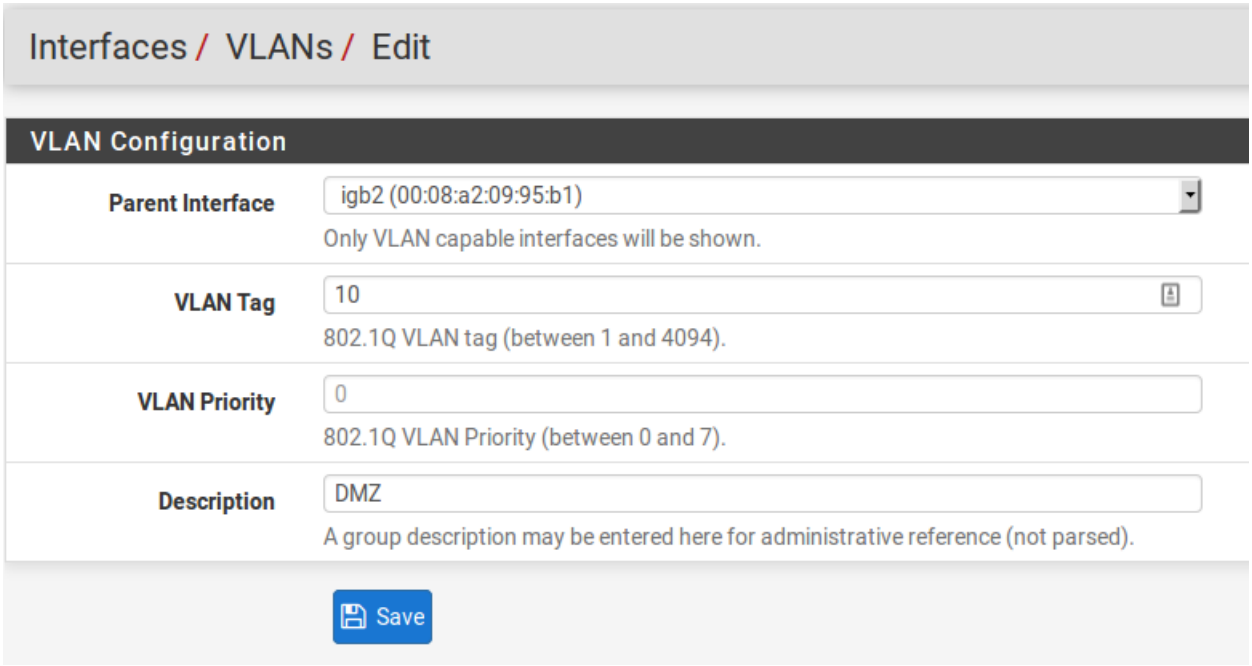


Fig. 1: Modificare la VLAN

- Fare clic su **Salvare** per tornare all'elenco della VLAN, che ora include la VLAN 10 appena aggiunta.

- Ripetere il processo per aggiungere ulteriori VLAN, come VLAN 20. Questi possono essere visti nella figura *Elenco di VLAN*

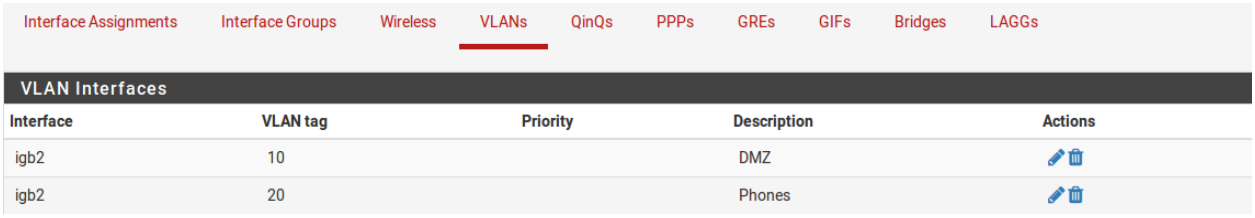


Fig. 2: Elenco di VLAN

Per assegnare le VLAN alle interfacce:

- Passare a **interfacce>(assegnare)**
- Fare clic su scheda **Assegnazioni interfaccia**
- Selezionare la VLAN da aggiungere dall'elenco **Porte di rete disponibili**, come *VLAN 10 su igb2 (DMZ)*
- Fare clic su **Aggiungere** per assegnare la porta di rete
- Ripetere gli ultimi due passaggi per assegnare la *VLAN 20 su igb2 (Telefoni)*

Quando finito, le interfacce appariranno come nella figura *Elenco di interfacce con VLAN*

Le interfacce OPT basate su VLAN si comportano come qualsiasi altra interfaccia OPT, il che significa che devono essere abilitate, configurate, avere regole di firewall aggiunte, e servizi come il server DHCP che dovranno essere configurati se necessario. Per ulteriori informazioni sulla configurazione delle interfacce opzionali, vedere *Nozioni di base sulla configurazione dell'interfaccia*.

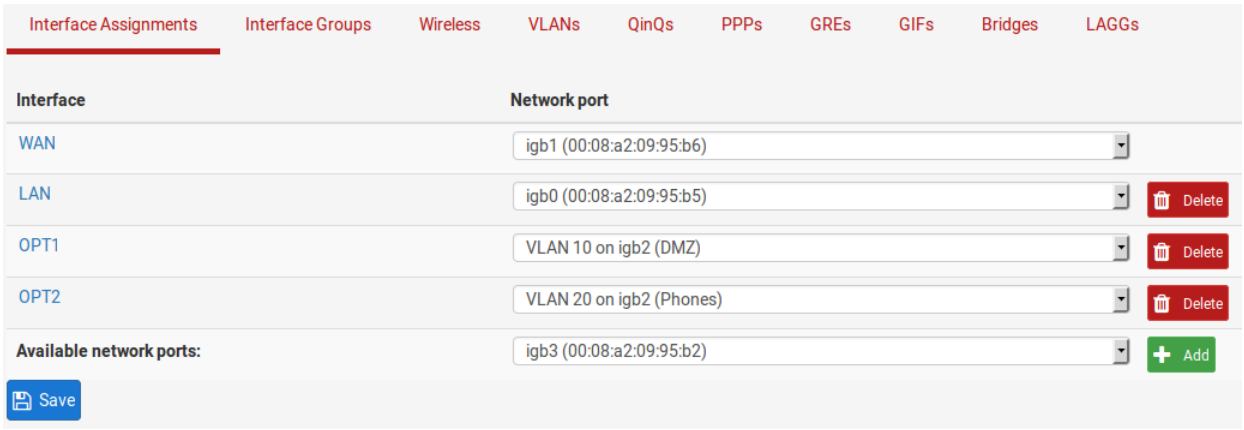


Fig. 3: Elenco di interfacce con VLAN

16.4 Configurazione VLAN sugli switch

Questa sezione fornisce una guida su come configurare alcune varietà di switch per l'uso con le VLAN. Questa offre una guida generica che si potrà applicare alla maggior parte se non tutti gli switch con capacità 802.1Q, passerà poi a coprire la configurazione specifica di Cisco, HP, Netgear, e Dell.

Nota: Da notare che questa è la configurazione minima necessaria per le VLAN in funzione, e non mostra necessariamente la configurazione degli switch ideali per qualsiasi ambiente specifico. Una discussione approfondita della sicurezza tramite switch è al di fuori della portata di questo libro.

16.4.1 Panoramica della configurazione degli switch

Generalmente tre o quattro cose devono essere configurate sugli switch con capacità di VLAN:

1. **Aggiungere/definire le VLAN**

   La maggior parte degli switch hanno mezzi per definire un elenco di VLAN configurate, e devono essere aggiunte prima di poter essere configurate su qualsiasi porta.

1. **Configurare la porta trunk**

   La porta a cui Firew4LL sarà collegato deve essere configurata come una porta trunk, contrassegnando tutte le VLAN possibili sull'interfaccia.

1. **Configurare le porte di accesso**

   Configurare le porte per gli host interni come porte di accesso sulle VLAN desiderate, con VLAN non regolate.

1. **Configura l'ID della VLAN della porta (PVID)**

   Alcuni switch richiedono la configurazione del PVID per le porte di accesso. Questo specifica quale VLAN usare per il traffico che entra in quella porta dello switch. Per alcuni switch questo è un processo a passi, configurando la porta come una porta di accesso su una particolare VLAN, esso contrassegna automaticamente il traffico in arrivo su quella porta. Altri switch richiedono che questo sia configurato in uno o due punti. Controllare la documentazione dello switch per i dettagli se non è uno descritto in questo capitolo.

16.4.2 Switch Cisco IOS

La configurazione e l'utilizzo di VLAN su switch Cisco con IOS è un processo abbastanza semplice, che richiede solo pochi comandi per creare e utilizzare VLAN, porte trunk e l'assegnazione di porte alle VLAN. Molti switch di altri fornitori si comportano in modo simile a IOS, e useranno quasi la stessa sintassi se non identica per la configurazione.

Creare VLAN

Le VLAN possono essere create in modo autonomo o utilizzando il protocollo trunk per le VLAN (VTP). L'uso del VTP può essere più conveniente, in quanto propaga automaticamente la configurazione VLAN a tutti gli switch su un dominio VTP, anche se può anche creare problemi di sicurezza e aprire la possibilità di cancellare inavvertitamente la configurazione VLAN. Con VTP, per aggiungere un'altra VLAN deve essere configurato solo su un singolo switch, e poi tutti gli altri switch del tronco del gruppo possono assegnare le porte a tale VLAN. Se le VLAN sono configurate in modo indipendente, devono essere aggiunte a mano ad ogni switch. Fare riferimento alla documentazione Cisco su VTP per garantire un uso sicuro della configurazione utilizzata, e che non sia soggetto a una distruzione accidentale. In una rete con solo pochi switch in cui le VLAN non cambiano frequentemente, il VTP può essere eccessivo ed evitarlo eviterà anche i suoi potenziali crolli.

VLAN indipendente

Per creare VLAN indipendenti:

sw# vlan database sw(vlan)# vlan 10 name «DMZ Servers» sw(vlan)# vlan 20 name «Phones» sw(vlan)# exit

VLAN di VTP

Per configurare uno switch per VTP e VLAN, creare un database VTP sullo switch primario e quindi creare due VLAN:

sw# vlan database sw(vlan)# vtp server sw(vlan)# vtp domain example.com sw(vlan)# vtp password SuperSecret sw(vlan)# vlan 10 name «DMZ Servers» sw(vlan)# vlan 20 name «Phones» sw(vlan)# exit

Configurare una porta trunk

Per Firew4LL, una porta dello switch non solo deve essere in modalità trunk, ma deve anche usare il tag 802.1q. Questo può essere fatto in questo modo:

sw# configure terminal sw(config)# interface FastEthernet 0/24 sw(config-if)# switchport mode trunk sw(config-if)# switchport trunk encapsulation dot1q

---

Nota: Su alcuni switch Cisco IOS più recenti, il metodo di incapsulamento della VLAN ISL del proprietario di Cisco è deprecato e non più supportato. Se uno switch non consente l'opzione di configurazione incapsulamento dot1q, supporta solo 802.1Q e l'incapsulamento non deve essere specificato.

Aggiungere porte alla VLAN

Per aggiungere porte a queste VLAN, assegnarle come segue:

sw# configure terminal sw(config)# interface FastEthernet 0/12 sw(config-if)# switchport mode access sw(config-if)# switchport access vlan 10

16.4.3 Switch basati sul CatOS di Cisco

La creazione di VLAN su Catos è un po" diversa, anche se la terminologia è la stessa dell'utilizzo di VLAN sotto IOS. Le VLAN indipendenti e il VTP sono entrambi possibili per mantenere il database VLAN:

```
# set vtp domain example mode server
# set vtp passwd SuperSecret
# set vlan 10 name dmz
# set vlan 20 name phones
```

Quindi configurare una porta tronco per gestire automaticamente ogni VLAN:

```
# set trunk 5/24 on dot1q 1-4094
```

Poi aggiungere porte alla VLAN:

```
# set vlan 10 5/1-8
# set vlan 20 5/9-15
```

16.4.4 Switch ProCurve di HP

Gli switch con Procurve di HP supportano solo il trunking 802.1q, quindi non è necessaria alcuna configurazione per l'incapsulamento. In primo luogo, usare ssh o telnet nello switch e aprire il menu di gestione.

Abilitare il supporto delle VLAN

In primo luogo, il supporto VLAN deve essere abilitato sullo switch se non è già:

- Scegliere la **configurazione dello switch**
- Scegliere le **funzionalità avanzate**
- Scegliere il **menu della VLAN**…
- Scegliere il **supporto della VLAN**
- Impostare **Abilitare le VLAN** su *Sì* se non è già impostato, e scegliere un certo numero di VLAN. Ogni volta che questo valore viene modificato lo switch deve essere riavviato, in modo da assicurarsi che sia abbastanza grande da supportare il numero di VLAN necessario.
- Riavviare lo switch per applicare le modifiche.

Creare le VLAN

Prima che le VLAN possano essere assegnate alle porte, devono essere create le VLAN. Nel menu di configurazione dello switch:

- Scegliere la **configurazione dello switch**
- Scegliere le **funzionalità avanzate**
- Scegliere il **menu della VLAN**…
- Scegliere i **nomi delle VLAN**
- Scegliere **Aggiungere**
- Inserire l'**ID della VLAN**, 10
- Inserire il **nome**, DMZ
- Scegliere **Salvare**
- Ripetere i passaggi da **Aggiungere** a **Salvare** per qualsiasi VLAN rimanente

Assegnazione porta Trunk alla VLAN

Successivamente, configurare la porta trunk per il firewall nonché eventuali porte trunk su altri switch contenenti più VLAN.

- Scegliere la **configurazione dello switch**
- Scegliere il **menu della VLAN**…
- Scegliere l'**assegnazione della porta manuale**
- Scegliere **Modificare**
- Trovare la porta da assegnare
- Premere **spazio** sulla VLAN di default fino a quando non compare **No**

- Spostare sulla colonna per ciascuna delle VLAN su questa porta trunk, e Premere **spazio** finché non compare **Taggata**. Ogni VLAN in uso deve essere contrassegnata sulla porta tronco.

Assegnazione delle porte di accesso alle VLAN

- Scegliere la **configurazione switch**
- Scegliere il **menu della VLAN**...
- Scegliere l'**assegnazione della porta della VLAN**
- Scegliere **Modificare**
- Trova la porta da assegnare
- Premere **spazio** sulla **VLAN di default** fino a quando non compare **No**
- Spostare verso la colonna per la VLAN a cui verrà assegnata questa porta
- Premere **spazio** fino a quando non compare **Senza tag**.

16.4.5 Switch gestiti Netgear

Questo esempio riguarda un `Gs108tv1`, ma altri modelli di Netgear sono tutti molto simili se non identici. Ci sono anche diversi altri fornitori tra cui Zyxel che vendono switch realizzati dallo stesso produttore, utilizzando la stessa interfaccia web con un logo diverso. Accedere all'interfaccia web dello switch per avviare.

Pianificazione della configurazione della VLAN

Prima di configurare lo switch, sono necessari diversi elementi:

1. Il numero di VLAN da configurare
2. Gli ID da usare per le VLAN
3. Come ogni porta di commutazione deve essere configurata

Per questo esempio, viene utilizzata una porta 8 Gs108tv1, e verrà configurata come mostrato nella tabella *Configurazione della VLAN di Netgear GS108T*.

Tabella 1: Configurazione della VLAN di Netgear GS108T

+=================+=================-+=======================+ | porta switch | modalità VLAN | VLAN assegnato | +=================+=================-+=======================+ | 1 | tronco | *10* e 20, taggato | +=================+=================-+=======================+ | 2 | accesso | *10* senza tag | +=================+=================-+=======================+ | 3 | accesso | *10* senza tag | +=================+=================-+=======================+ | 4 | accesso | *10* senza tag | +=================+=================-+=======================+ | 5 | accesso | *20* senza tag | +=================+=================-+=======================+ | 6 | accesso | *20* senza tag | +=================+=================-+=======================+ | 7 | accesso | *20* senza tag | +=================+=================-+=======================+ | 8 | accesso | *20* senza tag | +=================+=================-+=======================+

Abilitare VLAN 802.1Q

Per configurare lo switch da utilizzare per il trunking delle VLAN 802.1Q:

- Andare al menu del **Sistema** sul lato sinistro della pagina

- Fare clic sulle **impostazioni del gruppo di VLAN**, come indicato nella figura *impostazioni del gruppo di VLAN*.

Fig. 4: Impostazioni del gruppo della VLAN

- Selezionare IEEE 802.1Q VLAN (Figura *Abilitare le VLAN 802.1Q*).

Fig. 5: Abilitare le VLAN 802.1Q

- Fare clic su OK per confermare il passaggio al trunking 802.1Q, come mostrato nella figura *Confermare la modifica a 802.1Q VLAN*.

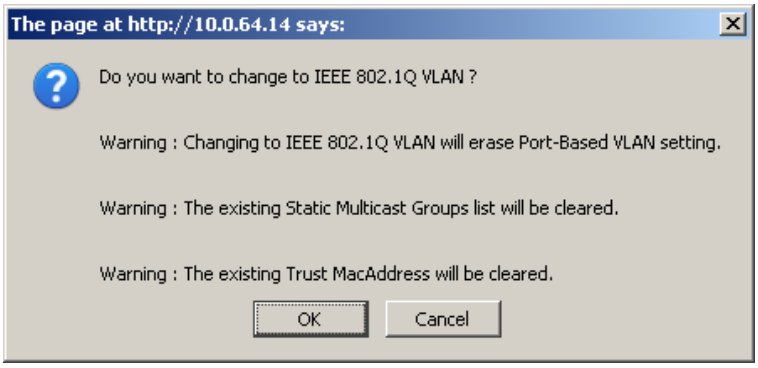


Fig. 6: Confermare la modifica a 802.1Q VLAN.

Dopo aver fatto clic su OK, la pagina si aggiornerà con la configurazione VLAN 802.1Q come mostrato in figura *Configurazione di default con 802.1Q*.

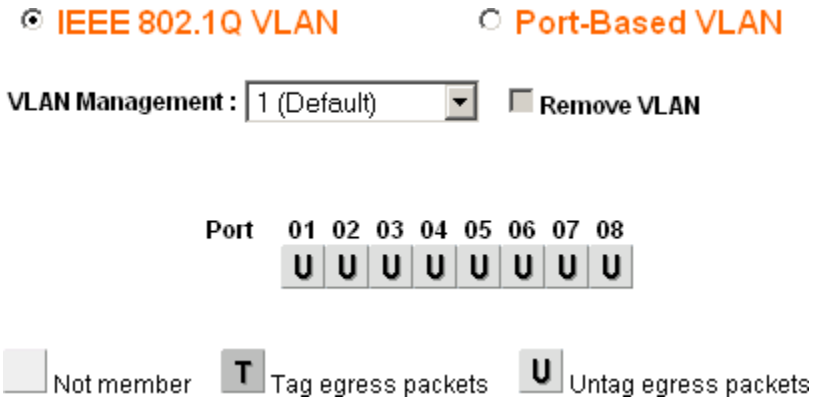


Fig. 7: Configurazione di default con 802.1Q

Aggiungere le VLAN

Per questo esempio, due VLAN verranno aggiunte con gli ID 10 e 20. Per aggiungere una VLAN:

- Fare clic sul menu a discesa della **Gestione delle VLAN**

- Fare clic su **Aggiungere una nuova VLAN**, come mostrato nella figura *Aggiungere una nuova VLAN*.

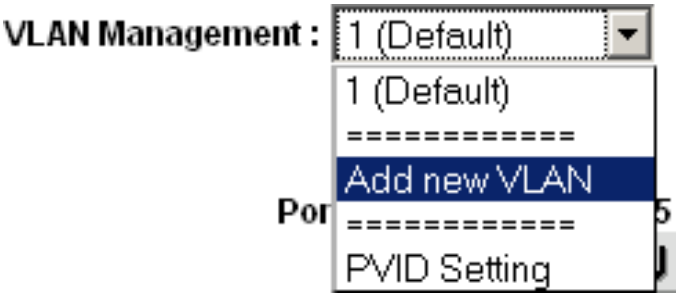


Fig. 8: Aggiungere una nuova VLAN

- Inserire l'ID della VLAN per questa nuova VLAN, come 10
- Fare clic su **Applicare**. La schermata VLAN è ora pronta per configurare la VLAN *10* (Figura *Aggiungere la VLAN 10*).
- Fare clic su **Aggiungere una nuova VLAN** di nuovo come mostrato nella figura *Aggiungere una nuova VLAN* per aggiungere VLAN *20* (Figura *Aggiungere VLAN 20*).

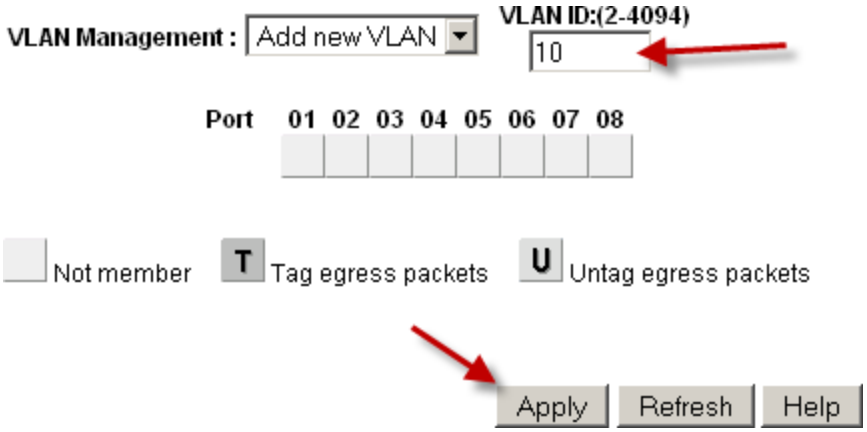


Fig. 9: Aggiungere la VLAN 10

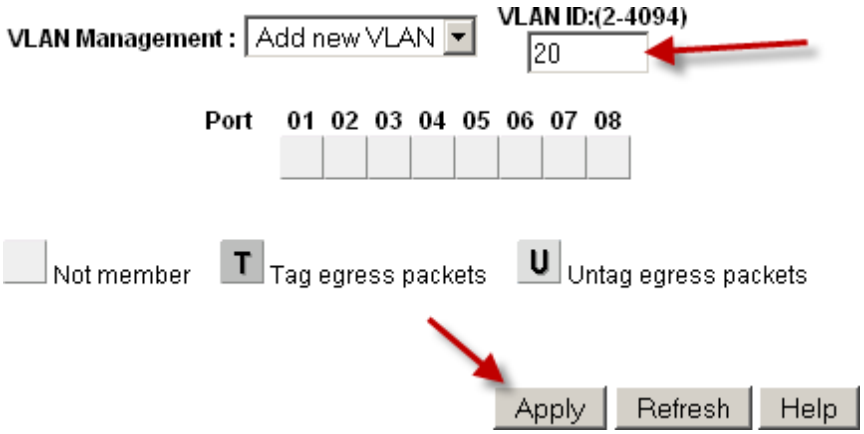


Fig. 10: Aggiungere la VLAN 20

Aggiungere il numero di VLAN in base alle esigenze, quindi passare alla sezione successiva.

Configurare il tag della VLAN

Quando una VLAN viene selezionata dal menu a discesa della **gestione delle VLAN**, mostra come la VLAN è configurata su ogni porta:

- Una casella **vuota** indica che la porta non è membro della VLAN selezionata.
- Una casella contenente **T** indica che la VLAN viene inviata su quella porta con il tag 802.1Q.
- **U** indica che la porta è un membro di tale VLAN e lascia la porta non protetta.

La porta trunk deve avere entrambe le VLAN aggiunte e taggate

Avvertimento:

Non modificare la configurazione della porta utilizzata per accedere all'interfaccia web dello switch! Questo bloccherà l'amministratore fuori dallo switch. L'unico mezzo di recupero sul Gs108tv2 è l'utilizzo del pulsante di reset alle impostazioni di fabbrica in quanto non dispone di una console seriale. Per gli switch dotati di console seriali, tenere a portata di mano un cavo modem null nel caso in cui la connettività di rete con lo switch venga persa. La configurazione della gestione VLAN è trattata più avanti in questa sezione.

Fare clic nelle caselle sotto il numero di porta, come mostrato nella figura *Alternanza dei membri di VLAN* per passare tra le tre opzioni di VLAN.

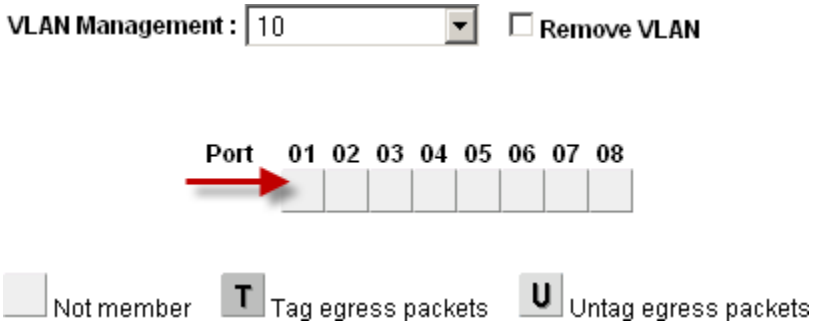


Fig. 11: Alternanza dei membri di VLAN

Configurare la VLAN 10 come membro

La figura *Configurare la VLAN 10 come membro* mostra la VLAN 10 configurata come descritto nella tabella *Configurazione della VLAN per il netgear gs10St*. Le porte di accesso su questa VLAN sono impostate come **senza tag** mentre la porta del tronco è impostata su taggata.

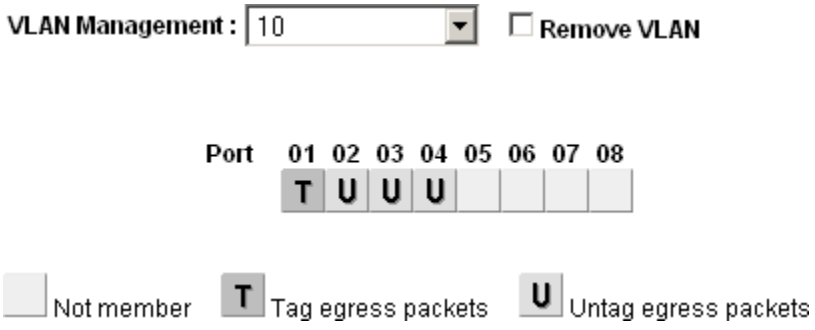


Fig. 12: Configurare la VLAN 10 come membro

Configurare la VLAN 20 come membro

Selezionare **20** dal menu a discesa della Gestione delle VLAN per configurare la porta membro per la VLAN **20**.

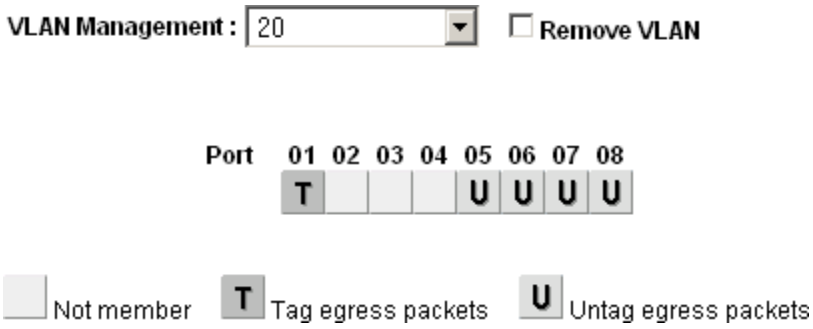


Fig. 13: Configurare la VLAN 20 come membro

Cambiare PVID

Sugli switch Netgear, oltre alle impostazioni di tag precedentemente configurate, il PVID deve essere configurato anche per specificare la VLAN utilizzata per i frame che entrano in una porta:

- Selezionare **PVID** dal menu a discesa della Gestione delle VLAN, come mostrato nella figura *Impostazioni di PVID*.

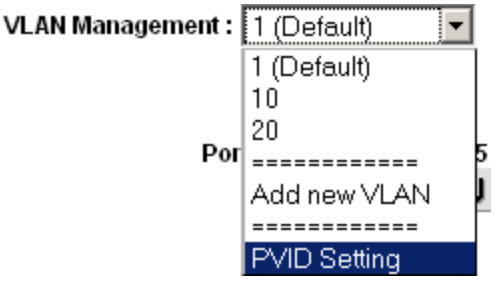


Fig. 14: Impostazioni di PVID

L'impostazione PVID predefinita è VLAN 1 per tutte le porte, come mostrato nella figura *Configurazione di PVID predefinita*.

- Cambiare il PVID per ogni porta di accesso, ma lasciare la porta tronco e la porta utilizzata per accedere all'interfaccia di gestione degli switch impostata a 1 .

  La figura *Configurazione PVID per le VLAN 10 e 20* mostra la configurazione PVID corrispondente alle assegnazioni di porta mostrate nella tabella *Configurazione della VLAN con Netgear GS108T*, con la porta 8 utilizzata per accedere all'interfaccia di gestione degli switch.

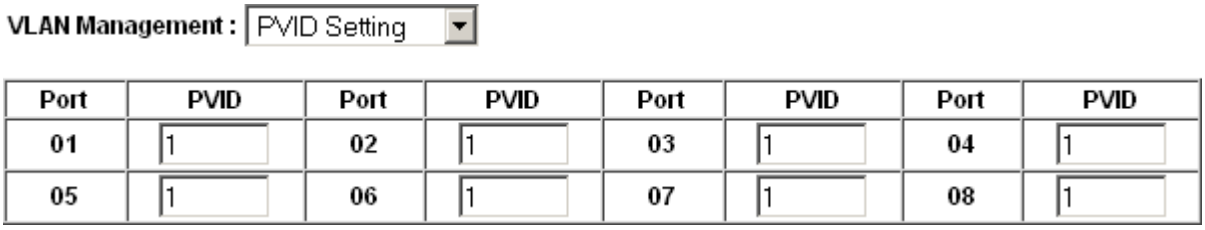


Fig. 15: Configurazione di PVID predefinita

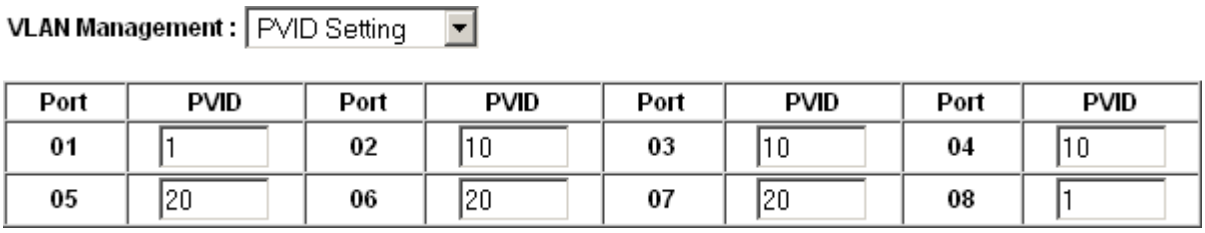


Fig. 16: Configurazione PVID per le VLAN 10 e 20

- Applicare le modifiche una volta terminato

Rimuovere la configurazione di VLAN 1

Per impostazione predefinita, tutte le porte sono membri della VLAN 1 con frame di uscita non taggati. Per rimuovere la VLAN 1 dalle altre porte:

- Seleziona *1 (predefinito)* dall'elenco a discesa della **gestione delle VLAN**
- Rimuovere la VLAN 1 da tutte le porte, tranne quella utilizzata per gestire lo switch e la porta tronco, per evitare di essere scollegato.

  In questo esempio, la porta 8 viene utilizzata per gestire lo switch. Al termine, la schermata apparirà come nella figura *Rimuovere la VLAN 1 come membro*.

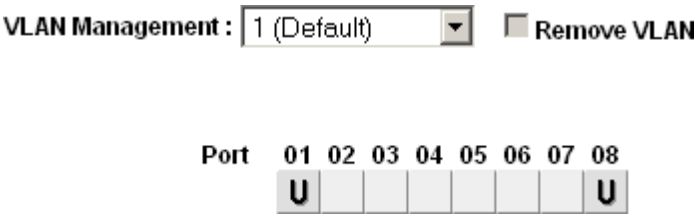


Fig. 17: Rimuovere la VLAN 1 come membro

- Applicare le modifiche una volta terminato

Verificare la funzionalità della VLAN

Configurare le VLAN su Firew4LL, incluso il server DHCP sulle interfacce VLAN, se necessario. Collegare i sistemi alle porte di accesso configurate e testare la connettività. Se tutto funziona come desiderato, continuare con la fase successiva. Se le cose non funzionano come previsto, rivedere la creazione del tag e la configurazione PVID sullo switch, e la configurazione VLAN e le assegnazioni di interfaccia su Firew4LL.

16.4.6 Switch Powerconnect di Dell

L'interfaccia di gestione degli switch Dell varia leggermente tra i modelli, ma la seguente procedura si accommoda alla maggior parte dei modelli. La configurazione è abbastanza simile allo stile di Cisco IOS.

Primo, creare le VLAN:

console# config console(config)# vlan database console(config-vlan)# vlan 10 name dmz media ethernet console(config-vlan)# vlan 20 name phones media ethernet console(config-vlan)# exit

Successivamente, configurare una porta trunk:

console(config)# interface ethernet 1/1 console(config-if)# switchport mode trunk console(config-if)# switchport allowed vlan add 1-4094 tagged console(config-if)# exit

Infine, aggiungere le porte alle VLAN:

console(config)# interface ethernet 1/15 console(config-if)# switchport allowed vlan add 10 untagged console(config-if)# exit

16.5 Configurazione QinQ in Firew4LL

Qinq, noto anche come IEEE 802.1ad o Vlan impilate, è un mezzo di annidamento di VLAN per il traffico contrassegnato all'interno di pacchetti che sono già taggati dalla VLAN, o presentano già il doppio tag della VLAN, o il traffico "che effettua un doppio tag".

Qinq è utilizzato per spostare i gruppi di VLAN su un singolo link contenente un tag esterno, come si può trovare su alcuni collegamenti ISP, Metro Ethernet, o datacenter tra le posizioni. Può essere un modo semplice/veloce di trunking della VLAN attraverso le posizioni senza avere una connessione con capacità di trunking tra i siti, a condizione che l'infrastruttura tra le posizioni non elimini i tag dai pacchetti.

Configurare le interfacce Qinq su Firew4LL è abbastanza semplice:

- Passare a **interfacce>(assegnare)**
- Fare clic sulla scheda **Qinq**
- Fare clic su **Aggiungere** per aggiungere una nuova voce Qinq
- Configurare la voce Qinq come segue:

  Interfaccia principale L'interfaccia che trasporterà il traffico Qinq.

  Tag di primo livello L'ID della VLAN esterna sull'interfaccia Qinq o l'ID VLAN fornito dal fornitore per il link sito-to-sito.

  Aggiungere l'interfaccia ai gruppi di interfaccia Qinq Se selezionata, verrà creato un nuovo gruppo di interfacce chiamato Qinq che può essere utilizzato per filtrare tutte le sottointerface Qinq contemporaneamente.

  Quando centinaia o potenzialmente migliaia di tag Qinq sono presenti, questo riduce notevolmente la quantità di lavoro necessario per utilizzare le interfacce Qinq

  Descrizione Testo facoltativo di riferimento, utilizzato per identificare la voce

  Membro(i) ID delle VLAN membro per il tag Qinq. Questi possono essere inseriti uno per riga cliccando su **Aggiungere tag**, o in intervalli come 100-150
- Fare clic su **Salvare** per completare l'interfaccia

Nel seguente esempio (Figura *Esempio di base di Qinq*), un'interfaccia Qinq è configurata per trasportare il traffico taggato per le Vlan *10* e *20* attraverso il link su *igb3* con un tag di primo livello di *2000*.

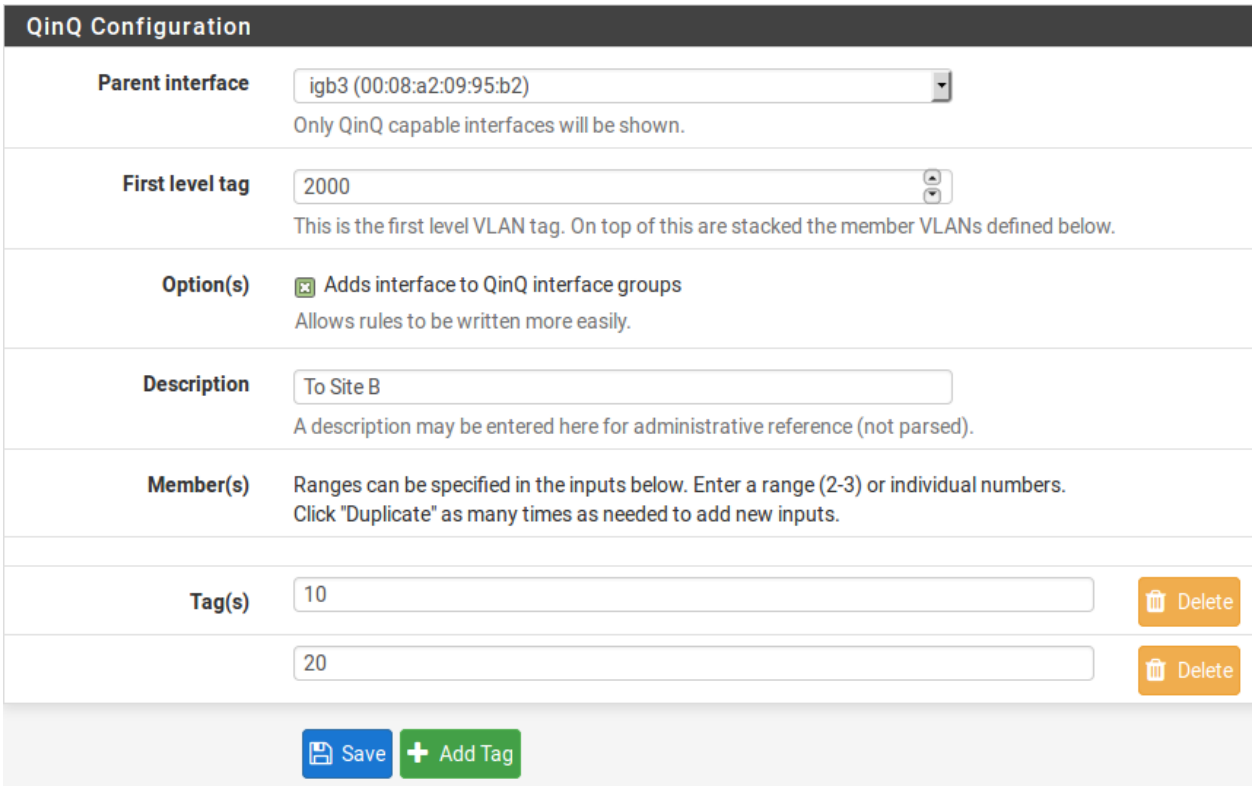


Fig. 18: Esempio di base di Qinq

Nella figura *Elenco Qinq*, questa voce viene visualizzata nella scheda dell'elenco Qinq riassuntivo.

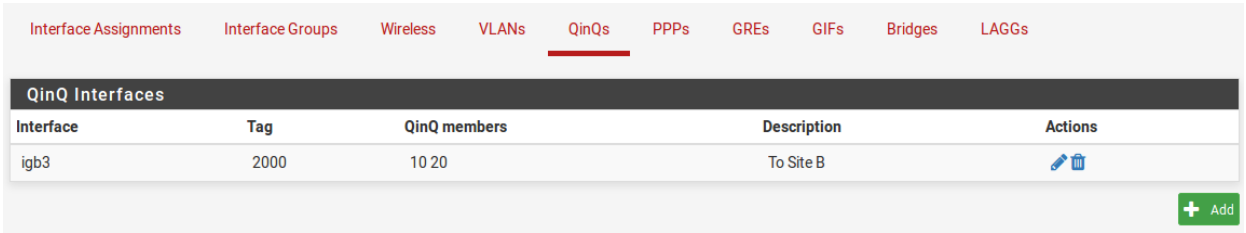


Fig. 19: Elenco Qinq

Il gruppo di interfaccia automatico, mostrato nella figura *Gruppo di interfacce Qinq*, non deve essere modificato manualmente. Poiché queste interfacce non sono assegnate, non è possibile apportare modifiche al gruppo senza romperlo. Per ricreare il gruppo, eliminarlo da questa lista e quindi modificare e salvare nuovamente l'istanza Qinq per aggiungerlo di nuovo.

Le regole possono essere aggiunte alla scheda **Qinq** in **Firewall>Regole** per far passare il traffico in entrambe le direzioni attraverso i link Qinq.

Da qui, il modo in cui vengono utilizzate le interfacce Qinq dipende principalmente dalle esigenze della rete. Molto probabilmente, le interfacce risultanti possono essere assegnate e poi configurate in qualche modo, o collegate alle loro VLAN equivalenti locali (ad es. creare un ponte tra igb2_vlan10 assegnata e igb3_2000_10 e così via).

La configurazione di QinQ sarà approssimativamente la stessa su entrambe le estremità del setup. Per esempio, se entrambe le parti utilizzano configurazioni di interfaccia identiche, quindi il traffico che lascia il sito A fuori su igb3_2000_10 passerà attraverso VLAN 2000 su igb3, uscirà dall'altro lato su VLAN 2000 su igb3 al sito B, e poi in igb3_2000_10 al sito B.

Le VLAN consentono a uno switch di trasportare più domini di trasmissione discreti, consentendo a un singolo switch di funzionare come se si trattasse di più switch. Le VLAN sono comunemente utilizzate per la segmentazione della rete nello stesso modo in cui possono essere utilizzati più switch: per posizionare gli host su un segmento specifico, isolato da altri segmenti. Quando il trunking è impiegato tra switch, i dispositivi sullo stesso segmento non devono necessariamente risiedere sullo stesso interruttore. I dispositivi che supportano il trunking possono anche comunicare su più VLAN attraverso una singola porta fisica.

Questo capitolo riguarda i concetti, la terminologia e la configurazione della VLAN

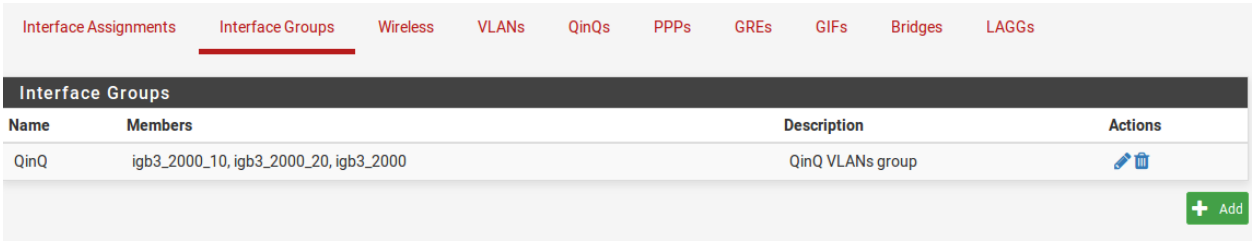


Fig. 20: Gruppo di interfacce QinQ

16.6 Requisiti

Vi sono due requisiti che devono essere soddisfatti per l'impiego delle VLAN.

1. **Switch con capacità di VLAN 802.1Q**

   Ogni switch gestito decente prodotto negli ultimi 15 anni supporta il trunking delle VLAN 802.1Q.

Avvertimento: La VLAN non può essere utilizzata con uno switch non gestito.

2. **Scheda di rete in grado di effetuare il tag delle VLAN**

   È necessario un NIC che supporti il tag della VLAN per l'hardware o che abbia un supporto di frame lungo. Ogni frame della VLAN ha un tag 802.1Q di 4 byte aggiunto nell'intestazione, quindi la dimensione del frame può arrvare fino a 1522 byte. È necessaria un tag della VLAN per hardware o frame lunghi perché altri adattatori non funzioneranno con frame più grandi del normale massimo di 1518 byte con l'Ethernet di 1500 MTU. Questo causerà grandi frame da eliminare, ciò causa problemi di prestazioni e di stallo di connessione.

Nota:

Anche se un adattatore è elencato come in grado di supportare un frame lungo, ciò non garantisce l'implementazione specifica di quel chipset NIC che supporta correttamente i frame lunghi. I NIC di Realtek rl(4) sono i maggiori trasgressori. Molti funzioneranno bene, ma alcuni non supportano correttamente i frame lunghi, e altri non accetteranno i frame etichettati 802.1Q. Se si riscontrano problemi utilizzando una delle NIC elencate sotto il supporto frame lungo, si consiglia di provare un'interfaccia con il supporto di tag della VLAN per hardware. Non siamo a conoscenza di problemi simili con NIC elencati sotto il supporto della VLAN per hardware.

Interfacce Ethernet con supporto hardware VLAN:

```
*ae(4), age(4), alc(4), ale(4), bce(4), bge(4), bxe(4), cxgb(4), cxgbe(4),
em(4), igb(4), ixgb(4), ixgbe(4), jme(4), msk(4), mxge(4), nxge(4), nge(4),
re(4), sge(4), stge(4), ti(4), txp(4), vge(4).*
```

Interfacce Ethernet con supporto long frame:

```
*axe(4)*, *bfe(4)*, *cas(4)*, *dc(4)*, *et(4)*, *fwe(4)*, *fxp(4)*, *gem(4)*,
*hme(4)*, *le(4)*, *nfe(4)*, *nve(4)*, *rl(4)*, *sf(4)*, *sis(4)*, *sk(4)*,
*ste(4)*, *tl(4)*, *tx(4)*, *vr(4)*, *vte(4)*, *xl(4)*
```

CAPITOLO 17

MultiWAN

17.1 Terminologia e concetti delle WAN multiple

Questa sezione tratta la terminologia e i concetti necessari per capire come configurare più reti WAN con Firew4LL.

17.1.1 Interfaccia di tipo WAN

Un'interfaccia di tipo WAN è un'interfaccia attraverso la quale Internet può essere raggiunto, direttamente o indirettamente. Il firewall tratta qualsiasi interfaccia con un gateway selezionato nella pagina del menu **Interfacce** come una WAN. Ad esempio, con una WAN con indirizzo IP statico, **Interfacce>WAN** ha un gateway selezionato, come **WAN_GW**. Se questa selezione del gateway non è presente, allora l'interfaccia verrà trattata come un'interfaccia locale. Non selezionare un gateway nella voce del menu **Interfacce** per le interfacce locali. Le interfacce IP dinamiche come DHCP e PPPoE ricevono automaticamente un gateway dinamico e sono sempre trattate come WAN.

La presenza di un gateway nella configurazione dell'interfaccia cambia il comportamento del firewall su tali interfacce in diversi modi. Ad esempio, le interfacce con un insieme di gateway hanno l'opzione reply-to sulle loro regole del firewall, sono utilizzate come interfacce di uscita per NAT in uscita automatico e ibrido, e sono trattate come WAN dalla procedura guidata di gestione del traffico.

Nota: Le interfacce locali e di altro tipo possono avere un gateway definito in **Sistema>Routing**, a condizione che tale gateway non sia scelto nell'ambito della configurazione dell'interfaccia, ad esempio in **Interfacce>LAN**.

17.1.2 Politica di routing

La politica del routing si riferisce ai mezzi di instradamento del traffico da più di un indirizzo IP di destinazione del traffico, come viene fatto con la tabella di routing nella maggior parte dei sistemi operativi e router. Questo si ottiene con l'uso di una politica di qualche tipo, di solito le regole di firewall o una lista di controllo degli accessi. In Firew4LL, il campo **Gateway** disponibile quando si modificano o si aggiungono le regole del firewall consente l'uso della politica di routing. Il campo Gateway contiene tutti i gateway definiti sul firewall sotto **Sistema>Routing**, più qualsiasi gruppo di gateway.

La politica di routing fornisce un potente mezzo per indirizzare il traffico verso l'interfaccia WAN appropriata o un altro gateway, dal momento che permette di abbinare qualsiasi regola del firewall. Host specifici, sottoreti, protocolli e altro ancora possono essere utilizzati per indirizzare il traffico.

Nota: Ricordare che tutte le regole del firewall, comprese le regole di politica del routing, sono elaborate in ordine dall'alto, e la prima che corrisponde vince.

17.1.3 Gruppi di gateway

I gruppi gateway definiscono come un set scelto di gateway fornisca funzionalità di failover e/o bilanciamento del carico. Sono configurati in **Sistema>Routing**, nella scheda **Gruppi di gateway**.

17.1.4 Failover

Failover si riferisce alla possibilità di utilizzare una sola connessione WAN, ma passare a un'altra WAN se la connessione preferita non riesce. Questo è utile per le situazioni in cui un certo traffico, tutto il traffico, dovrebbe utilizzare una connessione WAN specifica a meno che non sia indisponibile.

Vedi anche:

Per fallire da un *firewall* all'altro, piuttosto che da una WAN all'altra, vedere *Elevata disponibilità*.

17.1.5 Bilanciamento del carico

La funzionalità di **bilanciamento del carico** in Firew4LL consente di distribuire il traffico su più connessioni WAN in modo round-robin. Questo viene fatto su base **per-connessione**. Se un gateway che fa parte di un gruppo di bilanciamento del carico fallisce, l'interfaccia viene contrassegnata come down e rimossa da tutti i gruppi fino a quando non recupera.

17.1.6 Monitoraggio Indirizzi IP

Quando si configura il failover o il bilanciamento del carico, ogni gateway è associato a un indirizzo IP da monitorare (*IP da monitorare*). In una configurazione tipica, Firew4LL farà un ping su questo indirizzo IP e se smette di rispondere, l'interfaccia sarà contrassegnata come down. Le opzioni sul gruppo gateway possono selezionare diversi trigger di guasto oltre alla perdita di pacchetto. Gli altri trigger possono causare alta latenza, o una combinazione di perdita di pacchetti e alta latenza, o il circuito spento.

Che cosa costituisce il fallimento?

L'argomento è un po" più complesso di « se i ping all'IP da monitorare falliscono, l'interfaccia è contrassegnata come down[1]. I criteri effettivi per un guasto dipendono dalle opzioni scelte durante la creazione del gruppo gateway e delle singole impostazioni su un gateway.

Le impostazioni per ogni gateway che controllano quando è considerato up e down sono tutti discussi in *Avanzate*. Le soglie per la perdita dei pacchetti, la latenza, il tempo di inattività e persino l'intervallo di verifica del gateway sono tutte configurabili individualmente.

17.1.7 Switch Interrompere/Forzare lo stato

Quando un gateway è danneggiato, Firew4LL può facoltativamente far andare giù tutti gli stati per forzare i client a riconnettersi, e così facendo useranno un gateway che è in linea, invece di un gateway che è down. Questo attualmente funziona solo a senso unico, nel senso che può spostare le connessioni fuori di un gateway danneggiato, ma non li può costringere di nuovo se il gateway originale ritorna in linea.

Questo è un comportamento facoltativo, abilitato per impostazione predefinita. Per informazioni sulla modifica di questa impostazione, vedere *Monitoraggio del Gateway*.

17.1.8 Commutazione del gateway predefinito

Il traffico in uscita dal firewall userà il gateway predefinito a meno che un percorso statico non invii il pacchetto lungo un percorso diverso. Se il gateway predefinito è su una WAN che è inattiva, i demoni sul firewall non saranno in grado di effettuare connessioni in uscita, a seconda delle funzionalità del demone e della sua configurazione. Quando **la commutazione del gateway predefinito** (*Commutazione del gateway predefinito*) è abilitato, il gateway predefinito per il firewall sarà passato al gateway disponibile successivo se il gateway predefinito normale non riesce, e quindi è commutato quando la WAN recupera.

17.2 Strategie di politica di routing, bilanciamento del carico e failover

Questa sezione fornisce indicazioni sugli obiettivi comuni delle Multi-wan e su come vengono raggiunti con Firew4LL.

17.2.1 Aggregazione della larghezza di banda

Uno dei desideri primari con le multiWAN è l'aggregazione della larghezza di banda. Con il bilanciamento del carico, Firew4LL può aiutare a raggiungere questo obiettivo. C'è, tuttavia, un avvertimento: se il firewall ha due circuiti WAN da 5 Mbps, non può ottenere 10 Mbps di capacità di trasmissione con una *singola* connessione del client. Ogni singola connessione deve essere legata a una sola WAN specifica. Questo vale per qualsiasi soluzione multiWAN diversa da MLPPP. La larghezza di banda di due diverse connessioni Internet non può essere aggregata in un unico grande "tubo" senza il coinvolgimento dell'ISP. Con il bilanciamento del carico, dal momento che le singole connessioni sono bilanciate in modo roubd-robin, 10 Mbps di throughput possono essere raggiunti solo utilizzando due circuiti da 5 Mbps quando sono coinvolte connessioni multiple. Le applicazioni che utilizzano connessioni multiple, come molti acceleratori di download, saranno in grado di raggiungere la capacità di trasmissione combinata di due o più connessioni.

Nota: Il Multi-link PPPoE (MLPPP) è l'unico tipo di WAN che può raggiungere la piena larghezza di banda aggregata di tutti i circuiti in un gruppo, ma richiede un supporto speciale da parte dell'ISP. Per ulteriori informazioni su MLPPP, vedere *Multi-link Pppoe (MLPPP)*

Nelle reti con numerose macchine interne che accedono a Internet, il bilanciamento del carico raggiungerà velocità vicine alla capacità di trasmissione combinata bilanciando le numerose connessioni interne fuori da tutte le interfacce WAN.

17.2.2 Segregazione dei servizi prioritari

In alcune situazioni, un sito può avere una connessione Internet affidabile e di alta qualità che offre una bassa larghezza di banda, o costi elevati per trasferimenti eccessivi, e un'altra connessione che è veloce ma di minore qualità (maggiore

latenza, più jitter, o meno affidabile). In queste situazioni, i servizi possono essere separati tra le due connessioni Internet per la loro priorità. I servizi ad alta priorità possono includere VoIP, traffico destinato a una rete specifica come un fornitore di applicazioni si sergente esterna, o protocolli specifici utilizzati da applicazioni critiche, tra le altre opzioni. Il traffico a bassa priorità include comunemente qualsiasi traffico consentito che non corrisponda all'elenco del traffico ad alta priorità. Le regole di politica di routing possono essere impostate per indirizzare il traffico ad alta priorità fuori dalla connessione Internet di alta qualità, e il traffico a bassa priorità fuori dalla connessione di minore qualità.

Un altro esempio di uno scenario simile è ottenere una connessione dedicata di Internet per i servizi critici di qualità quale VoIP e che usano soltanto quella connessione per quei servizi.

17.2.3 Solo failover

Ci sono scenari in cui solo l'utilizzo di failover è la migliore pratica. Alcuni utenti Firew4LL hanno una connessione Internet di backup secondaria con un limite di larghezza di banda bassa, come un modem 3G, e vogliono utilizzare tale connessione solo se la loro connessione primaria fallisce, i gruppi Gateway configurati per failover possono raggiungere questo obiettivo.

Un altro utilizzo per il failover è quello di garantire che un certo protocollo o destinazione usi sempre solo una WAN a meno che non vada down.

17.2.4 Bilanciamento del carico dal costo impari

Firew4LL può ottenere un bilanciamento del carico dal costo impari impostando pesi appropriati sui gateway come discusso in *Peso*. Impostando un peso su un gateway, sarà utilizzato più spesso in un gruppo di gateway. I pesi possono essere impostati da *1* a *30*.

Tabella 1: Bilanciamento del carico dal costo impari

peso WAN_GW	peso WAN2_GW	carico WAN	carico wan2
3	2	60%	40%
2	1	67%	33%
3	1	75%	25%
4	1	80%	20%
5	1	83%	17%
5	1	83%	17%
30	1	97%	3%

Si noti che questa distribuzione bilancia strettamente il numero di *connessioni*, non prende in considerazione il throughput dell'interfaccia. Questo significa che l'utilizzo della larghezza di banda non sarà necessariamente distribuito allo stesso modo, anche se nella maggior parte degli ambienti funziona per essere approssimativamente distribuito come configurato nel tempo. Ciò significa anche che se un'interfaccia è caricata alla sua capacità con una singola connessione ad alta velocità, le connessioni aggiuntive saranno ancora dirette a quell'interfaccia.

17.3 Avvertenze e considerazioni sulle WAN multiple

Questa sezione contiene gli avvertimenti e le considerazioni specifiche per multiWAN in Firew4LL.

17.3.1 WAN multiple che condividono un singolo IP del gateway

A causa del modo in cui pf gestisce le connessioni multiWAN, il traffico può essere diretto solo utilizzando l'indirizzo IP del gateway di un circuito, che va bene per la maggior parte degli scenari. Se il firewall ha più connessioni sullo stesso ISP utilizzando lo stesso indirizzo IP della sottorete e del gateway, come è comune quando si utilizzano più modem via cavo, un dispositivo NAT intermedio deve essere utilizzato su tutti tranne uno di essi in modo che Firew4LL veda ogni gateway WAN come un indirizzo IP unico.

Quando si utilizza il dispositivo NAT, può essere configurato per inoltrare tutto il traffico indietro a Firew4LL che può aiutare con l'utilizzo di tale WAN per altri servizi. Tuttavia, alcuni protocolli, come VoIP, avranno problemi se usano una WAN con NAT in tale configurazione.

Se possibile, contattare l'ISP e far configurare i circuiti WAN in modo che siano in sottoreti diverse con gateway diversi.

Un'eccezione a questo è una WAN di tipo PPP come PPPoE. Le WAN di tipo PPP sono in grado di avere lo stesso gateway su più interfacce, ma ogni voce del gateway deve essere configurata per utilizzare un indirizzo IP da monitorare diverso (vedere *IP da monitorare*).

17.3.2 Molteplici WAN PPPoE

Quando sono presenti più linee PPPoE dello stesso ISP e l'ISP supporta Multi-link PPPoE (MLPPP), può essere possibile legare le linee in un unico collegamento aggregato. Questo collegamento incollato ha una larghezza di banda totale pari a tutte le linee insieme come fossero una singola WAN vista da Firew4LL. La configurazione di MLPPP è coperta in *Multi-link Pppoe (MLPPP)*.

17.3.3 Servizi locali e MultiWAN

Ci sono alcune considerazioni sui servizi locali e le multiWAN, dal momento che qualsiasi traffico avviato dal firewall stesso non sarà influenzato dalla politica di routing configurata sulle regole di interfaccia interna. Il traffico proveniente dal firewall stesso segue sempre la tabella di routing del sistema. Quindi, in alcune circostanze, sono necessari percorsi statici quando si utilizzano interfacce WAN aggiuntive, altrimenti si userebbe solo l'interfaccia WAN con il gateway predefinito.

Nel caso di traffico avviato su Internet destinato per una qualsiasi interfaccia WAN, Firew4LL utilizza automaticamente l'opzione *reply-to* di pf direttiva in tutte le regole di interfaccia di tipo WAN, che assicura che il traffico di risposta sia indirizzato indietro fuori la corretta interfaccia WAN.

Risolutore DNS

Le impostazioni predefinite per il risolutore del DNS richiedono la **commutazione del gateway predefinito** per funzionare correttamente con Multi-wan. Vedere *Commutazione del gateway predefinito* per i dettagli. In alternativa all'utilizzo del gateway di default, è possibile apportare alcune modifiche per rendere il risolutore del DNS più adatto alle Multi-wan, compresa l'abilitazione della modalità di inoltro. I dettagli sono descritti più avanti in questo capitolo.

DNS Forwarder

I server DNS utilizzati dallo forwarder del DNS devono avere gateway definiti se utilizzano un'interfaccia WAN OPT, come descritto più avanti in questo capitolo. Non ci sono altri avvertimenti per il forwarder del DNS in ambienti con WAN multiple.

DNS dinamico (DynDNS)

Le voci Dyndns possono essere impostate usando un gruppo di gateway per la loro interfaccia. Questo sposterà una voce Dyndns tra le WAN in modalità failover, consentendo a un host pubblico di passare da una WAN all'altra in caso di guasto.

IPsec

Ipsec è completamente compatibile con le multiWAN. Viene aggiunto automaticamente un percorso statico per l'indirizzo peer del tunnel remoto che punta al gateway della WAN specificato per garantire che il firewall invii il traffico fuori dal percorso corretto quando si avvia una connessione. Per le connessioni mobili, il client avvia sempre la connessione e il traffico di risposta è correttamente instradato dalla tabella di stato.

Un tunnel Ipsec può anche essere impostato utilizzando un gruppo di gateway come interfaccia per failover. Questo è discusso ulteriormente in *Ambienti con WAN multiple*.

OpenVPN

Le funzionalità multiWAN di OpenVPN sono descritte in *OpenVPN e MultiWAN*. Come Ipsec, si può utilizzare qualsiasi WAN o gruppo di gateway.

CARP e multiWAN

CARP è una multiWAN, purché tutte le interfacce WAN utilizzino indirizzi IP statici e ci siano almeno tre indirizzi IP pubblici disponibili per WAN. Questo è coperto in *Multi-wan con HA*.

17.3.4 IPv6 e multiWAN

Ipv6 è anche in grado di funzionare con capacità multiWAN, ma di solito richiede la traduzione dei prefissi di rete (NPt) su una o più WAN. Questo è trattato più in dettaglio in *Multi-wan per Ipv6*.

17.4 Riepilogo dei requisiti delle MultiWAN

Prima di coprire la maggior parte delle specifiche multiWAN, ecco un breve riepilogo dei requisiti per realizzare una configurazione multiWAN completamente implementata:

- Creare un gruppo di gateway in **Sistema>Routing** nella scheda **Gruppi**
- Configurare il risolutore o il forwarder del DNS per Multi-wan, iniziando ad impostare almeno un server del DNS unico per ogni gateway della WAN in **Sistema>Configurazione generale**
- Usare il gruppo di gateway sulle regole del firewall della LAN

17.5 Bilanciamento del carico e failover con I gruppi di gateway

> Un gruppo di gateway è necessario per impostare una configurazione di bilanciamento del carico o failover. Il gruppo stesso non fa intraprendere alcuna azione, ma quando il gruppo viene utilizzato in seguito, come nelle regole del firewall della politica di routing, definisce come gli elementi che utilizzino il gruppo si comporteranno.

Lo stesso gateway può essere incluso in più gruppi in modo che diversi scenari possano essere configurati allo stesso tempo. Per esempio, un po" di traffico può essere bilanciato dal carico, e altro traffico può utilizzare il failover, e la stessa WAN può essere utilizzata in entrambe le capacità utilizzando diversi gruppi di gateway.

Un esempio molto comune di configurazione per due firewall WAN contiene tre gruppi:

- Bilanciamento del carico - Gateway per WAN1 e WAN2 entrambe sul livello 1
- Wan preferita 1 - Gateway per WAN1 sul livello 1 e WAN2 sul livello 2
- Wan preferita 2 - Gateway per WAN1 sul livello 2 e WAN2 sul livello 1

17.5.1 Configurazione di un gruppo di gateway per il bilanciamento del carico o il failover

Per creare un gruppo di gateway per il bilanciamento del carico o il failover:

- Andare a **sistema>Routing**, scheda **Gruppi**
- Fare clic su **Aggiungere** per creare un nuovo gruppo di gateway
- Inserire le opzioni nella pagina come necessario:

  Nome del gruppo Un nome per il gruppo gateway. Il nome deve avere una lunghezza inferiore a 32 caratteri e può contenere solo lettere a-z, cifre da 0 a 9 e un trattino basso. Questo sarà il nome usato per riferirsi a questo gruppo di gateway nel campo **Gateway** nelle regole del firewall. Questo campo è obbligatorio.

  Livello (Tier) Scegliere la priorità per i gateway all'interno del gruppo. All'interno dei gruppi di gateway, i gateway sono organizzati in Livelli. I livelli sono numerati da *1* a *5*, e vengono usati **prima** i numeri **più bassi.** Ad esempio, i gateway del *Tier 1* vengono utilizzati prima dei gateway del *Tier 2*, e così via. Vedere le sezioni seguenti per maggiori dettagli su come utilizzare i Livelli.

  IP virtuale Opzionalmente specifica un indirizzo IP virtuale da utilizzare per un'interfaccia, se presente. Questa opzione viene utilizzata per funzioni come OpenVPN, consentendo di scegliere un indirizzo virtuale specifico, piuttosto che utilizzare solo l'indirizzo dell'interfaccia direttamente quando un gateway specifico è attivo nel gruppo. Nella maggior parte dei casi, questo viene lasciato al valore predefinito dell'Indirizzo di interfaccia.

  Livello di attivazione (Trigger) Decide quando contrassegnare un gateway come inferiore.

  Membro down Segna il gateway come down solo quando è completamente inattivo, dopo una o entrambe le soglie superiori configurate per il gateway. Questo causa il peggior tipo di guasti, quando il gateway è completamente insensibile, ma può perdere i problemi minori con un circuito che può renderlo inutilizzabile molto prima che il gateway raggiunga quel livello.

  Perdita di pacchetti Segna il gateway come down quando la perdita di pacchetti supera la soglia di allarme inferiore (vedere *Soglie della perdita di pacchetti*).

  Alta latenza Segna il gateway come down quando la latenza supera la soglia di allarme inferiore (vedere *Soglie di latenza*).

  Perdita o latenza elevata dei pacchetti Segna il gateway come down per entrambi i tipi di allerta.

  Descrizione Testo che descrive lo scopo di questo gruppo di gateway.

Bilanciamento del carico

Due gateway sullo stesso livello sono bilanciate. Ad esempio, *se Gateway A*, *Gateway B* e *Gateway C* sono tutti del Tier 1, le connessioni sarebbero bilanciate tra di loro. I gateway che sono bilanciati dal carico falliscono automaticamente

tra di loro. Quando un gateway fallisce viene rimosso dal gruppo, quindi in questo caso se uno qualsiasi dei gateway A, B, o C è andato down, il firewall bilancerebbe il carico tra i restanti gateway online.

Bilanciamento ponderato

Se due WAN devono essere bilanciate in modo ponderato a causa di differenti quantità di larghezza di banda tra di loro, possono essere sistemati regolando il parametro **Peso** sul gateway come descritto in *Bilanciamento del carico cn costi impari* e *Peso*.

Failover

I gateway su un livello di numero **inferiore** sono preferiti, e se sono down allora vengono utilizzati gateway di un livello di numero superiore. Per esempio, se il *Gateway A* è sul livello 1, il *Gateway B* è sul livello 2 e il *Gateway C* è sul livello 3, allora il *Gateway A* dovrebbe essere utilizzato per primo. Se il *Gateway A* va down, allora il *Gateway B* verebbe usato. Se sia il *Gateway A* che il *Gateway B* sono down, allora il *Gateway C* verrebbe usato.

Scenari complessi/combinati

Estendendo i concetti di cui sopra per il bilanciamento del carico e il failover, molti scenari complicati sono possibili combinando sia il bilanciamento del carico sia il failover. Per esempio, se il *Gateway A* è al Tier 1, e il *Gateway B* e il *Gateway C* sono al Tier 2, poi il *Gateway D* al Tier 3, si verifica il seguente comportamento: il *Gateway A* è preferito da solo. Se il *Gateway A* è inattivo, allora il traffico sarebbe bilanciato tra il *Gateway B* e il *Gateway C*. Se il *Gateway B* o il *Gateway C* dovessero andare down, il gateway online rimanente in quel livello verrebbe ancora utilizzato. Se il *Gateway A*, il *Gateway B* e il *Gateway C* sono fuori uso, il traffico passerà al *Gateway D*.

Qualsiasi altra combinazione di quanto sopra può essere utilizzata, purché possa essere disposta entro il limite di **5** livelli.

17.5.2 Problemi con il bilanciamento del carico

Alcuni siti web memorizzano le informazioni sulla sessione, compreso l'indirizzo IP del client, e se una successiva connessione a quel sito viene deviata da un'interfaccia WAN diversa utilizzando un diverso indirizzo IP pubblico, il sito web non funzionerà correttamente. Questo sta diventando sempre più comune con le banche e altri siti di sicurezza. Il mezzo suggerito per aggirarlo è quello di creare un gruppo di failover e traffico diretto destinato a questi siti al gruppo di failover piuttosto che un gruppo di bilanciamento del carico. In alternativa, eseguire il failover per tutto il traffico HTTPS.

La connessione sticky di pf è ideata per risolvere questo problema, ma è stata storicamente problematica. E "sicura da usare, e dovrebbe alleviarlo, ma c'è anche un lato negativo nell'utilizzare l'opzione sticky. Quando si utilizzano connessioni sticky, un'associazione è tenuta tra l'*indirizzo IP del client* e un dato *gateway*, essa non si trova fuori dalla destinazione. Quando l'opzione delle connessioni sticky è abilitata, un dato client non caricherebbe il bilanciamento delle sue connessioni tra più WAN, ma sarebbe associato a qualsiasi gateway utilizzato per la sua prima connessione. Una volta che tutti gli stati client sono scaduti, il client può uscire da una WAN diversa per la sua connessione successiva, con conseguente nuova accoppiamento gateway.

17.6 Interfaccia e configurazione del DNS

I primi due elementi da configurare per le Multi-wan sono le Interfacce e il DNS.

17.6.1 Configurazione dell'interfaccia

Configurare la WAN primaria come descritto in precedenza nella procedura guidata di configurazione. Quindi, per le interfacce WAN aggiuntive, eseguire le seguenti operazioni:

- Assegnare le interfacce se non esistono ancora
- Visitare la voce del menu Interfacce per ogni WAN aggiuntiva (ad es. Interfacce>OPT1)
- Abilitare l'interfaccia
- Inserire un nome adatto, come WAN2
- Selezionare il tipo di configurazione dell'indirizzo IP desiderato a seconda del tipo di connessione Internet.
- Inserire i dettagli rimanenti per il tipo di WAN. Ad esempio, sulle connessioni IP statiche, inserire l'indirizzo IP, la maschera di sottorete e aggiungere o selezionare un gateway.

17.6.2 Configurazione del server DNS

Se il forwarder del DNS è in uso, o se il resolver DNS verrà utilizzato in modalità di inoltro, Firew4LL deve essere configurato con i server DNS da ogni connessione WAN per garantire che sia sempre in grado di risolvere il DNS. Questo è particolarmente importante se la rete interna utilizza il firewall per la risoluzione del DNS.

Se i server DNS vengono utilizzati solo da una singola WAN, un'interruzione della connessione WAN comporterà un'interruzione completa di Internet indipendentemente dalla configurazione della politica di routing poiché il DNS non funzionerà più.

1. #### Configurazione del risolutore del DNS

   Il risolutore del DNS può funzionare con le WAN multiple ma la configurazione esatta dipende dal comportamento desiderato e dalle impostazioni correnti.

   Se DNSSEC deve essere utilizzato e i server DNS configurati non supportano DNSSEC, allora la modalità di inoltro non può essere abilitata. Può ancora funzionare con MultiWAN ma richiede la **commutazione del gateway predefinito**. Vedere *Commutazione del gateway predefinito*.

   Se il DNSSEC non è un requisito per questo firewall, o i server DNS configurati supportano DNSSEC, allora si può eseguire la seguente procedura:

- Impostare almeno un server DNS per WAN in **Sistema>Configurazione generale**, come descritto nella sezione successiva.
- Controllare **Abilitare la modalità di inoltro** in **Servizi>Risolutore DNS**
- Deselezionare **Abilitare il supporto DNSSEC** se i server DNS configurati upstream non supportano DNSSEC

17.6.3 Server DNS e route statiche

Quando si utilizza il forwarder DNS o il risolutore DNS in modalità di inoltro, Firew4LL utilizza la sua tabella di routing per raggiungere i server DNS configurati. Ciò significa che senza alcun percorso statico configurato, utilizzerà solo la connessione WAN primaria per raggiungere i server DNS. I gateway devono essere selezionati per ogni server DNS definito sul firewall in modo che Firew4LL utilizzi la corretta interfaccia WAN per raggiungere il server DNS. I server DNS che provengono da gateway dinamici vengono automaticamente reindirizzati al percorso corretto. Se possibile, dovrebbe essere selezionato almeno un gateway da ciascuna WAN.

Per configurare i gateway del server DNS:

- Andare a **Sistema>Configurazione generale**
- Definire almeno un server DNS *unico* per ogni WAN (fino a quattro).
- Per ogni server DNS, selezionare un gateway appropriato in modo da utilizzare una specifica interfaccia WAN

Nota: Lo stesso server DNS non può essere inserito più di una volta. Ogni voce deve essere unica.

La selezione dei gateway per i server DNS è necessaria per diversi motivi. Uno, la maggior parte degli ISP vieta le query ricorsive da parte di host esterni alla propria rete, quindi il firewall deve utilizzare la corretta interfaccia WAN quando accede ai server DNS per uno specifico ISP. In secondo luogo, se la WAN primaria fallisce e il firewall non ha un gateway scelto per uno degli altri server DNS, il firewall perderà tutte le capacità di risoluzione del DNS dal firewall stesso. L'accesso al DNS viene perso in quella situazione perché tutti i server DNS saranno irraggiungibili quando il gateway predefinito è irraggiungibile. Se Firew4LL viene utilizzato come server DNS per la rete locale, ciò si tradurrà in un errore completo del DNS.

Quando si utilizza il Risolutore del DNS con la modalità di inoltro disabilitata, il demone unbound parla direttamente ai server DNS di root e ad altri server DNS autorevoli, il che rende impossibile l'utilizzo di tali rotte statiche e di assegnazioni di gateway. In tal caso, è necessaria la **commutazione del gateway predefinito** in modo che il demone unbound possa mantenere la connettività in uscita.

17.6.4 Scalabilità a un gran numero di interfacce WAN

Ci sono numerosi utenti Firew4LL che distribuiscono 6-12 connessioni Internet su un'unica installazione. Un utente Firew4LL ha 10 linee DSL perché nel suo paese è significativamente più conveniente ottenere dieci connessioni da 256 Kb che una connessione da 2.5 Mb. Questo cliente utilizza Firew4LL per caricare un gran numero di macchine interne su 10 diverse connessioni. Per ulteriori informazioni su questa scala di distribuzione, vedere *MultiWAN su una Stick* più avanti in questo capitolo.

17.7 MultiWAN e NAT

Le regole NAT predefinite generate da Firew4LL tradurranno qualsiasi traffico che lascia un'interfaccia di tipo WAN a quell'indirizzo IP dell'interfaccia. In una configurazione predefinita di due interfacce LAN e WAN, Firew4LL utilizzerà il NAT su tutto il traffico che dalla sottorete LAN lascia l'interfaccia WAN all'indirizzo IP della WAN. L'aggiunta di più interfacce di tipo WAN estende questo comportamento del NAT a qualsiasi traffico che lascia un'interfaccia di tipo WAN a quell'indirizzo IP dell'interfaccia. Tutto questo viene gestito automaticamente a meno che il NAT in uscita manuale non sia abilitato.

Le regole di politica del routing del firewall indirizzano il traffico verso l'interfaccia WAN utilizzata, e le regole in uscita e il NAT 1:1 specificano come il traffico verrà tradotto man mano che lascia quella WAN.

17.7.1 MultiWAN e NAT in uscita manuale

Se il **NAT in uscita manuale** deve essere utilizzato con multiWAN, assicurarsi che le regole NAT siano configurate per tutte le interfacce di tipo WAN.

17.7.2 MultiWAN e Port forward

Ogni port forward si applica ad una singola interfaccia WAN. Una determinata porta può essere aperta su più interfacce WAN utilizzando più voci di inoltro della porta, una per interfaccia WAN. Il modo più semplice per farlo è:

- Aggiungere una port forward sulla prima connessione WAN come di consueto
- Fare clic su  a destra di quella voce per aggiungere un'altra port forward in base a quella selezionata
- Modificare l'**interfaccia** sulla WAN desiderata
- Fare clic su **Salvare**

La parola chiave della reply-to in pf, utilizzata sulle regole di interfaccia di tipo WAN, assicura che quando il traffico arriva su una specifica interfaccia WAN, il traffico di ritorno tornerà indietro nel modo in cui è entrato nel firewall. Quindi gli inoltri di porta possono essere utilizzati attivamente su tutte le interfacce WAN in qualsiasi momento, indipendentemente da qualsiasi configurazione di failover presente. Questo è particolarmente utile per i server di posta, in quanto un indirizzo su una WAN secondaria può essere utilizzato come MX di backup, consentendo al sito di ricevere posta anche quando la linea principale è inattiva. Questo comportamento è configurabile, per informazioni su questa impostazione, vedere *Disabilitare reply-to*.

17.7.3 MultiWAN e NAT 1:1

Le voci del NAT 1:1 sono specifiche per una singola interfaccia WAN e, come il NAT in uscita, controllano solo ciò che accade al traffico quando esce da un'interfaccia. I sistemi interni possono essere configurati con una voce del NAT 1:1 su ogni interfaccia WAN, o una voce 1:1 su una o più interfacce WAN e utilizzare il NAT di default in uscita su altre. Dove le voci 1:1 sono configurate, sovrascrivono sempre qualsiasi altra configurazione del NAT in uscita per quella specifica interfaccia.

Se un dispositivo locale deve sempre utilizzare una voce del NAT 1:1 su una specifica WAN, allora il traffico da quel dispositivo deve essere costretto a utilizzare quel gateway WAN specifico.

17.8 Configurazione della politica di routing

A questo punto, il firewall è pronto per WAN multiple, ma non sarà ancora utilizzato. Il traffico non fallirà o non sarà caricato in modo bilanciato senza regole di politica di routing del firewall.

Nota: Una possibile eccezione è se la **commutazione del gateway

---

predefinito** è abilitato (*Commutazione del gateway predefinito*), nel qual caso il failover potrebbe ancora funzionare senza politica di routing.

17.8.1 Configurare regole del firewall per la politica di routing

L'impostazione di un **gateway** su una regola del firewall farà sì che il traffico corrispondente alla regola utilizzi il gateway o il gruppo scelto, seguendo il comportamento configurato del gruppo.

Il modo più semplice per configurare un firewall per la politica di routing è quello di modificare la regola di passaggio predefinita per la LAN e selezionare il gruppo di gateway. Con quell'impostazione, tutto il traffico che corrisponde alla regola di passaggio predefinita sul LAN userà il gateway o il gruppo scelto.

Per fare quella modifica:

- Passare a **Firewall>Regole**, scheda **LAN**
- Fare clic su  sulla riga con la regola di passaggio predefinita

- Fare clic su  **Visualizzare avanzate** sotto **opzioni extra**
- Selezionare il gruppo di gateway desiderato dall'elenco a discesa del **Gateway**
- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche**

Solo le distribuzioni più basilari saranno soddisfatte con questa configurazione, la maggior parte delle configurazioni sono più complesse. Continuare a leggere per ulteriori fattori che possono richiedere una configurazione aggiuntiva.

17.8.2 Escludere la politica di routing

Se ci sono altre interfacce locali, VPN, interfacce MPLS o traffico che devono seguire diversamente la tabella di routing del sistema, quindi quel traffico deve essere configurato per bypassare la politica di routing. Questo è semplice da fare creando una regola che corrisponda al traffico in questione e poi mettendo quella regola sopra tutte le regole che hanno un gateway configurato, perché la prima regola da corrisponde è quella che viene utilizzata.

Ciò può essere generalizzato realizzando un alias per tutto il traffico *RFC1918* che coprirebbe tutte le reti riservate ed poi usandolo in una regola. L'alias contiene 192.168.0.0/16, 172.16.0.0/12 e 10.0.0.0/8.

Nella figura *Esempio di aggiramento della politica di routing*, il traffico locale e la VPN bypassano la politica di routing, ol traffico HTTPS preferisce WAN2, e tutto il traffico effettua bilanciamento del carico:

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	0/0 B	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	⚙
☐ ✔	0/0 B	IPv4 *	LAN net	*	RFC1918	*	*	none		Bypass policy routing for local/VPN traffic	⚓✎⧉⊘🗑
☐ ✔ ⚙	0/0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	PreferWAN2	none		Force HTTPS out WAN2, fail to WAN1	⚓✎⧉⊘🗑
☐ ✔ ⚙	0/10 KiB	IPv4 *	LAN net	*	*	*	LoadBalance	none		Load Balance LAN Traffic	⚓✎⧉⊘🗑

Fig. 1: Esempio di aggiramento della politica di routing

17.8.3 Unire failover e bilanciamento del carico

Come mostrato nella figura *Esempio di aggiramento della politica di routing*, il failover e il bilanciamento del carico possono essere utilizzati allo stesso tempo ordinando attentamente le regole su un'interfaccia. Le regole vengono elaborate dall'alto verso il basso e la prima corrispondente vince. Piazzando regole più specifiche in cima alla lista, e le regole generali del tipo "corrispondenza a tutto" in basso, qualsiasi numero di combinazioni diverse è possibile con regole che utilizzano diversi gateway o gruppi.

17.8.4 Forzare l'uso del gateway

Ci sono situazioni in cui il traffico dovrebbe usare solo un gateway e mai il bilanciamento del carico o il failover. In questo esempio, un dispositivo deve uscire solo tramite una specifica WAN e perdere tutta la connettività quando la WAN non riesce.

In primo luogo, impostare il **gateway** su una regola firewall corrispondente al traffico da questo dispositivo a uno specifico gateway WAN. Se quel gateway è inattivo, la regola agirà come se il gateway non fosse stato impostato affatto, quindi devono essere fatti un paio di passi avanti.

Aggiungere una regola immediatamente sotto la regola corrispondente al traffico, e impostare il rifiuto o il blocco. Questa regola non deve avere un gateway impostato.

Successivamente, configurare il firewall per omettere le regole per i gateway che sono inattivi (*Monitoraggio dei gateway*):

- Passare a **Sistema>Avanzate** nella scheda **Varie**
- Selezionare **Non creare regole quando il gateway è inattivo**
- Fare clic su **Salvare**

Con questa opzione abilitata, la prima regola verrà omessa completamente, passando alla regola successiva. In questo modo, quando la prima regola viene omessa automaticamente, il traffico sarà fermato dalla regola di blocco.

17.9 Verificare le funzionalità

Una volta che la multiWAN è stata configurata, la migliore procedura è quindi quella di testare la sua funzionalità per verificare le funzioni come previsto. Le seguenti sezioni descrivono come testare ogni porzione della configurazione della multiWAN.

17.9.1 Testare il failover

Testare la Multi-wan in modo controllato immediatamente dopo la configurazione è un passo chiave nel processo. Non commettere l'errore di aspettare che una connessione a Internet fallisca naturalmente per la prima prova, solo per scoprire i problemi quando sono molto più difficili e stressanti da risolvere.

Innanzitutto, passare a **Stato>Gateway** e assicurarsi che tutti i gateway della WAN siano visualizzati come **Online** sotto **Stato**, nonché nella scheda **Gruppi di gateway**. In caso contrario, verificare che sia utilizzato un indirizzo IP da monitorare corretto come discusso in *IP da monitorare*.

Creare un guasto alla WAN

Esistono diversi modi per simulare un guasto WAN a seconda del tipo di connessione Internet utilizzata. Per qualsiasi tipo, provare prima a scollegare il cavo Ethernet dell'interfaccia WAN di destinazione dal firewall.

Per le connessioni via cavo e DSL, provare a spegnere il modem/CPE, e in un test separato, scollegare la linea coassiale o telefonica dal modem. Per fibre, wireless e altri tipi di connessioni con un router esterno a Firew4LL, provare a scollegare la connessione Internet dal router e anche a spegnere il router stesso.

Tutti gli scenari di prova descritti finiranno probabilmente con lo stesso risultato. Tuttavia, ci sono alcune circostanze in cui provare tutte queste cose individualmente troverà un difetto che altrimenti non sarebbe stato notato fino ad un guasto reale. Uno dei più comuni è usare inconsapevolmente un indirizzo IP da monitorare assegnato al modem DSL o via cavo. Quindi quando la linea coassiale o telefonica è scollegata, simulando un guasto del provider piuttosto che un guasto Ethernet o modem, il ping per il monitoraggio riesce ancora dal momento che è il ping del modem. Da quando a Firew4LL è stato detto di monitorare, la connessione è ancora attiva, quindi non fallirà anche se la connessione upstream è effettivamente inattiva. Ci sono altri tipi di guasto che allo stesso modo possono essere rilevati solo testando tutte le singole possibilità di guasto. L'indirizzo IP da monitorare può essere modificato sulla voce del gateway come indicato nell'*IP da monitorare*.

Verificare lo stato dell'interfaccia

Dopo aver creato un errore nella WAN, aggiornare **Stato>Gateway** per controllare lo stato corrente. Mentre il demone di monitoraggio del gateway nota la perdita, la perdita alla fine passerà oltre le soglie di allarme configurate e sarà contrassegnata come down.

17.9.2 Verificare la funzionalità del bilanciamento del carico

Questa sezione descrive come verificare le funzionalità di una configurazione di bilanciamento del carico.

Verificare il bilanciamento del carico con HTTP

Il modo più semplice per verificare il bilanciamento del carico con HTTP è visitare un sito web che visualizza l'indirizzo IP pubblico utilizzato dal client per accedere al sito. Una pagina sul sito Firew4LL è disponibile per questo scopo, e innumerevoli altri siti offrono la stessa funzionalità. Cercare "qual è il mio indirizzo IP" e verranno restituiti numerosi siti web che mostreranno l'indirizzo IP pubblico facendo la richiesta a HTTP. Molti di questi siti tendono ad essere pieni di annunci spammy, in modo da fornire un paio di siti che semplicemente segnalano l'indirizzo IP del cliente:

- *https://www.netgate.com/ip*
- *https://www.pfsense.org/ip*
- *https://files00.netgate.com/ip*
- *https://files01.netgate.com/ip*

I browser hanno l'abitudine di mantenere aperte le connessioni al server e i risultati sulla cache, quindi il miglior test basato sul browser è quello di caricare più siti, o di chiudere la finestra del browser tra i tentativi di caricare un sito. Durante ogni tentativo di connessione, dovrebbe essere mostrato un indirizzo IP diverso se il bilanciamento del carico funziona correttamente. Se nella rete è presente altro traffico, l'indirizzo IP potrebbe non essere modificato ad ogni caricamento di pagina. Ripetere il test più volte e l'indirizzo IP dovrebbe cambiare almeno un paio di volte.

Se l'indirizzo IP non cambia mai, provare diversi siti, e assicurarsi che il browser stia davvero richiedendo la pagina di nuovo, e non restituisca qualcosa dalla sua cache o utilizzando una connessione persistente al server. Cancellare manualmente la cache, chiudere e riaprire il browser, e provare più browser web sono buone cose da provare prima di risolvere ulteriormente i problemi della configurazione del bilanciamento del carico.

Usare curl come descritto in *Verificare il bilanciamento del carico* è un test migliore in quanto garantisce che la cache e le connessioni persistenti non avranno alcun impatto sui risultati.

Testare il bilanciamento del carico con traceroute

L'utilità `traceroute` (o `tracert` in Windows) mostra il percorso di rete preso per una data destinazione. Vedere *Utilizzo di traceroute* per i dettagli sull'utilizzo di traceroute. Con il bilanciamento del carico, l'esecuzione di un traceroute da un sistema client dietro il firewall dovrebbe mostrare un percorso preso diverso per ogni tentativo. A causa delle funzioni di traceroute, attendere almeno un minuto dopo aver fermato un traceroute prima di iniziare un altro test in modo che gli stati scadano, o provare diverse destinazioni ad ogni tentativo.

Utilizzare i grafici del traffico

I grafici del traffico in tempo reale sotto **Stato>Grafico del traffico** e sul widget della dashboard dei grafici del traffico sono utili per mostrare il flusso in tempo reale sulle interfacce WAN. Solo un grafico alla volta può essere visualizzato per finestra del browser quando si utilizza **Stato>Grafico del traffico**, ma ulteriori finestre o schede possono essere aperte nel browser per vedere tutte le interfacce WAN contemporaneamente. Il widget del grafico del traffico per la dashboard consente la visualizzazione simultanea di grafici di traffico multipli su una singola pagina per semplificare questo processo. Se il bilanciamento del carico funziona correttamente, l'attività sarà osservata su tutte le interfacce WAN.

I grafici del traffico RRD in **Stato>Monitoraggio** sono utili per la valutazione storica e a lungo termine dell'utilizzo della WAN.

Nota: L'utilizzo della larghezza di banda può non essere esattamente distribuito in modo uguale, poiché le connessioni sono semplicemente dirette su una base round robin senza tenere conto dell'utilizzo della larghezza di banda.

17.10 Risoluzione dei problemi

Questa sezione descrive alcuni dei problemi più comuni con multiWAN e come risolverli.

17.10.1 Verificare la configurazione della regola del firewall

L'errore più comune durante la configurazione multiWAN sono le regole del firewall improprie. Ricordare, la prima regola corrispondente vince e qualsiasi altra regola viene ignorata. Se una regola di politica del routing è al di sotto della regola LAN predefinita nell'elenco, nessun traffico corrisponderà mai a quella regola perché prima corrisponderà alla regola LAN predefinita. Rivedere *Configurazione della politica di routing* e verificare che le regole siano corrette.

Se l'ordinamento e la configurazione delle regole appaiono corretti, può aiutare abilitare l'accesso alle regole. Vedere *Risoluzione dei problemi con le regole del firewall* per la per maggiori informazioni. Assicurarsi che la regola di politica del routing sia quella di far passare il traffico.

17.10.2 La politica di routing non funziona per il traffico web o tutto il traffico

Quando un pacchetto proxy che può catturare in modo trasparente il traffico HTTP viene utilizzato, come squid, sovrascrive qualsiasi politica di routing definita per il traffico client su quella porta. Quindi non importa quale gateway è impostato nelle regole del firewall, il traffico per HTTP (porta TCP 80) continuerà a passare attraverso squid e seguire il percorso predefinito del firewall.

17.10.3 Il failover non funziona

Se si verificano problemi quando una connessione Internet non riesce, in genere è perché l'indirizzo IP da monitorare sta ancora rispondendo, quindi il firewall pensa che la connessione sia ancora disponibile. Controllare **Stato>Gateway** per verificare. Un indirizzo IP sul modem può essere utilizzato come indirizzo IP da monitorare, che sarà comunque accessibile anche se la connessione Internet è disattivata.

17.10.4 Il bilanciamento del carico non funziona

- Controllare che il Gruppo di Gateway sia configurato correttamente per il bilanciamento del carico, con almeno due gateway sullo stesso livello.
- Controllare che le regole del firewall siano corrispondenti al traffico diretto al gruppo di gateway per il bilanciamento del carico.
- Controllare che tutti i gateway del gruppo siano visualizzati come Online in **Stato>Gateway**. Le connessioni contrassegnate come Offline non saranno utilizzate.
- Controllare la metodologia di test. Piuttosto che il test con un browser web, provare con curl come descritto in *Verificare il bilanciamento del carico*.
- Controlla che il traffico non stia usando un proxy o sia altrimenti avviato da un demone sul firewall stesso.

17.10.5 Il gateway viene segnalato erroneamente offline

Se un gateway è elencato come offline, ma la WAN è in realtà attiva, diverse cose potrebbero essere in errore:

- In primo luogo, verificare se l'indirizzo IP da monitorare risponde a un ping da un dispositivo client sulla LAN, e di nuovo da **Diagnostica>Ping**.
- Se il dispositivo con l'indirizzo IP da monitorare o un altro hop intermedio rilascia i pacchetti di richiesta di eco ICMP senza un payload, i ping manuali funzionerebbero ma il monitoraggio del gateway fallirebbe. Vedere *Payload dei dati* e impostare il carico utile a un valore pari o superiore a 1.
- Se il gateway o l'indirizzo IP da monitorare non risponde alle richieste di eco ICMP, inserire un indirizzo IP da monitorare diverso da usare.
- Se l'indirizzo IP da monitorare è configurato come server DNS per una WAN diversa, i percorsi statici potrebbero causare un conflitto e le richieste di eco al gateway potrebbero non seguire il percorso previsto. Impostare un indirizzo IP da monitorare non in conflitto sul gateway.
- Se c'è una regola NAT in uscita sulla WAN con una fonte come *qualsiasi*, si possono causare problemi con il traffico sul firewall, compreso il monitoraggio del traffico, perché anche quello userà il traffico NAT dal firewall stesso. Questo può essere particolarmente problematico se l'indirizzo sorgente viene cambiato in un VIP CARP. Fissare il NAT in uscita.

Se tutto il resto fallisce, è possibile che il circuito sia davvero down, ma la metodologia di test sembra dimostrarlo. Verificare le impostazioni dell'interfaccia e del gateway ed eseguire nuovamente il test, e provare traceroute per assicurarsi che il traffico in uscita stia utilizzando il percorso previsto.

17.10.6 Il ping funziona dall'indirizzo IP, ma la navigazione web non riesce

In questo caso, la causa più probabile è il DNS. Se le impostazioni DNS del firewall non corrispondono a quelle di *Interfaccia e configurazione DNS*, i client potrebbero non essere in grado di risolvere il DNS quando una WAN è inattiva. Rivedere le impostazioni e risolvere gli eventuali problemi che si trovano.

17.11 MultiWAN su uno stick

Nel mondo dei router, Cisco e altri si riferiscono a un router VLAN come a "un router su uno stick", in quanto può essere un router funzionante con una sola connessione di rete fisica. Anche Firew4LL può essere configurato in questo modo, utilizzando le VLAN e uno switch gestito in grado di eseguire trunking 802.1q. La maggior parte delle distribuzioni con più di 5 WAN utilizza questa metodologia per limitare il numero di interfacce fisiche richieste sul firewall. In una tale distribuzione, le interfacce WAN risiedono tutte su un'interfaccia fisica sul firewall, con la rete(i) interna(e) su interfacce fisiche aggiuntive. La figura *Multi-wan su uno stick* illustra questo tipo di distribuzione.

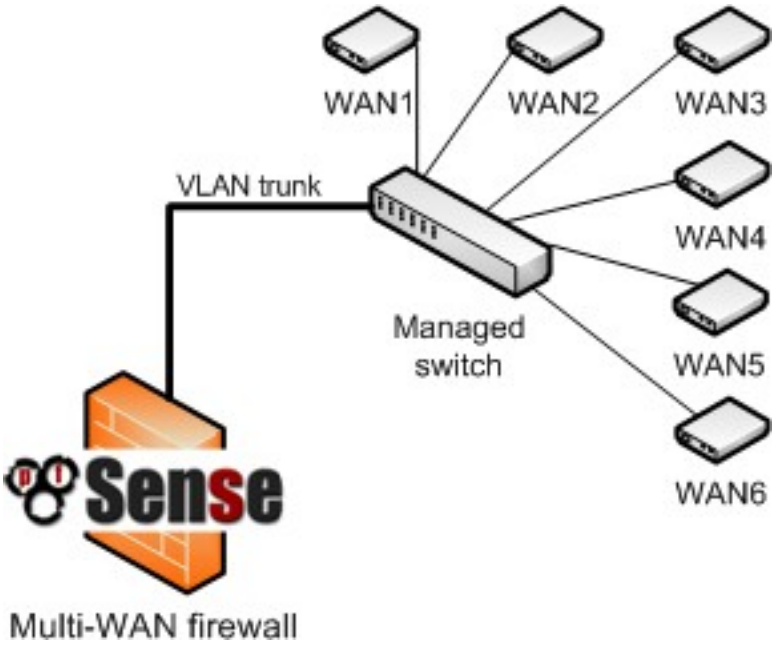


Fig. 2: MultiWAN su uno stick

17.12 MultiWAN per IPv6

Le WAN multiple possono essere utilizzate con Ipv6 a condizione che il firewall sia collegato a più ISP o ai tunnel con indirizzi statici.

Vedi anche:

Vedere *Collegamento con un servizio di intermediazione del tunnel* per assistenza nella creazione di un tunnel.

I gruppi gateway funzionano allo stesso modo per Ipv6 e per Ipv4, ma le famiglie di indirizzi non possono essere mescolate all'interno di un gruppo. Un gruppo deve contenere *solo* gateway Ipv4 o *solo* gateway Ipv6.

In tutta questa sezione "Seconda WAN" si riferisce alla seconda interfaccia o interfaccia aggiuntiva con la connettività Ipv6. Può essere un'interfaccia reale che ha connettività nativa, o un'interfaccia tunnel quando si utilizza un intermediario del tunnel.

17.12.1 Avvertenze

Nella maggior parte dei casi, il NAT non viene utilizzato con l'Ipv6 in quanto tutto viene instradato. Questo è ottimo per la connettività e per le imprese o luoghi che possono permettersi un spazio di indirizzo indipendente del fornitore (Provider Indipendent, PI) e un peering BGP, ma non funziona in pratica per le piccole imprese e gli utenti domestici.

La traduzione dei prefissi di rete (NPt) consente di utilizzare una sottorete per la LAN che ha piena connettività tramite la sua WAN nativa, ma ha anche tradotto la connettività sulle WAN aggiuntive in modo che sembrasse provenire da lì. Sebbene non ci sia vera connettività per la sottorete LAN tramite i percorsi alternativi, è meglio che non vi sia alcuna connettività se la WAN primaria è inattiva.

Avvertimento: Questo non funziona per tipi di IPv6 dinamici dove la sottorete non è statica, come DHCP6-PD

17.12.2 Requisiti

Per configurare Multi-wan per Ipv6 il firewall deve avere:

- Connettività Ipv6 con indirizzi statici su due o più WAN
- Gateway aggiunti a **System>Routing** per entrambe le WAN Ipv6, e connettività confermata su entrambe.
- Un /64 instradato da ogni provider/percorso
- LAN che utilizzi un /64 statico instradato o simile

17.12.3 Setup

La configurazione per MultiWAN Ipv6 è molto vicina alla configurazione per Ipv4. La differenza principale è che usa NPt invece di NAT.

Per prima cosa, in **Sistema>Routing** nella scheda **Gruppi di gateway**, aggiungere Gruppi di gateway per i gateway Ipv6, con i livelli impostati come desiderato. Questo funziona in modo identico per Ipv4.

Successivamente, passare a **Sistema>Generale** e impostare un server DNS Ipv6 impostato per ogni WAN Ipv6, in maniera identica anche per Ipv4.

Ora aggiungere una voce NPt in **Firewall>NAT** nella scheda **NPt**, usando le seguenti impostazioni:

Interfaccia WAN secondaria (o tunnel se si utilizza un intermediario)

Prefisso Ipv6 interno La sottorete *LAN* Ipv6

Prefisso Ipv6 di destinazione La seconda sottorete IPv6 instradata su WAN

Nota: Questo non è il /64 dell'interfaccia WAN stessa - è il /64

---

instradato al firewall su quella WAN attraverso l'upstream.

Ciò che fa è simile al NAT 1:1 per l'Ipv4, ma per l'intera sottorete. Quando il traffico lascia la seconda WAN, se proviene dalla sottorete LAN, sarà tradotto nell'indirizzo IP equivalente nell'altra sottorete.

Per esempio se il firewall ha 2001:xxx:yyy::/64 su LAN, e 2001:aaa:bbb::/64 sulla seconda WAN, allora 2001:xxx:yyy::5 apparirebbe come 2001:aaa:bbb::5 se il traffico esce dalla seconda WAN. Per ulteriori informazioni su NPt, vedere *Traduzione dei prefissi di rete Ipv6 (NPt)*.

Come per Ipv4, i Gruppi di Gateway devono essere utilizzati sulle regole del firewall LAN. Modificare le regole LAN per il traffico Ipv6 e impostarle usando il gruppo di gateway, assicurandoti di avere regole per le sottoreti/VPN direttamente connesse senza un set di gateway in modo che non siano indirizzate alla politica di routing.

17.12.4 Tattiche alternative

Alcuni utenti preferiscono configurare la LAN con una sottorete Ipv6 privata dallo spazio fc00:/7 e configurare NPt per entrambe le WAN.

17.13 Multi-Link PPPoE (MLPPP)

Multi-link PPPoE (MLPPP) è un'opzione WAN unica in grado di collegare più linee PPPoE dallo stesso ISP per formare un circuito virtuale più grande. Ciò significa che un firewall può ottenere la vera larghezza di banda aggregata

di tutti i circuiti del pacchetto. Ad esempio, se un firewall ha tre linee DSL da 5 Mbit/s in un bundle, potrebbe potenzialmente ottenere 15Mbit/s da una singola connessione.

17.13.1 Requisiti

Il più grande ostacolo per MLPPP è che l'ISP deve supportarlo sui circuiti collegati al firewall. Pochi ISP sono disposti a sostenere MLPPP, quindi se un ISP è disponibile a farlo, varrebbe la pena approfittarne. Inoltre, ogni linea deve trovarsi su un'interfaccia separata collegata a Firew4LL.

17.13.2 Setup

La configurazione per MLPPP è molto semplice:

- Configurare una WAN per una singola linea con le credenziali corrette
- Passare a **Interfacce>Assegnare**, scheda **PPPs**
- Fare clic su  per modificare la voce per WAN PPPoE
- Usare Ctrl-click per selezionare le altre interfacce fisiche che appartengono allo stesso pacchetto MLPPP
- Fare clic su **Salvare**

Firew4LL tenterà di legare le linee usando MLPPP.

17.13.3 Avvertenze

Un lato negativo dell'utilizzo di MLPPP è che la risoluzione dei problemi è molto più difficile. Le statistiche e lo stato non sono disponibili per le singole linee. Per determinare lo stato, leggere il registro PPP, in quanto non c'è ancora un modo per interrogare le linee separatamente. In alcuni casi è ovvio che se una linea è down, ci può essere un problema notevole al modem (fuori sincrono) o la larghezza di banda massima raggiungibile è ridotta.

Le molteplici funzionalità WAN (multiWAN) di Firew4LL consentono a un firewall di utilizzare più connessioni Internet per ottenere una connettività più affidabile e una maggiore capacità di throughput. Prima di procedere con una configurazione multiWAN, il firewall deve avere una configurazione funzionale a due interfacce (LAN e WAN). Firew4LL è in grado di gestire molte interfacce WAN, con implementazioni multiple che utilizzano 10-12 WAN in produzione. Aumenterà ancora di più, anche se non siamo a conoscenza di installazioni che utilizzano più di 12 WAN.

Tutte le interfacce di tipo WAN sono trattate in modo identico nella GUI. Tutto ciò che può essere fatto con la WAN primaria può essere fatto anche con un'interfaccia WAN OPT aggiuntiva. Non vi sono differenze significative tra la WAN primaria e le WAN aggiuntive.

Questo capitolo inizia coprendo gli elementi da considerare quando si implementa una *qualsiasi* soluzione multiWAN, quindi copre la configurazione multiWAN con Firew4LL..

17.14 Scegliere la connettività Internet

La scelta ideale della connettività Internet dipenderà in gran parte dalle opzioni disponibili in una data località, ma ci sono alcuni fattori aggiuntivi da prendere in considerazione.

17.14.1 Percorsi dei cavi

Parlando dall'esperienza di coloro che hanno visto in prima persona gli effetti di molteplici terne in ricerca di cavi, così come i nefasti ladri di rame, è molto importante assicurarsi che le scelte di connettività per una distribuzione multiWAN utilizzino percorsi di cablaggio disparati. In molte località, le connessioni DSL così come tutte le altre che utilizzano coppie di rame sono trasportate su un singolo cavo soggetto allo stesso taglio del cavo, e altre dallo stesso telco come i circuiti in fibra che possono funzionare lungo gli stessi poli o condotti.

Se una connessione entra in una coppia di rame (DSL), scegliere una connessione secondaria che utilizzi un diverso tipo e percorso di cablaggio. Le connessioni via cavo sono in genere l'opzione più ampiamente disponibile non soggetta alla stessa interruzione dei servizi in rame. Altre opzioni includono il servizio in fibra o wireless fisso in arrivo su un percorso diverso dai servizi in rame.

Due connessioni dello stesso tipo non possono essere invocate per fornire ridondanza nella maggior parte dei casi. Un guasto ISP o un taglio del cavo comunemente abbatte tutte le connessioni dello stesso tipo. Alcuni utenti Firew4LL utilizzano più linee DSL o modem via cavo multipli, anche se l'unica ridondanza che tipicamente offre è isolare un sito dal modem o altri guasti CPE (Attrezzatura iniziale del cliente, Customer Premise Equipment). Considerare connessioni multiple dello stesso provider come una soluzione solo per una larghezza di banda aggiuntiva, in quanto la ridondanza offerta da una distribuzione è minima.

17.14.2 Percorsi per Internet

Un'altra considerazione quando si seleziona la connettività Internet per un sito è il percorso dalla connessione stessa a Internet. Per motivi di ridondanza, non si dovrebbe fare affidamento su connessioni Internet multiple dello stesso provider, soprattutto dello stesso tipo, in quanto potrebbero fallire tutte contemporaneamente.

Con i fornitori più grandi, due diversi tipi di connessioni come una linea fibra e DSL di solito attraversano reti completamente diverse fino a raggiungere parti centrali della rete. Questi componenti della rete centrale sono generalmente progettati con elevata ridondanza e tutti i problemi sono affrontati rapidamente poiché hanno effetti diffusi. Quindi tale connettività è isolata dalla maggior parte dei problemi ISP, ma dal momento che comunemente utilizzano lo stesso percorso del cavo, lascia ancora un sito vulnerabile a interruzioni prolungate dei cavi.

17.14.3 Migliore ridondanza, maggiore larghezza di banda, meno soldi

In passato, i servizi telco di alta qualità come i circuiti DS1 o DS3 erano la scelta per ambienti con requisiti di disponibilità elevati. Generalmente gli accordi sul livello dei servizi (Service Level Agreements, SLA) offerti sulle connessioni DS1 e DS3 erano migliori di altri tipi di connettività, e questi circuiti erano generalmente considerati più affidabili. Tuttavia, gli utenti finali hanno in gran parte lasciato indietro tali circuiti, perché sono troppo lenti o troppo costosi secondo gli standard attuali. Con le funzionalità multiWAN su Firew4LL, un sito può avere più larghezza di banda e una migliore ridondanza per meno soldi in molti casi. I servizi in fibra stanno rapidamente diventando più diffusi, scuotendo questo concetto fornendo quantità estremamente grandi di larghezza di banda per costi relativamente bassi, anche se tali servizi possono ancora avere un SLA meno desiderabile per la risposta di interruzione.

La maggior parte delle organizzazioni che richiedono connessioni Internet ad alta disponibilità non vogliono fare affidamento su connessioni Internet DSL, via cavo o altre connessioni Internet a banda larga di classe inferiore. Mentre di solito sono significativamente più veloci e più economici, il minore SLA è sufficiente per fare in modo che molte aziende si attengano alla connettività DS1 o DS3. Nelle aree in cui sono disponibili più opzioni a banda larga a basso costo, come DSL e cavo, la combinazione di Firew4LL e due connessioni Internet a basso costo fornisce maggiore larghezza di banda e una migliore ridondanza a un costo inferiore. La possibilità che due diverse connessioni a banda larga vadano down simultaneamente è significativamente inferiore alla possibilità di qualsiasi interruzione del servizio. L'aggiunta di un cavo di backup o di una linea DSL per integrare una linea di fibra molto più veloce assicura che la connettività continuerà quando un'interruzione si verifica sulla linea di fibra, anche se è un evento raro.

CAPITOLO 18

VPN - Virtual Private Network

18.1 IPSec

18.1.1 IPsec e IPv6

IPsec è in grado di connettersi a un tunnel su indirizzi peer con IPv4 o IPv6 di fase 1, ma con IKEv1 il tunnel può contenere solo lo stesso tipo di traffico all'interno della definizione della fase 2 del tunnel che viene utilizzato per superare il traffico all'esterno del tunnel. Ciò significa che, anche se IPv4 o IPv6 possono essere trasportati all'interno del tunnel, per utilizzare il traffico IPv6 all'interno del tunnel deve essere collegato tra indirizzi IP peer con IPv6, non IPv4. In altre parole, la famiglia dell'indirizzo interno ed esterno deve corrispondere, non possono essere mescolati.

Come per la maggior parte delle altre carenze di IKEv1, questo problema è stato affrontato in IKEv2. I tunnel che utilizzano IKEv2 possono trasportare entrambi i tipi di traffico, indipendentemente dal protocollo utilizzato per creare il tunnel esterno. Con IKEv2, i client di dispositivi mobili possono anche utilizzare sia IPv4 che IPv6, a condizione che il client lo supporti.

18.1.2 Scegliere le opzioni di configurazione

IPsec offre numerose opzioni di configurazione, che influenzano le prestazioni e la sicurezza delle connessioni IPsec. Realisticamente, per un uso di banda da bassa a moderata, importa poco quali opzioni sono scelte qui finché non viene utilizzato il DES e viene definita una forte chiave pre-condivisa, A meno che il traffico protetto non sia così prezioso che un avversario non sia disposto a investire molti milioni di dollari di potenza di elaborazione per rompere la crittografia IPsec. Anche in questo caso, c'è probabilmente un modo più facile e molto più economico per entrare nella rete e ottenere lo stesso risultato finale (ingegneria sociale, per esempio). Le prestazioni sono il fattore più importante per molti, e nei casi in cui questa è una preoccupazione, è necessaria più cura quando si crea una configurazione.

Impostazioni della fase 1 (Phase1)

Le impostazioni qui controllano la fporzione di negoziazione della fase 1 del tunnel, come descritto in precedenza.

Abilitare/disabilitare il tunnel

La casella di controllo **Disattivato** controlla se questo tunnel (e le relative voci di fase 2 associate) sono attivi e utilizzati.

Versione Key Exchange

Il selettore **Versione Key Exchange** controlla se il tunnel userà la versione 1 (V1) o la versione 2 (V2) di IKE. IKEv2 è una versione più recente di IKE che è auspicabile per molti motivi. Le differenze sono discusse in *IKE*. Nella maggior parte dei casi, IKEv1 verrà utilizzato a meno che entrambe le parti non supportino correttamente IKEv2.

Protocollo Internet

Il selettore **protocollo di Internet** imposta il protocollo per l'*esterno* del tunnel. Cioè, il protocollo che verrà utilizzato tra gli indirizzi peer esterni. Per la maggior parte, questo sarà *IPv4*, ma se entrambe le estremità sono in grado di supportare Ipv6, che può essere utilizzato altrimenti. Il protocollo scelto sarà utilizzato per convalidare il gateway remoto e gli identificatori associati.

Nota: Un tunnel che utilizza IKEv1 può portare solo lo stesso traffico di protocollo nella fase 2 come è stato usato per la fase 1. Ad esempio, gli indirizzi peer IPv4 limitano la fase 2 solo alle reti IPv4. Un tunnel che utilizza IKEv2 può trasportare sia il traffico IPv4 che quello IPv6 contemporaneamente nella fase 2, indipendentemente dal protocollo utilizzato per la fase 1.

Selezione dell'interfaccia

In molti casi, l'opzione **Interfaccia** per un tunnel IPsec sarà WAN, poiché i tunnel sono collegati a siti remoti. Tuttavia, ci sono un sacco di eccezioni, le più comuni delle quali sono delineate nel resto di questa sezione.

Ambienti CARP

Gli indirizzi IP virtuali di tipo CARP sono disponibili anche nel menu a discesa di **Interfaccia** per l'utilizzo in ambienti ad elevata disponibilità (*Elevata disponibilità*). In questi ambienti, un indirizzo CARP appropriato deve essere scelto per la WAN dove terminerà il tunnel IPsec. Con l'uso dell'indirizzo IP del CARP, si garantisce che il tunnel IPsec sarà gestito dal membro del cluster ad elevata disponibilità attualmente in stato MASTER, quindi anche se il firewall primario è disattivato, il tunnel si collegherà a qualsiasi membro del cluster abbia assunto il ruolo di MASTER.

VIP dell'alias dell'IP

Se sono disponibili più indirizzi IP su un'interfaccia che utilizza i VIP di tipo alias dell'IP, saranno disponibili anche in questo elenco. Per utilizzare uno di questi indirizzi IP per la VPN, invece, selezionarlo qui.

Ambienti con MultiWAN

Quando si utilizza MultiWan (*Connessioni WAN multiple*), scegliere l'interfaccia appropriata per l'interfaccia di tipo WAN a cui il tunnel si connetterà. Se la connessione entra via WAN, scegliere WAN. Se il tunnel utilizza una WAN

diversa, scegliere l'interfaccia WAN OPT necessaria. Verrà aggiunto automaticamente un percorso statico per garantire che il traffico verso i percorsi del **gateway remoto** attraverso la WAN appropriata.

Un gruppo gateway può anche essere scelto da questa lista. Un gruppo gateway da usare con IPsec deve avere un solo gateway per livello. Quando si utilizza un gruppo di gateway, se il primo gateway si spegne, il tunnel passa alla prossima WAN disponibile nel gruppo. Quando la prima WAN torna su, il tunnel sarà ricostruito di nuovo lì. Se l'endpoint sul lato opposto è uno che non supporta più indirizzi peer, come un altro firewall di Firew4LL, questo deve essere combinato con un set di host del DynDNS che utilizza lo stesso gruppo di gateway per failover. L'host del DynDNS aggiornerà l'indirizzo IP come visto dal lato opposto, in modo che l'endpoint remoto sappia di accettare il traffico dalla WAN appena attivata.

Protezione interna wireless

Quando si configura IPsec per aggiungere LA crittografia a una rete wireless, come descritto in *Protezione aggiuntiva per una rete wireless*, scegliere l'interfaccia OPT che corrisponde alla scheda wireless. Quando si utilizza un punto di accesso wireless esterno, selezionare l'interfaccia collegata al punto di accesso wireless.

Gateway remoto

Il **gateway remoto** è il peer di IPsec per questa fase 1. Questo è l'endpoint dall'altro lato del tunnel verso il quale IPsec negozierà questa fase 1. Questo può essere impostato su un indirizzo IP o un nome di dominio completamente qualificato. Quando impostata per usare un nome, la voce viene periodicamente risolta dal DNS e aggiornata quando viene rilevata una modifica.

Descrizione

La **Descrizione** per la fase 1 è un testo da usare per identificare questa fase 1. Non è utilizzata nelle impostazioni Ipsec, è solo per riferimento.

Metodo per l'autenticazione

Una fase 1 di IPsec può essere autenticata usando una chiave pre-condivisa (PSK) o certificati RSA, il selettore **del metodo di autenticazione** sceglie quale di questi metodi verrà utilizzato per autenticare il peer remoto. I campi appropriati al metodo scelto saranno visualizzati nella schermata di configurazione della fase 1.

PSK reciproco

Quando si usa il PSK reciproco, il peer viene validato usando una stringa definita. Più lunga è, migliore risulta, ma dal momento che è una semplice stringa, c'è una possibilità che si possa indovinare. Per questo motivo una chiave lunga/complessa è più sicura quando si utilizza la modalità PSK.

RSA reciproco

In modalità *RSA reciproca*, selezionare una CA e un certificato utilizzati per verificare il peer. Durante lo scambio di fase 1, ogni peer invia il proprio certificato all'altro peer e poi lo convalida contro la propria CA condivisa. La CA e il certificato devono essere creati per il tunnel prima di tentare di impostare la fase 1.

Modalità PSK+Xauth reciproca

Utilizzata con IPsec e IKEv1 mobili, questa selezione consente la verifica del nome utente e della password xauth insieme a una chiave pre-condivisa (o gruppo).

Modalità RSA+Xauth reciproca

Utilizzata con IPsec e IKEv1 per dispositivi mobili, questa selezione consente la verifica del nome utente e della password xauth insieme all'autenticazione dei certificati RSA utilizzando certificati sia sul client che sul server.

Modalità RSA+Xauth

Utilizzata con dispositivi mobili con IPsec e IKEv1, questa selezione la verifica del nome utente e della password xauth insieme a un certificato solo sul lato server. Non è abbastanza sicuro come la *modalità RSA+Xauth reciproca,* ma è più facile per i client.

EAP-TLS

Utilizzato con dispositivi mobili con IPsec e IKEv2, EAP-TLS dell'RSA verifica che i certificati sul client e sul server provengano dalla stessa CA condivisa, simile all'RSA reciproco. I certificati client e server richiedono un trattamento speciale:

- **Il certificato del server deve avere il nome del firewall come esiste** nel DNS elencato nel suo Nome Comune, e di nuovo come Nome del Soggetto Alternativo (SAN). L'indirizzo IP del firewall deve anche essere elencato in un SAN.
- **L'identificatore nella fase 1 deve anche essere impostato per** corrispondere al nome dell'host del firewall come elencato nel nome comune del certificato.
- **Il certificato client deve avere il nome dell'utente elencato come** nome comune e poi di nuovo come SAN.

I certificati CA e server devono essere generati prima di tentare di configurare EAP-TLS. Il CA e oò certificato dell'utente devono essere importati nel client.

EAP-RADIUS

Utilizzato con IPsec e IKEv2 per dispositivi mobili, questa selezione esegue la verifica di CA insieme all'autenticazione del nome utente e della password via RADIUS. Un server RADIUS deve essere selezionato nella scheda **client per dispositivi mobili.** Anche se i certificati utente non sono necessari, EAP-RADIUS richiede ancora che un CA e un certificato del server siano presenti utilizzando gli stessi attributi menzionati in EAP-TLS. La CA deve essere importata al client, ma nessun certificato utente.

EAP-MSCHAPv2

Utilizzato con IPsec e IKEv2 su dispositivi mobili, EAP-Mschapv2 funziona in modo identico a EAP-RADIUS ad eccezione dei nomi utente e password che sono definiti nella scheda **Chiave pre-condivisa** in **VPN>IPsec** con il **tipo segreto** impostato su EAP. Si richiede anche un CA e un certificato del server con gli stessi requisiti elencati in precedenza. La CA deve essere importata al client, ma nessun certificato utente.

Modalità di negoziazione

Per IKEv1, sono supportate due **modalità di negoziazione**: principale , aggressiva. Questa selezione non è presente quando si utilizza Ikev2.

Modalità principale

Principale è la modalità più sicura, sebbene richieda anche più pacchetti tra i peer per realizzare una negoziazione di successo. E "anche molto più rigorosa nella sua convalida.

Modalità aggressiva

Aggressiva è generalmente il più compatibile ed è la modalità più veloce. È un po" più indulgente con i tipi di identificatore, e tende ad avere più successo quando si negozia con dispositivi di terze parti in alcuni casi. È più veloce perché invia tutte le informazioni identificative in un singolo pacchetto, il che lo rende anche meno sicuro perché la verifica di tali dati non è così rigorosa come quella che si trova nella modalità principale.

Mio identificatore/Identificatore peer

Qui, scegliere l'identificatore utilizzato per inviare al peer remoto, e anche per verificare l'identità del peer remoto. I seguenti tipi di identificatore possono essere scelti per i selettori **Mio identificatore** e **Identificatore peer**. Se necessario, una casella di testo apparirà per inserire un valore da utilizzare per l'identificatore.

Mio indirizzo IP/Indirizzo IP peer

Questa scelta è una macro che utilizzerà automaticamente l'indirizzo IP sull'interfaccia, o il VIP selezionato, come identificatore. Per i peer, questo è l'indirizzo IP da cui sono stati ricevuti i pacchetti, che dovrebbe essere il **gateway remoto.**

Indirizzo IP

L'opzione *Indirizzo IP* consente di utilizzare un indirizzo IP diverso come identificatore. Un uso potenziale per questo sarebbe se il firewall è dietro un router che esegue il NAT. Il vero indirizzo IP esterno potrebbe essere utilizzato in questo campo.

Distinguished Name

Un *Distinguished Name* è un altro termine per un nome di dominio completamente qualificato, come *host.esempio.com*. Inserire un valore in quel formato nella casella.

Nome utente distinto

Un *nome utente distinto* è un indirizzo e-mail, come vpn@esempio.com, piuttosto che un FQDN.

Distinguished Name dell' ASN.1

Se si utilizza l'autenticazione in modalità *RSA reciproca*, questo può essere il soggetto del certificato utilizzato, o una stringa simile.

Tag dell'ID della chiave (KeyID)

Una stringa arbitraria da usare come identificatore.

DNS Dinamico

Un hostname da risolvere e utilizzare come identificatore. Questo è utile soprattutto se il firewall è dietro il NAT e non ha alcuna conoscenza diretta del suo indirizzo IP esterno a parte un hostname del DNS dinamico. Questo non è rilevante o disponibile per un **identificatore peer** in quanto l'hostname può essere utilizzato direttamente nel campo **gateway remoto** e utilizzare l'"*indirizzo IP del peer* per l'identificatore.

Any

Nei casi in cui l'identificatore remoto non è noto o non può essere abbinato, l'"**identificatore peer** può essere impostato su **Any**. Questo è più comune su alcuni tipi di configurazioni mobili, ma è una scelta molto meno sicura che abbinare correttamente l'identificatore.

Pre-Shared Key (se si utilizza il PSK reciproco)

Questo campo è usato per entrare nel PSK per l'autenticazione di fase 1. Come accennato in precedenza, farei di questa una chiave lunga/complessa. Se questo PSK è stato fornito dal peer, inserirlo qui. Se un nuovo PSK deve essere generato, si consiglia di utilizzare uno strumento di generazione di password impostato ad una lunghezza di almeno 15, ma può essere molto più lungo.

Phase 1 - Algoritmi di crittografia

Ci sono molte opzioni per gli algoritmi di crittografia sia di fase 1 sia di fase 2.

Le opzioni attuali sono tutte considerate crittograficamente sicure. La scelta dipende dal dispositivo a cui il tunnel si connetterà e dall'hardware disponibile in questo firewall. In generale, AES è il cifrario più desiderabile e la lunghezza della chiave più lunga (256 bit) è la migliore. Quando ci si connette a dispositivi di terze parti, 3DES (chiamato anche "Triplo DES") è una scelta comune in quanto potrebbe essere l'unica opzione supportata dall'altro terminale.

Ulteriori informazioni sui cifrari e sull'accelerazione sono disponibili negli *algoritmi di crittografia fase 2*.

Phase 2 - Algoritmi di hash

Gli algoritmi di hash vengono utilizzati con IPsec per verificare l'autenticità dei dati dei pacchetti. MD5, SHA1, SHA256, SHA384, SHA512, e AES-XCBC sono gli algoritmi di hash disponibili per la fase 1 e la fase 2. Tutti sono considerati crittograficamente sicuri, anche se SHA1 (Algoritmo di hash sicuro, Revisione 1) e le sue varianti sono considerati i più forti rispetto MD5. SHA1 richiede più cicli di CPU di MD5, e i valori più grandi di SHA a loro volta richiedono una potenza della CPU ancora maggiore. Questi algoritmi di hash possono anche essere riferiti a HMAC (Codice di autenticazione del messaggio di hash) nel nome in alcuni contesti, ma tale utilizzo varia a seconda dell'hardware o del software in uso.

Nota: L'implementazione di SHA256-512 è conforme a RFC 4868 sulla versione di FreeBSD usata da Firew4LL. La conformità con RFC 4868 rompela compatibilità con gli stack che sono implementato con draft-ietf-ipsec-ciph-sha-256-00, inclusi FreeBSD 8.1 e precedenti. Prima di utilizzare SHA256, 384 o 512, verificare con l'altro lato per assicurarsi che ci siano anche implementazioni conformi a RFC 4868 o non funzioneranno. Il messaggio di impegno di FreeBSD pertinente quando compare spiega in modo più dettagliato.

Gruppo di chiavi DH

Tutte le opzioni del gruppo di chiavi DH (Diffie-Hellman, dal nome dei suoi autori) sono considerate crittograficamente sicure, anche se i numeri più alti sono leggermente più sicuri a costo di un maggiore utilizzo della CPU.

Durate di vita

La durata specifica la frequenza con cui la connessione deve essere impostata, specificata in secondi. 28800 secondi sulla fase 1 è una configurazione comune ed è appropriata per la maggior parte degli scenari.

Certificato Autonono (se si utilizza l'RSA reciproco)

Questa opzione appare solo se si utilizza una **modalità di autenticazione** basata su RSA. L'elenco è compilato utilizzando i certificati presenti nella configurazione del firewall. I certificati possono essere importati e gestiti in **Sistema>Gestione dei certificati** nella scheda **Certificati**. Sceglere il certificato da usare per questa fase 1 di IPsec dall'elenco. La CA per questo certificato deve corrispondere a quella scelta nel selettore **Autorità del mio certificato**.

L'autorità di certificazione autonoma (se si utilizza l'RSA reciproco)

Questa opzione appare solo se si usa una **modalità di autenticazione** basata su RSA. L'elenco è riempito usando le CA presenti nella configurazione del firewall. Una CA può essere importata e gestita in **Sistema>Gestione dei certificati**. Scegliere la CA da usare per questa fase 1 di IPsec dall'elenco.

Disabilitare Rekey

Selezionando questa opzione si ordina a Firew4LL di non avviare un rekey sul tunnel. Alcuni client (specialmente i client Windows dietro NAT) si comportano male quando ricevono una richiesta rekey, quindi è più sicuro in questi casi permettere al client di avviare rekey disabilitando l'opzione sul server. Normalmente entrambe le parti dovrebbero effettuare un rekey se necessario, ma se il tunnel fallisce quando si verifica un evento rekey, provare a selezionare questa opzione su un solo lato.

Disabilitare la ri-autentificazione

Questa opzione viene visualizzata solo per i tunnel IKEv2, IKEv1 sarà sempre ri-autenticato. Se questa opzione è selezionata, quando un tunnel effettua un rekey non ri-autentica il peer. Quando non è controllato, la SA viene rimossa e negoziata per intero, piuttosto che effettuare solo il rekey.

Solo per i risponditori

Se è selezionato **Solo rispondente**, Firew4LL non tenterà di avviare il tunnel quando il traffico tenta di attraversare. Il tunnel verrà stabilito solo quando il lato opposto avvia la connessione. Inoltre, se DPD rileva che il tunnel è fallito, il tunnel sarà lasciato down piuttosto che essere riavviato, lasciandolo up sul lato opposto per ricollegare.

NAT Traversal

L'opzione di NAT Traversal, nota anche come NAT-T, è disponibile solo per IKEv1. IKEv2 ha il NAT Traversal integrato in modo che l'opzione sia inutile. L'NAT Traversal può incapsulare il traffico ESP per IPsec all'interno dei pacchetti UDP, per funzionare più facilmente in presenza del NAT. Se questo firewall o il firewall dall'altra parte del tunnel saranno dietro un dispositivo NAT, allora l'NAT Traversal sarà probabilmente necessario. L'impostazione predefinita *Automatico* utilizzerà l'attraversamento del NAT nei casi in cui ne viene rilevata la necessità. L'opzione può anche essere impostata su *Forzare* per garantire che il'attraversamento del NAT sia sempre utilizzato per il tunnel. Questo può aiutare se c'è un problema noto che trasporta traffico ESP tra i due endpoint.

MOBIKE

MOBIKE è un'estensione di IKEv2 che gestisce client con diverse case e client che vagano tra diversi indirizzi IP. Questo viene utilizzato principalmente con i client con dispositivi mobili per consentire loro di cambiare gli indirizzi remoti mantenendo attiva la connessione.

Connessioni divise

Questa opzione è specifica per IKEv2 e configura le voci della fase modo da utilizzare voci di connessione separate, piuttosto che un unico selettore del traffico per ogni associazione di sicurezza secondaria. In particolare, questo è noto per essere un problema con i prodotti Cisco come ASA.

Se un tunnel IKEv2 è in uso con più voci della Fase 2, e solo una coppia di reti Fase 2 stabilisce una connessione, attivare questa opzione.

Rilevamento dei peer morti (Dead Peer Detection, DPD)

Il rilevamento dei peer morti (DPD) è un controllo periodico che controlla che l'host dall'altra parte del tunnel IPsec sia ancora vivo. Se un controllo DPD fallisce, il tunnel viene abbattuto rimuovendo le voci SAD associate e si tenta di rinegoziare.

Il campo **Ritardo** controlla quante volte viene tentato un controllo DPD, e il campo **Fallimenti massimi** controlla quanti di questi controlli devono fallire prima che un tunnel sia considerato in stato di down. I valori di default di 10 secondi e 5 fallimenti risulteranno nel tunnel che sarà considerato down dopo circa un minuto. Questi valori possono essere aumentati per i collegamenti di cattiva qualità per evitare di abbattere un tunnel utilizzabile, ma con perdite.

Phase 2 - Impostazioni

Le impostazioni della fase 2 per un tunnel IPsec regolano il traffico che entra nel tunnel e come viene cifrato. Per i tunnel normali, questo controlla le sottoreti che entreranno nel firewall. Per i client con dispositivi mobili controlla principalmente la crittografia per la fase 2, ma può anche fornire opzionalmente un elenco di reti ai clienti per l'uso del tunnel diviso. Per ogni fase 1 possono essere aggiunte definizioni multiple della fase 2 per consentire l'utilizzo di più sottoreti all'interno di un singolo tunnel.

Abilitare/Disabilitare

Questa impostazione controlla se questa voce della fase 2 è attiva o meno.

Modalità

Questa opzione consente la modalità tradizionale di tunnel di Ipsec o la modalità di trasporto. La modalità di tunnel può anche specificare IPv4 o IPv6.

Modalità tunnel IPv4/IPv6

Quando si utilizza il *tunnel IPv4* o il *tunnel IPv6* per questa voce di fase 2, il firewall userà il tunnel IPv4 o IPv6 per il traffico corrispondente alla **rete locale** e alla **rete remota** specificata. Una fase 2 ci può essere per IPv4 o IPv6, e i valori di rete sono convalidati in base a tale scelta. Il traffico corrispondente sia alla rete locale che alla rete remota entrerà nel tunnel e verrà consegnato all'altro lato.

Nota: Con IKEv1, può essere utilizzato solo uno tra IPv4 o IPv6, e

---

deve corrispondere alla stessa famiglia di indirizzi utilizzata per stabilire la fase 1 del tunnel. Con IKEv2, entrambi i tipi possono essere utilizzati nello stesso tunnel.

Modalità di trasporto

La modalità di *trasporto* cifrerà il traffico tra gli indirizzi IP utilizzati come endpoint di fase 1. Questa modalità consente di crittografare il traffico dall'indirizzo IP esterno del firewall all'indirizzo IP esterno sul lato opposto. Qualsiasi traffico inviato tra i due nodi sarà crittografato, in modo da utilizzare altri metodi di effettuare il tunnel che non utilizzano la crittografia, come un tunnel GIF o GRE, in modo sicuro. La **rete locale** e la **rete remota** non sono impostate per la modalità di trasporto, essa assume gli indirizzi in base alle impostazioni della fase 1.

Rete locale (se si utilizza una modalità tunnel)

Come suggerisce il nome, questa opzione imposta la **Rete Locale** che sarà associata a questa fase 2. Questa è tipicamente la LAN o altra sottorete interna per la VPN, ma può anche essere un singolo indirizzo IP se solo un client ha bisogno di usare il tunnel. Il selettore Tipo è pre-caricato con scelte di sottorete per ogni interfaccia (es. *sottorete LAN*), così come le scelte di *Indirizzo* e *Rete* che permettono di inserire un indirizzo IP o sottorete manualmente.

Traduzione NAT/BINAT

Per eseguire il NAT su indirizzi di rete locali per farli apparire come sottorete diversa o come indirizzo IP pubblico, utilizzare i campi di **traduzione NAT/BINAT**. Se un singolo indirizzo IP è specificato in **Rete Locale** e un singolo indirizzo IP nel campo del **tipo di traduzione NAT/BINAT**, allora verrà impostata una traduzione NAT 1:1 tra i due. Il NAT 1:1 è anche configurato se una sottorete della stessa dimensione è usata in entrambi i campi. Se la rete locale è una sottorete, ma la **traduzione NAT/BINAT** è impostata su un singolo indirizzo IP, allora viene impostata una traduzione 1:molti NAT (PAT) che funziona come una regola del NAT in uscita sulla WAN, tutto il traffico in uscita sarà tradotto dalla rete locale al singolo IP nel campo NAT. Se il NAT non è necessario sul traffico IPsec, lasciarlo impostato su *Nessuno*.

Rete remota (se si utilizza una modalità tunnel)Remote Network

Questa opzione (presente solo per tunnel su dispositivi non mobili) specifica l'*indirizzo* IP o la *rete* che esiste sull'altro lato (remoto) della VPN. Funziona in modo simile all'opzione **Rete Locale** menzionata in precedenza.

Protocollo

IPsec ha la possibilità di scegliere AH (Intestazione autenticata) o ESP (Incapsulamento del carico utile di sicurezza). In quasi tutte le circostanze, ESP è utilizzato in quanto è l'unica opzione che crittografa il traffico. AH fornisce solo la garanzia che il traffico proviene dalla fonte attendibile ed è raramente utilizzato.

Phase 2 - Algoritmi di crittografia

Nei sistemi con AES-NI, la scelta più rapida e sicura è AES-GCM, a condizione che il dispositivo remoto lo supporti. Quando si utilizza AES-GCM nella fase 2, utilizzare AES nella fase 1 con una lunghezza di chiave equivalente. Anche se AES-CGM è utilizzato, non selezionare alcuna opzione per gli **algoritmi di hash** nella fase 2.

Quando si utilizzano sistemi con acceleratori *glxsb*, come ALIX, scegliere AES 128 per le migliori prestazioni. Per i sistemi con acceleratori *hifn*, scegliere 3DES o AES per le migliori prestazioni. Sia AES che Blowfish permettono di selezionare la lunghezza della chiave del cifrario in passi variabili tra 128-bit e 256-bit. Valori più bassi saranno più veloci, valori più grandi sono più crittograficamente sicuri. Per i sistemi senza un acceleratore di crittografia hardware, Blowfish e CAST sono le opzioni più veloci.

Le scelte di crittografia di fase 2 consentono selezioni multiple in modo che siano accettate scelte multiple quando si agisce come rispondente, o si tenteranno combinazioni multiple quando si lavora come iniziatore. È meglio selezionare solo il cifrario desiderato, ma in alcuni casi selezionarne di più permetterà ad un tunnel di lavorare meglio sia come rispondente sia come iniziatore.

Phase 2 - Algoritmi di hash

Come con gli algoritmi di crittografia, possono essere selezionati più hash. È comunque meglio selezionare solo la scelta desiderata, se possibile. Per ulteriori discussioni sulla qualità dei vari tipi di hash, vedere *Algoritmi di hash di fase 1*.

Nota: Quando si utilizza AES-GCM per l'algoritmo di crittografia di

---

faase 2, non selezionare alcuna opzione per l'algoritmo di hash!

Gruppo di chiavi PFS

La perfetta segretezza forward (Perfect Forward Secrecy, PFS) fornisce materiale per creare chiavi con maggiore entropia, migliorando così la sicurezza crittografica della connessione, al costo di un maggiore utilizzo della CPU quando si verifica il rekey. Le opzioni hanno le stesse proprietà dell'opzione del gruppo di chiavi DH nella fase 1 (Vedere *gruppo di chiavi DH*), e alcuni prodotti si riferiscono a loro anche come valori di "DH" anche nella fase 2.

Durata di vita

L'opzione **durata di vita** specifica la frequenza con cui la connessione deve essere impostata, in secondi. 3600 secondi sulla fase 2 è una configurazione comune ed è appropriata per la maggior parte degli scenari.

Host per il ping automatico (Mantenere in vita)

Per l'uso su tunnel con dispositivi non mobili, questa opzione dice al firewall di avviare un ping periodicamente all'indirizzo IP specificato. Questa opzione funziona solo se il firewall ha un indirizzo IP all'interno della **rete locale** per questa voce di fase 2 e il valore dell'host del ping qui deve essere all'interno della **rete remota**.

18.1.3 Regole di firewall e IPsec

Quando un tunnel Ipsec è configurato Firew4LL aggiunge automaticamente le regole del firewall nascoste per consentire le porte UDP 500 e 4500, e il protocollo ESP dall'indirizzo IP del **gateway remoto** destinato all'indirizzo IP dell'interfaccia specificato nella configurazione del tunnel. Quando il supporto del client da dispositivo mobile è abilitato, le stesse regole del firewall vengono aggiunte, tranne quelle con il codice sorgente impostato su *qualsiasi*. Per annullare l'aggiunta automatica di queste regole, selezionare **Disabilitare tutte le regole VPN aggiunte automaticamente** in **Sistema>Avanzate** nella scheda **Firewall/NAT**. Quando questa casella è selezionata, le regole del firewall devono essere aggiunte manualmente per UDP 500, UDP 4500 ed ESP all'interfaccia WAN appropriata.

Il traffico iniziato dall'estremità remota di una connessione IPsec è filtrato con le regole configurate in **Firewall>Regole** nella scheda **IPsec**. Qui le restrizioni possono essere poste sulle risorse rese accessibili agli utenti IPsec remoti. Per controllare quale traffico può essere passato dalle reti locali ai dispositivi o alle reti collegate con IPsec della VPN da remoto, le regole sono sull'interfaccia locale in cui risiede l'host controllano il traffico (ad es. la connettività dagli host sulla LAN sono controllate con le regole LAN).

18.1.4 Sito-a-sito

Un tunnel IPsec con opzione sito-a-sito collega due reti come se fossero collegate direttamente da un router. I sistemi del Sito A possono raggiungere server o altri sistemi del Sito B e viceversa. Questo traffico può anche essere regolato tramite regole firewall, come con qualsiasi altra interfaccia di rete. Se più di un client si connette ad un altro sito dalla stessa posizione controllata, un tunnel sito-a-sito sarà probabilmente più efficiente, per non parlare dell'essere più comodo e più facile da supportare.

Con un tunnel sito-a-sito, i sistemi su entrambe le reti non devono avere alcuna conoscenza dell'esistenza di una VPN. Non è necessario alcun software del client, e tutto il lavoro del tunnel è gestito dagli endpoint del tunnel. Questa è una buona soluzione anche per i dispositivi che hanno il supporto di rete ma non gestiscono le connessioni VPN come stampanti, telecamere, sistemi HVAC e altri hardware incorporati.

Esempio di configurazione sito-a-sito

La chiave per creare un tunnel IPsec funzionante è garantire che entrambe le parti abbiano impostazioni corrispondenti per l'autenticazione, la crittografia e così via. Prima di iniziare, annotare gli indirizzi IP delle WAN locali e remote, nonché le sottoreti interne locali e remote che saranno trasportate attraverso il tunnel. Un indirizzo IP dalla sottorete remota per effettuare un ping è opzionale, ma è consigliato per mantenere vivo il tunnel. Il firewall non controlla le risposte, in quanto qualsiasi traffico avviato a un indirizzo IP sulla rete remota attiverà la negoziazione IPsec, quindi non importa se l'host effettivamente risponde o meno finché c'è un indirizzo IP dall'altro lato della connessione. Oltre alla **descrizione** estetica del tunnel e queste informazioni, le altre impostazioni di connessione saranno identiche.

In questo esempio e alcuni degli esempi successivi in questo capitolo, le seguenti impostazioni saranno assunte:

Tabella 1: Impostazioni degli endpoint Ipsec

+=====================-+====================-+=====================-
+====================-+ | Sito A | Sito B | | | +"""""""""""""""""""""=+"""""""""""""""""""""=+"""""""""""""""""""""=+"""""
| | Ufficio di Austin | | Ufficio di Londra | +=====================-+====================-
+=====================-+====================-+ | IP della WAN | 198.51.100.3 | IP della WAN

| 203.0.113.5 | +=====================-+====================-+=====================-
+====================-+ | Sottorete della LAN | 10.3.0.0/24 | Sottorete della LAN |
10.5.0.0/24 | +=====================-+====================-+=====================-
+====================-+ | IP della LAN | 10.3.0.1 | IP della LAN | 10.5.0.1 | +=====================-
+====================-+=====================-+====================-+

Iniziare con Sito A. Creare il tunnel facendo clic su  **Aggiungere P1**. Viene mostrata la pagina di configurazione della fase 1 per il tunnel. Molte di queste impostazioni possono essere lasciate ai loro valori predefiniti.

In primo luogo, compilare la sezione superiore che contiene le informazioni generali di fase 1, come mostrato nella figura *Impostazioni del tunnel della VPN*. Gli elementi in grassetto sono necessari. Inserire le impostazioni come descritto:

Deselezionato Deselezionare questa casella in modo che il tunnel sia operativo.

Versione con scambio di chiave Specifica se utilizzare IKEv1 o IKEv2. Per questo esempio, IKEv2 è utilizzato, ma se un lato non supporta IKEv2, utilizzare nvece IKEv1.

Protocollo Internet Sarà *IPv4* nella maggior parte dei casi, a meno che entrambe le WAN abbiano l'IPv6, nel qual caso è possibile utilizzare entrambi i tipi.

Interfaccia Molto probabilmente impostata su *WAN*, ma vedere la nota in *Selezione dell'interfaccia* sulla selezione dell'interfaccia corretta quando non si è sicuri.

Gateway remoto L'indirizzo WAN del sito B, 203.0.113.5 in questo esempio.

Descrizione Testo per indicare lo scopo o l'identità del tunnel. È una buona idea mettere il nome del sito B in questa casella, e qualche dettaglio sullo scopo del tunnel per aiutare la futura amministrazione. Per questo esempio Ufficio di Londra dell'EsempioCo viene utilizzato nella descrizione per identificare dove termina il tunnel.

La sezione successiva controlla la fase 1 di IPsec, o l'autenticazione. È mostrata in figura *Impostazioni della fase del sito A*. I valori predefiniti sono desiderabili per la maggior parte di queste impostazioni e semplificano il processo.

Metodo di autenticazione L'impostazione predefinita, *PSK reciproco*, è usata per questo esempio.

Mio identificatore Il valore predefinito, *mio indirizzo IP*, viene mantenuto.

Identificatore del peer Il valore predefinito, *Indirizzo IP del Peer IP*, viene mantenuto.

Chiave pre-condivisa Questa è l'impostazione più importante per funzionare. Come indicato nella panoramica VPN, IPsec che utilizza chiavi pre-condivise può essere rotto se viene utilizzata una chiave debole. Utilizzare una chiave forte, di almeno 10 caratteri di lunghezza contenente un mix di lettere, numeri e simboli maiuscoli e minuscoli. La stessa chiave esatta dovrà essere inserita nella configurazione del tunnel per il Sito B in seguito, quindi annotarla o copiarla e incollarla altrove. Copiare e incollare può essere utile, specialmente con una chiave complessa come abc123%Xyz9$7qwErty99.

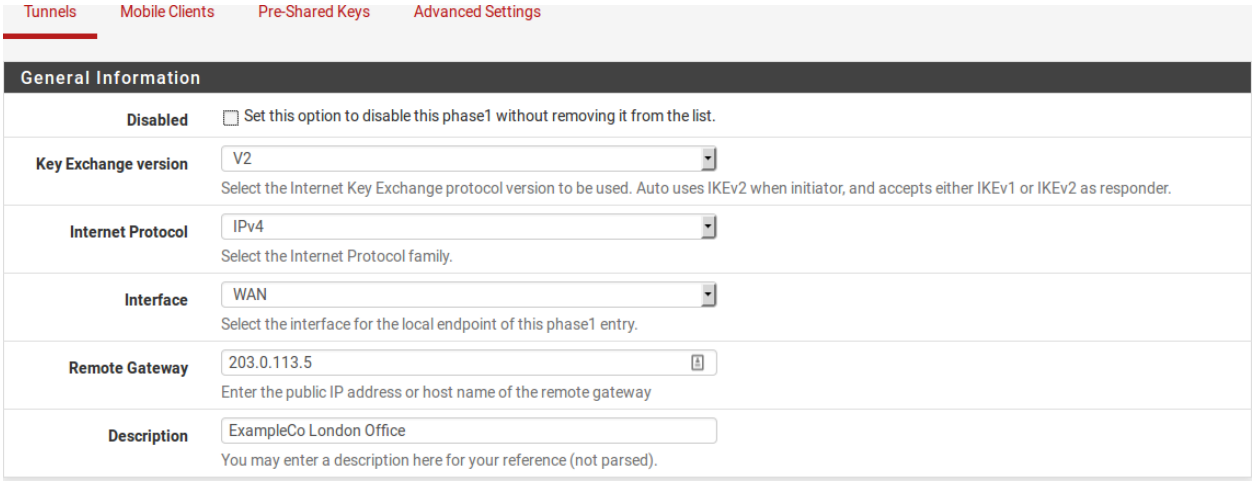


Fig. 1: Impostazioni del tunnel della VPN del sito A

Algoritmo di crittografia Usa *AES* con una lunghezza della chiave di 256 bit.

Algoritmo hash Usa *SHA256* se entrambi i lati lo supportano, altrimenti usa *SHA1* predefinito.

Gruppo DH Il valore predefinito di *2 (1024 bit)* è OK, valori più alti sono più sicuri ma usano più CPU.

Durata di vita Può anche essere specificata, altrimenti verrà utilizzato il valore predefinito di *28800*.

Disabilitare rekey Lasciare deselezionato

Solo rispondente Lasciare deselezionato

NAT Traversal Lasciare su *Automatico*, poiché in questo esempio nessuno dei due firewall è dietro NAT.

Rilevamento dei peer morti Lasciare selezionato, il **ritardo** predefinito di 10 secondi e Max Failure di 5 è ade-quate. A seconda delle esigenze in un sito un valore più elevato può essere migliore, come 30 secondi e 6 tentativi, ma una connessione WAN problematica su entrambi i lati può renderlo troppo basso.

Fare clic su **Salvare** per completare la fase 1 di installazione.

Dopo l'aggiunta della fase 1, aggiungere una nuova definizione di fase 2 alla VPN:

- **Fare clic su** **Mostrare voci di fase 2 come visto nella** figura *elenco della fase 2 del sito A (vuoto)* per espandere l'elenco di fase 2 per questa VPN.
- **Fare clic su** **Aggiungere P2 per aggiungere una nuova voce** di fase 2, come si vede nella figura *Aggiunta di una voce di fase 2 al sito A*.

Ora aggiungere le impostazioni per la fase 2 su questa VPN. Le impostazioni per la fase 2 (Figura *Impostazioni generali della fase 2 del sito A*) possono variare più della fase 1.

Modalità Poiché il traffico di tunnel è desiderato, selezionare Tunnel IPv4

Sottorete locale Meglio lasciare questo come *sottorete LAN*, ma potrebbe anche essere cambiato in *rete* con il valore di sottorete corretto compilato, in questo caso *10.3.0.0/24*. Lasciarlo come *sottorete LAN* assicura che se la rete viene rinumerata, questa estremità del tunnel seguirà. Se ciò accade, l'altra estremità deve essere cambiata manualmente.

NAT/BINAT Impostare su *nessuno*.

Sottorete remota Impostare la rete del sito B, in questo caso *10.5.0.0/24*.

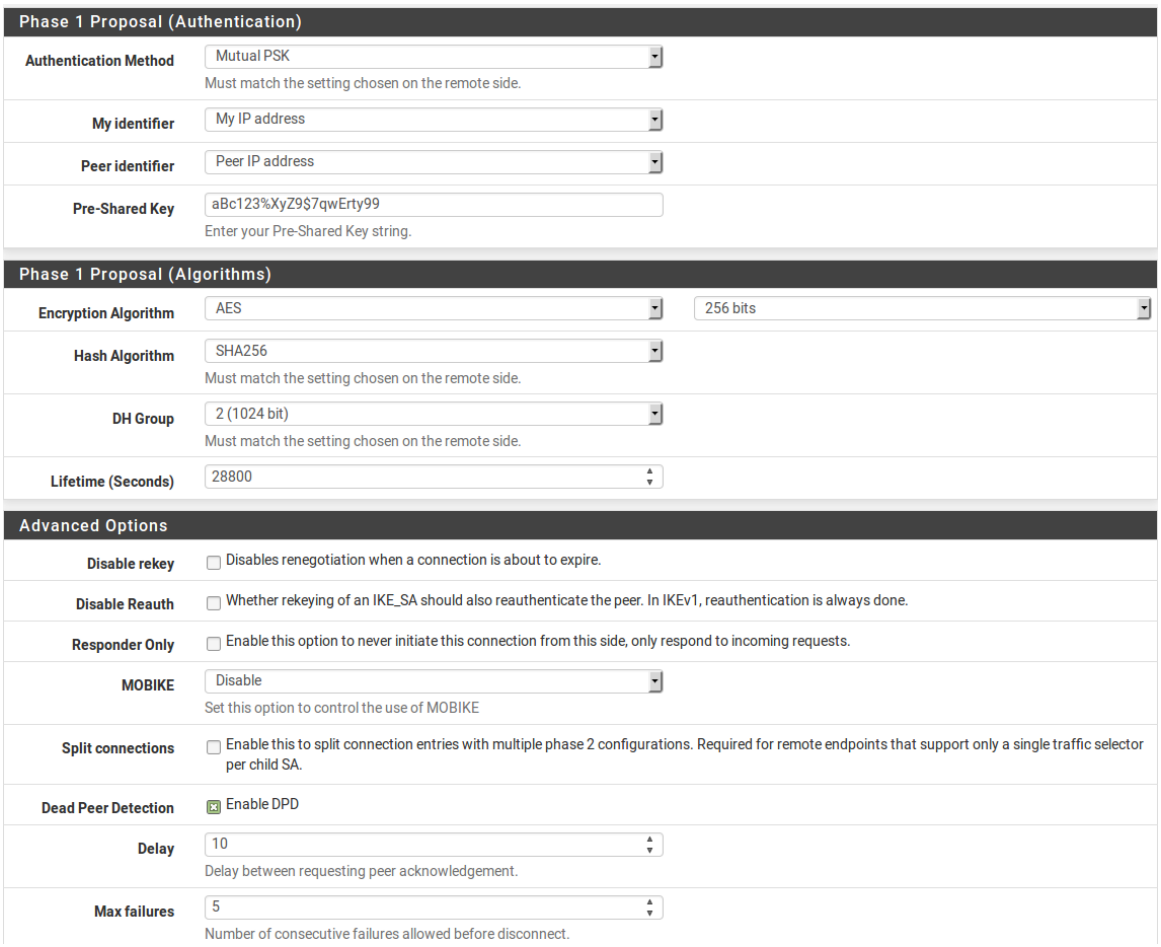


Fig. 2: Impostazione della fase 1 del sito A

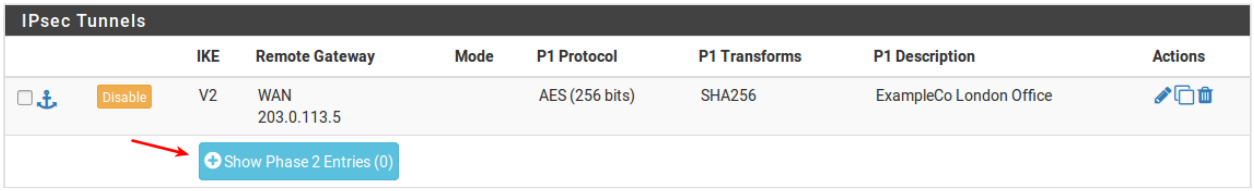


Fig. 3: Elenco della fase 2 del sito A (Vuoto)

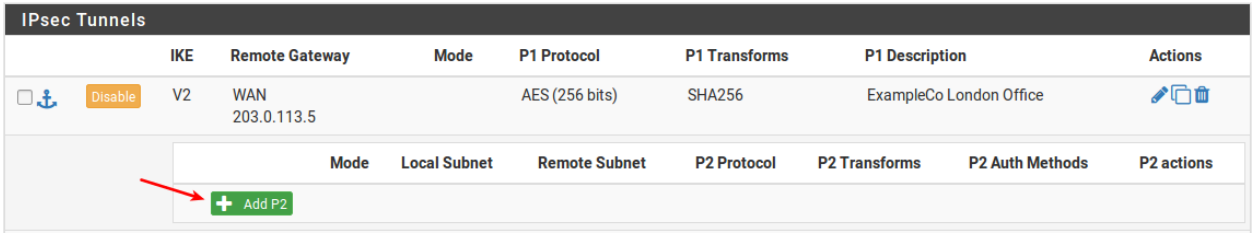


Fig. 4: Aggiunta di una voce di fase 2 al sito A

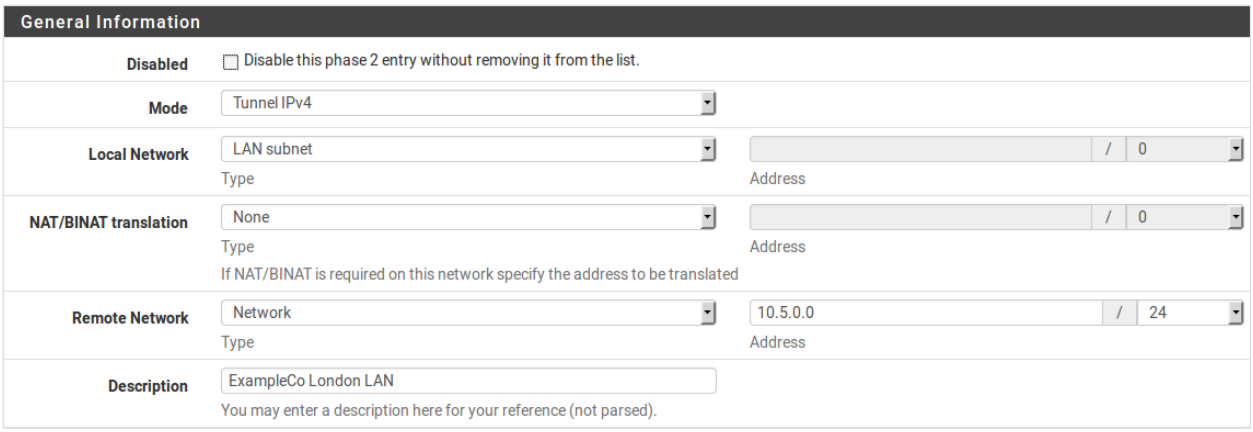


Fig. 5: Impostazioni generali della fase 2 del sito A

Il resto delle impostazioni della fase 2, visto in figura *Impostazioni della fase 2 per il sito A*, coprono la crittografia del traffico. Gli algoritmi di crittografia e gli algoritmi di hash possono essere impostati per consentire opzioni multiple nella fase 2, ed entrambe le parti negoziano e concordano sulle impostazioni finché ciascuna parte ha almeno una di esse in comune. In alcuni casi può essere una buona cosa, ma di solito è meglio limitare questo alle singole opzioni specifiche desiderate da entrambe le parti.

Protocollo Impostare su *ESP* per la crittografia.

Algoritmo di crittografia Idealmente, se entrambe le parti lo supportano, selezionare *AES256-GCM* con una lunghezza della chiave di *128 bit*. In caso contrario, utilizzare *AES 256*, o qualsiasi cifrario entrambe le estremità supportino.

Algoritmo hash Con AES-GCM in uso, non è richiesto alcun hash. In caso contrario, utilizzare *SHA 256* o *SHA 1*. Evitare *MD5* quando possibile.

PFS Perfetta segretezza forward può aiutare a proteggere da alcuni attacchi chiave, ma è opzionale. In questo esempio, è disattivato.

Durata di vita Usare 3600 per questo esempio.

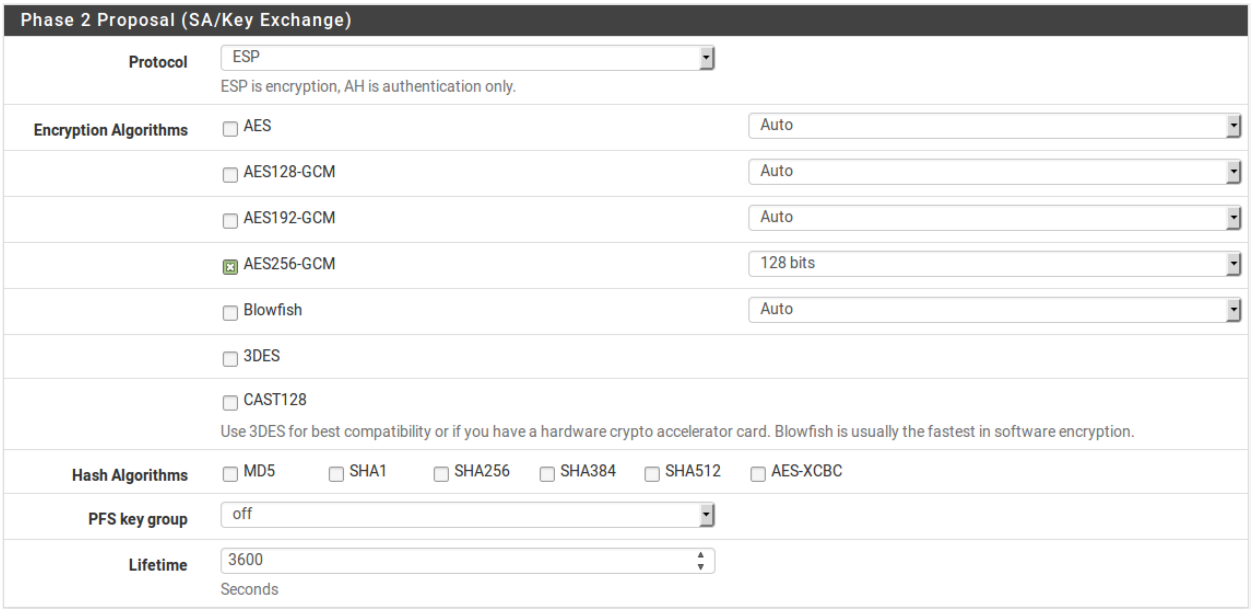


Fig. 6: Impostazioni della fase 2 per il sito A

Infine, un indirizzo IP può essere inserito per un sistema sulla LAN remota a cui verrà inviato periodicamente un ping ICMP, come nella figura *Mantenere in vita il sito A*. Il valore di ritorno del ping non è controllato, questo invierà solo il traffico del tunnel in modo che rimanga stabilito. In questa configurazione viene utilizzato l'indirizzo IP della LAN del firewall di Firew4LL per il Sito B, *10.5.0.1*.

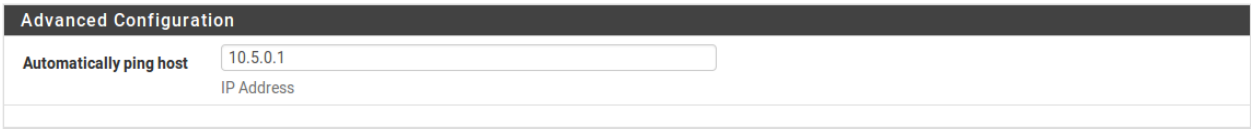


Fig. 7: Mantenere in vita il sito A

Per finalizzare le impostazioni e metterle in azione: * Fare clic su *Salvare* * Fare clic su *Applicare le modifiche* nella schermata del tunnel di IPsec, come visto nella figura *Applicare le impostazioni IPsec*.

Fig. 8: Applicare le impostazioni IPsec

Il tunnel per il Sito A è terminato, ma ora sono necessarie le regole di firewall per consentire il traffico dalla rete del Sito B di entrare attraverso il tunnel IPsec. Queste regole devono essere aggiunte alla scheda **IPsec** in **Regole firewall**. Vedere *Firewall* per le specifiche sull'aggiunta di regole. Le regole possono essere permissive come desiderato, (permettono qualsiasi protocollo da qualsiasi luogo a dovunque), o restrittive (permettono il TCP da un certo host sul Sito B a un certo host sul Sito A su una certa porta). In ogni caso, assicurarsi che gli indirizzi sorgente siano indirizzi del sito B, come 10.5.0.0/24. Gli indirizzi di destinazione saranno la rete del Sito A, 10.3.0.0/24.

Ora che il sito A è configurato, è il momento di affrontare il sito B. Ripetere il processo sull'endpoint del sito B per aggiungere un tunnel.

Solo alcune parti di questa configurazione differiscono dal Sito A come mostrato nella figura *Impostazioni della fase 1 per il sito B* e nella figura *Impostazioni della fase 2 per il sito B*:

- Le impostazioni di fase 1 per l'indirizzo WAN e la descrizione
- Le reti del tunnel della fase 2
- Impostazione per mantenere in vita

Aggiungere una fase 1 al firewall del Sito B utilizzando impostazioni identiche a quelle utilizzate nel Sito A ma con le seguenti differenze:

Gateway remoto L'indirizzo WAN del sito A, 198.51.100.3.

Descrizione Ufficio di Austin della EsempioCo.

- Fare clic su Salvare

Aggiungere una voce di fase 2 al firewall del sito B utilizzando le stesse impostazioni utilizzate sul sito A, ma con le seguenti differenze.

Sottorete remota La rete del sito A, in questo caso 10.3.0.0/24.

Host per il ping automatico (Figura *Mantenere in vita il sito B*). L'indirizzo IP della LAN del firewall di Firew4LL sul Sito A, 10.3.0.1.

- Fare clic su **Salvare**
- Fare clic su **Applicare modifiche** nella schermata Tunnel IPsec.

Come per il Sito A, anche le regole del firewall devono essere aggiunte per permettere al traffico sul tunnel di attraversare dal Sito A al Sito B. Aggiungere queste regole alla scheda IPsec sotto la scheda Regole del Firewall. Per maggiori

dettagli, consulta le *regole IPsec e firewall*. Questa volta, la sorgente del traffico sarebbe il Sito A, la destinazione del Sito B.

Entrambi i tunnel sono ora configurati e sono ora attivi. Controllare lo stato di IPsec visitando **Stato>IPsec**. Una descrizione del tunnel è mostrata con il suo stato.

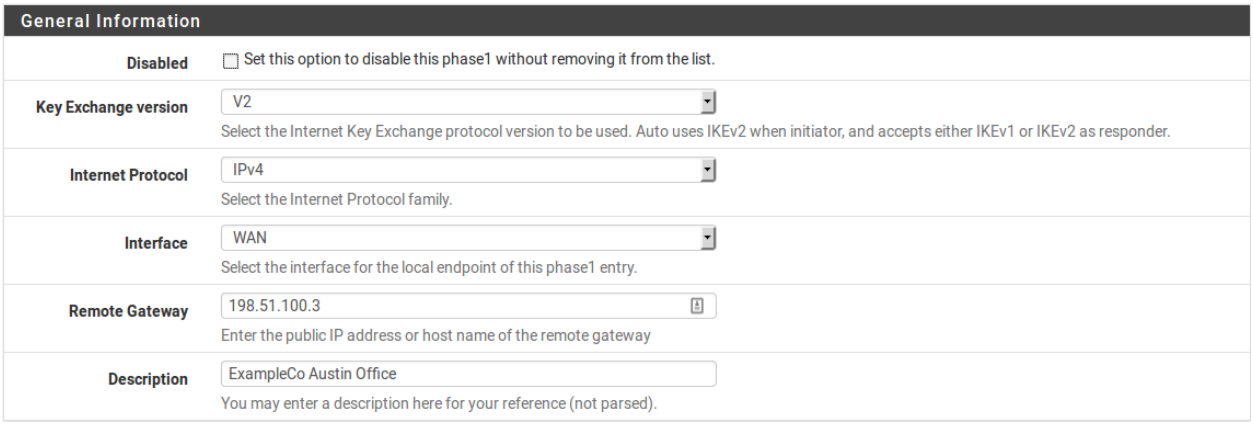


Fig. 9: Impostazioni della fase 1 per il sito B

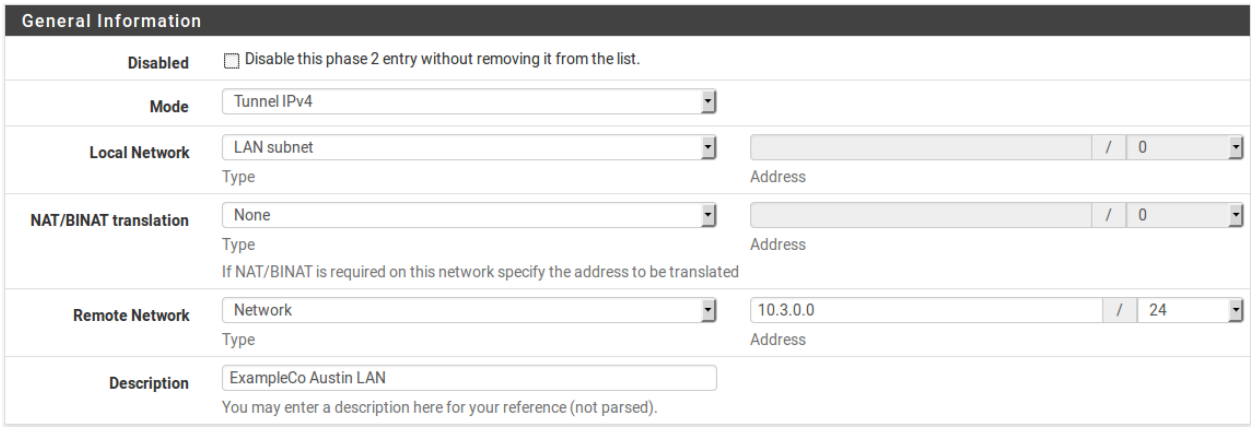


Fig. 10: Impostazioni della fase 2 per il sito B

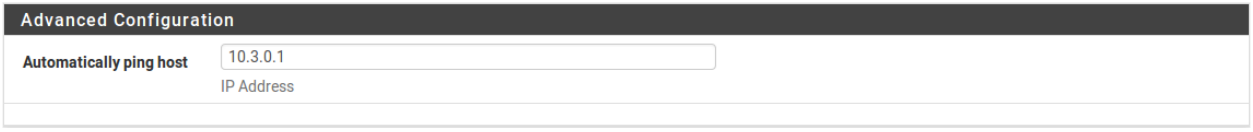


Fig. 11: Mantenere in vita il sito B

Se il tunnel non è elencato come **stabilito**, ci può essere un problema per stabilire il tunnel. La ragione più probabile è che nessun traffico ha tentato di attraversare il tunnel. Dal momento che la rete locale include un indirizzo che il firewall ha, un pulsante di connessione è offerto su questa schermata che avvierà un ping per la fase remota 2. Fare clic sul pulsante  **Connettere la VPN** per tentare di far apparire il tunnel, come visto nella figura *Stato dell'IPsec per il Sito A*. Se il pulsante di connessione non compare, provare a fare un ping su un sistema nella sottorete remota al Sito B da un dispositivo all'interno della rete locale di fase 2 al Sito A (o viceversa) e vedere se il tunnel si stabilisce. Provare la connettività IPsec con gli altri metodi di test di un tunnel.

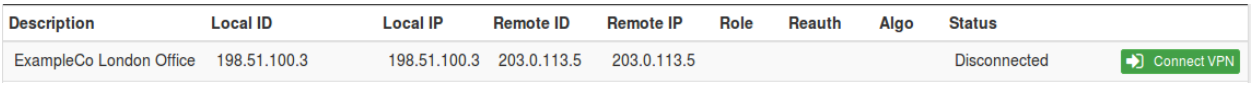


Fig. 12: Stato dell'IPsec per il sito A

In caso contrario, i registri di IPsec offriranno una spiegazione. Si trovano in **Stato>registro di sistema** nella scheda **IPsec**. Assicurarsi di controllare lo stato e i registri in entrambi i siti. Per ulteriori informazioni sulla risoluzione dei problemi, consultare la sezione *Risoluzione dei problemi con IPsec* più avanti in questo capitolo.

Considerazioni sul gateway e il routing

Quando l'endpoint della VPN, in questo caso un firewall Firew4LL, è il gateway predefinito per una rete, normalmente non ci sono problemi di routing. Quando un PC client invia traffico, andrà al firewall di Firew4LL, oltre il tunnel, e fuori l'altra estremità. Tuttavia, se il firewall di Firew4LL non è il gateway predefinito per una data rete, allora sarà necessario adottare altre misure di routing.

Ad esempio, immaginate che il firewall di Firew4LL sia il gateway del Sito B, ma non del sito A, come illustrato nella figura *IPsec con Sito-a-Sita dove |firew4ll| non è il gateway*. Un client, PC1 per il Sito B, invia un ping al PC2 per il Sito A. Il pacchetto lascia PC1, poi attraverso il firewall Firew4LL va al Sito B, attraverso il tunnel, fuori dal firewall Firew4LL del Sito A, e poi sul PC2. Ma cosa succede al ritorno? Il gateway su PC2 è completamente un altro router. La risposta al ping sarà inviata al router del gateway e molto probabilmente sarà buttata fuori, o peggio ancora, può essere inviata al collegamento a Internet e essere persa in quel modo.

Ci sono parecchi modo per risolvere questo problema e ognuno può essere migliore in base alle circostanze di un dato caso.

- Un percorso statico potrebbe essere inserito nel router del gateway che reindirizzerà il traffico destinato al lato lontano del tunnel al firewall Firew4LL. Anche con questo percorso, ulteriori complessità sono introdotte perché questo scenario si traduce in un routing asimmetrico come coperto in *Aggirare le regole del firewall per il traffico sulla stessa interfaccia*.
- Un percorso statico potrebbe essere aggiunto ai sistemi del client singolarmente in modo che sappiano di inviare il traffico direttamente al firewall di Firew4LL e non tramite il gateway predefinito. A meno che non ci sia solo un numero molto piccolo di host che hanno bisogno di accedere alla VPN, questo è un mal di testa per la gestione e dovrebbe essere evitato.
- In alcune situazioni può essere più facile rendere il firewall di Firew4LL il gateway e lasciarlo gestire la connessione Internet al posto del gateway esistente.

Traffico iniziato da Firew4LL e IPsec

Per accedere all'estremità remota delle connessioni IPsec dal firewall di Firew4LL stesso, «fingere» il sistema fuori aggiungendo un percorso statico che punta la rete remota all'indirizzo IP della LAN del firewall di Firew4LL. Si noti che questo esempio presume che la VPN stia collegando l'interfaccia LAN su entrambi i lati. Se la connessione IPsec è collegata a un'interfaccia OPT, sostituire l'interfaccia e l'indirizzo IP dell'interfaccia di conseguenza. A causa del modo in cui IPsec è collegato al kernel di FreeBSD, senza il percorso statico il traffico seguirà la tabella di routing del sistema, che probabilmente invierà questo traffico fuori dall'interfaccia WAN piuttosto che attraverso il tunnel IPsec. Prendere la figura *IPsec con sito-a-sito*, come esempio.

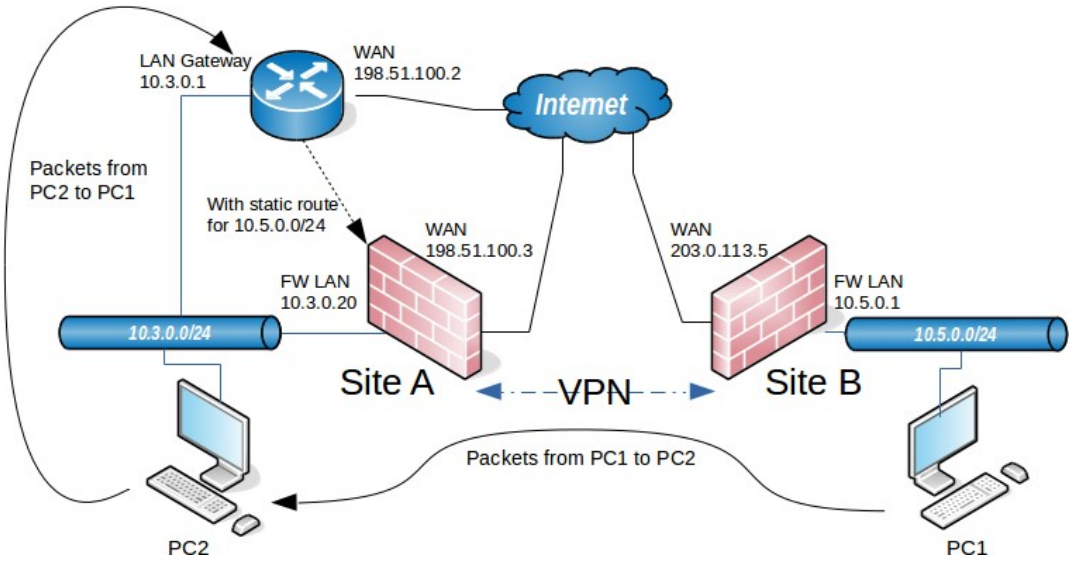


Fig. 13: IPsec con Sito-a-Sita dove Firew4LL non è il gateway

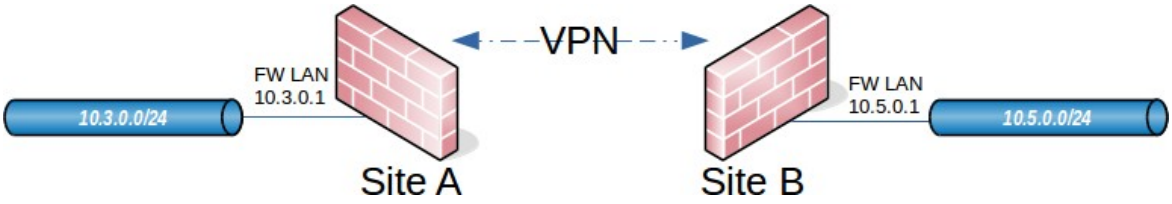


Fig. 14: IPsec con sito-a-sito

Un percorso statico è richiesto su ogni firewall, che viene fatto aggiungendo prima un gateway che punta all'indirizzo IP della LAN del firewall (vedere *Gateway*), e poi aggiungendo un percorso statico utilizzando questo gateway (vedere *Route statiche*). La figura *Route statica per il Sito A alla sottorete remota* mostra il percorso da aggiungere su ogni lato.

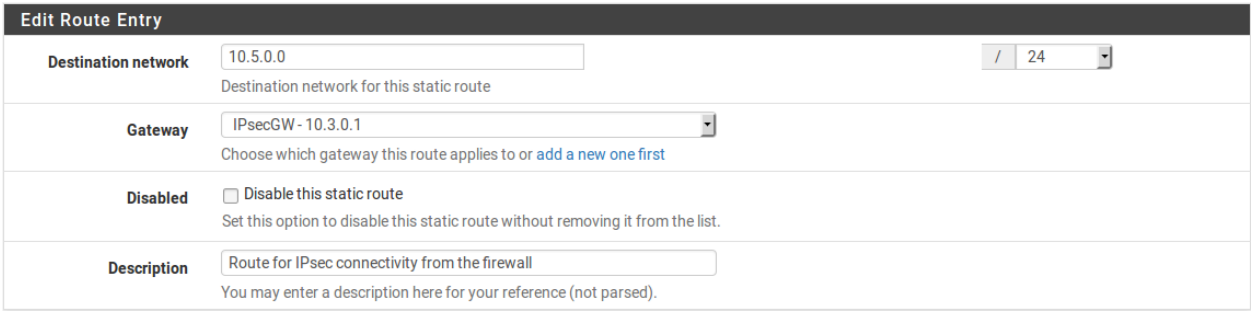


Fig. 15: Route statica per il Sito A alla sottorete remota

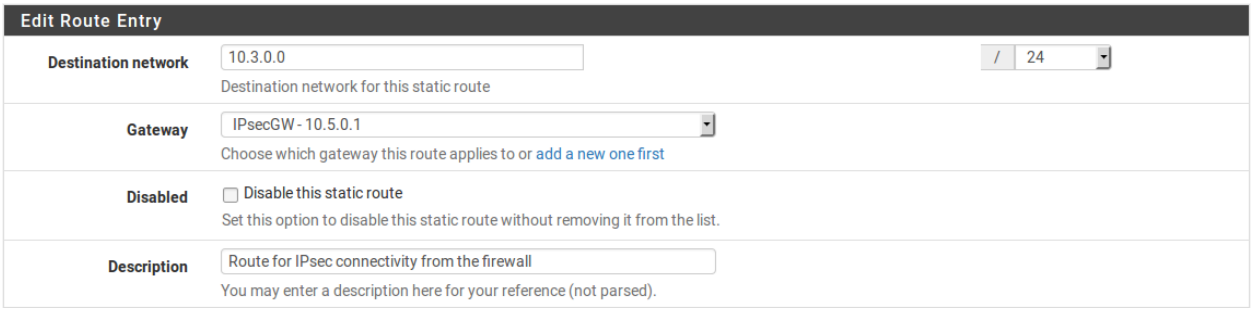


Fig. 16: Route statica per il Sito A alla sottorete remota

18.1.5 IPSec per I dispositivi mobili (Mobile IPsec)

Scegliere uno stile di IPsec per i dispositivi mobili

Attualmente solo un tipo di IPsec per dispositivi mobili può essere configurato alla volta, anche se ci sono diversi stili tra cui scegliere.

- IKEv2 con EAP-TLS per l'autenticazione del certificato per utente
- **IKEv2 con EAP-Mschapv2 per l'autenticazione locale di nome utente e** password
- **IKEv2 con EAP-RADIUS per l'autenticazione remota di nome utente e** password
- Xauth+PSK per l'autenticazione locale o remota di username e password
- **Xauth+RSA per i certificati e l'autenticazione locale o remota di** nome utente e password
- Chiave pre-condivisa per la connettività IPsec dai client più anziani
- **L2TP/IPsec per l'autenticazione locale o remota di nome utente e** password con i client che non supportano uno dei metodi di sopra.

A partire da questa scrittura, la maggior parte dei sistemi operativi **attuali** supporta nativamente IKEv2 o può utilizzare un'app/componente aggiuntivo. Attualmente è la scelta migliore, e sarà quella dimostrata più avanti in questo capitolo. Windows 7 e le versioni successive, MAC OS X 10.11 (El Capitan) e le versioni successive, iOS 9 e le versioni successive, e la maggior parte delle distribuzioni Linux hanno il supporto integrato per IKEv2. C'è una app con IKEv2 per strongSwan facile-da-usare per Android 4.x e seguenti versioni.

Nota: Tutti i tipi di IKEv2 richiedono una struttura di certificato comprendente almeno un'autorità di certificazione e un certificato server, e in alcuni casi certificati utente. Per ulteriori informazioni sui certificati, vedere *Gestione dei certificati*. I client possono essere molto esigenti sugli attributi dei certificati, quindi prestare molta attenzione a questo capitolo quando si crea la struttura dei certificati.

Avvertimento: Quando si genera un certificato server da utilizzare con IKEv2, il nome comune del certificato deve essere il nome del firewall così come esiste nel DNS. Il nome deve essere ripetuto di nuovo come denominazione alternativa del soggetto (Subject Alternative Name, SAN) di tipo FQDN. L'indirizzo IP del firewall deve essere presente anche come SAN di tipo indirizzo IP. Questa informazione sarà ripetuta più avanti nel capitolo, ma richiede ulteriore enfasi a causa della sua importanza. Vedere Creare un certificato server

IKEv2 con EAP-MSCHAPv2

Con il supporto per IKEv2 ormai diffuso, è una scelta ideale per i sistemi operativi attuali. Anche se ci sono diverse varianti, EAP-Mschapv2 è il più semplice da configurare in quanto non richiede la generazione o l'installazione di certificati per utente e non richiede un server RADIUS funzionante. Il certificato CA deve ancora essere installato sul client come certificato root attendibile.

EAP-Mschapv2 consente l'autenticazione di nome utente e password utilizzando le password memorizzate nella scheda **Chiavi pre-condivise** in **VPN>IPsec**. Queste password sono memorizzate in testo normale, quindi non è sicuro come utilizzare un server RADIUS, anche se è più conveniente.

IKEv2 con EAP-RADIUS

EAP-RADIUS funziona in modo identico a EAP-Mschapv2, tranne che l'autenticazione utente avviene tramite RADIUS. Quando si sceglie EAP-RADIUS, un server RADIUS deve trovarsi nella scheda **Client son dispositivi mobili**. Il server RADIUS deve accettare e comprendere le richieste EAP e deve anche consentire Mschapv2. La sicurezza della password è lasciata al server RADIUS.

EAP-RADIUS è in genere la scelta migliore quando è disponibile un server RADIUS.

IKEv2 con EAP-TLS

EAP-TLS utilizza l'autenticazione dei certificati per utente invece dell'autenticazione di nome utente e password. Come tale, EAP-TLS richiede la generazione di certificati per ogni utente, il che lo rende un po" più ingombrante dal punto di vista dell'amministrazione. I certificati sono convalidati con la CA in modo simile a OpenVPN. Il certificato CA, il certificato utente e la chiave associata devono essere tutti importati correttamente al client.

Avvertimento: Quando si creano i certificati utente, il nome utente deve essere usato come nome comune del certificato e di nuovo come denominazione alternativa del soggetto di tipo DNS/FQD. Se lo stesso nome non è presente in entrambi i luoghi, i client non possono essere validati correttamente.

IKEv1 con Xauth e chiavi pre-condivise

Xauth + PSK funziona sulla maggioranza di piattaforme, l'eccezione notevole sono le versioni attuali di Android. Windows XP attraverso Windows 8 può utilizzare il client di Shrew Soft, ma Windows 10 non funziona con qualsiasi client. OS X e iOS possono utilizzare il loro client integrato per connettersi.

Nota: Quando si utilizza Xauth, gli utenti locali devono esistere nella **gestione utenti** e tali utenti devono avere il privilegio di *dial-in di Xauth di IPsec della VPN per l'utente*.

IKEv1 con Xauth e certificati RSA

Xauth+RSA funziona nella maggior parte delle stesse condizioni di Xauth+PSK, anche se in realtà funziona su dispositivi Android correnti. I certificati devono essere redatti per ciascun utilizzatore e i certificati devono essere importati nei client.

IKEv1 con solo chiavi pre-condivise

Le VPN di IPsec con solo chiavi pre-condivise per Ipsec mobile sono diventate rare in tempi moderni. Il supporto non era molto comune, trovato solo nel client di Shrew Soft, alcune versioni molto specifiche di Android (come quelle di Motorola), e in altri client di terze parti. Non sono molto sicure e non sono più raccomandate per l'uso generale. L'unico momento in cui possono essere necessarie è nei casi in cui la parte lontana non può sostenere qualsiasi altro metodo.

L2TP/IPsec (IKEv1)

L2TP/IPsec è una combinazione unica che, purtroppo, non funziona molto bene nella maggior parte dei casi. In questo stile di configurazione, Mobile IPsec è configurato per accettare connessioni in modalità di trasporto che protegga

no tutto il traffico tra gli endpoint degli indirizzi IP pubblici. Attraverso questo canale di trasporto, viene effettuata una connessione L2TP al traffico degli utenti del tunnel in modo più flessibile. Anche se il supporto per questo modello si trova nella maggior parte delle versioni di Windows, MAC, Android e altri sistemi operativi, sono tutti pignoli in modi diversi incompatibili riguardo quello che funzionerà.

Ad esempio, il client Windows non funziona correttamente quando il sistema client è dietro il NAT, che è il luogo più comune in cui un client VPN si troverebbe. Il problema è nell'interazione tra il client e il demone IPsec usato su Firew4LL, strongSwan. Il progetto strongSwan afferma che si tratta di un bug nel client di Windows, ma è improbabile che sia risolto dal momento che invece sia strongSwan sia Windows hanno focalizzato i loro sforzi riguardo i client con dispositivi mobili su implementazioni più moderne e sicure come IKEv2.

Avvertimento: La combinazione L2TP/IPsec dovrebbe essere evitata quando possibile.

Esempio di configurazione del server IKEv2

Ci sono diversi componenti per la configurazione del server per i client mobili:

- Creare una struttura di certificati per la VPN
- Configurare le impostazioni di IPsec per i **client mobili**
- Creare la fase 1 e la fase 2 per la connessione del client
- Aggiungere le regole del firewall IPsec.
- Creare le credenziali dell'utente per la VPN

Struttura del certificato IKEv2

Creare un'autorità di certificazione

Avvertimento: Attenzione: Seguire queste indicazioni esattamente, prestando particolare attenzione a come il certificato del server viene creato ad ogni passo. Se una parte non è corretta, alcuni o tutti i client potrebbero non riuscire a connettersi.

Se un'autorità di certificazione (CA) idonea non è presente nella gestione dei certificati, crearne una è il primo compito:

- Passare a **Sistema>Gestione certificati** sul firewall Firew4LL
- Fare clic su  **Aggiungere** per creare una nuova autorità di certificazione
- Selezionare *Creare un'autorità di certificazione interna* per il **metodo**
- Compilare il resto dei campi a piacere con informazioni specifiche dell'azienda o del sito
- Fare clic su **Salvare**

Creare un certificato del server

Avvertimento: Seguire queste indicazioni esattamente, prestando particolare attenzione a come il certificato del server viene creato ad ogni passo. Se una parte non è corretta, alcuni o tutti i client potrebbero non riuscire a connettersi.

- Passare a **Sistema>Gestione dei certificati**, scheda **Certificati** sul firewall Firew4LL
- Fare clic su  **Aggiungere** per creare un nuovo certificato
- Selezionare *Creare un certificato interno* per il **metodo**
- Inserire un **nome descrittivo** come Server IKEv2
- Selezionare l'**autorità di certificazione** appropriata creata nella fase precedente
- Scegliere la **lunghezza della chiave** desiderata, l'**algoritmo Digest** e la **durata di vita**
- Impostare il **tipo di certificato** sul *certificato del server*
- Inserire i valori regionali e aziendali nei campi **Distinguished Name** come desiderato, vengono copiati dalla CA e possono essere lasciati così come sono
- Immettere il **nome comune** come hostname del firewall esistente nel DNS. Se i client si connettono tramite l'indirizzo IP, posizionare l'indirizzo IP qui
- Fare clic su  **Aggiungere** per aggiungere un nuovo **nome alternativo**
- Inserire DNS nel campo **Tipo**
- Immettere nuovamente l'hostname del firewall *come esiste nel DNS* **di nuovo** nel campo **Valore**
- Fare clic su  **Aggiungere** per aggiungere un altro nuovo **nome alternativo**
- Inserire IP nel campo **Tipo**
- Immettere l'indirizzo IP della WAN del firewall nel campo **Valore**
- Aggiungere altri **nomi alternativi** necessari per nomi host o indirizzi IP aggiuntivi sul firewall che i client possono utilizzare per connettersi
- Fare clic su **Salvare**

Impostazioni del client sui dispositivi mobili

Prima di configurare un'istanza per IPsec mobile, scegliere prima un intervallo di indirizzi IP da utilizzare per i client mobili. Assicurarsi che gli indirizzi IP non si sovrappongano a qualsiasi rete esistente; gli indirizzi IP devono differire da quelli in uso presso il sito che ospita il tunnel mobile e la LAN da cui il client si connetterà. In questo esempio, verrà utilizzato *10.3.200.0/24*, ma può essere qualsiasi sottorete non utilizzata.

In primo luogo, abilitare IPsec sul firewall se non è già stato abilitato:

- Passare a VPN>IPsec
- Selezionare Abilitare IPsec
- Fare clic su Salvare

Anche il supporto per i client dei dispositivi mobili deve essere abilitato:

- Passare a VPN>Ipsec
- Fare clic sulla scheda client mobili (figura *Abilitare i client di Ipsec sui dispositivi mobili*).
- Selezionare Abilitare il supporto per IPsec dei client mobili

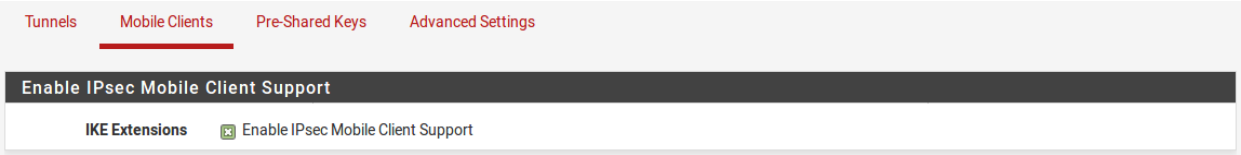


Fig. 17: Abilitare i client di Ipsec sui dispositivi mobili

- Lasciare le fonti di autenticazione impostate sul *Database locale*, come visto nella figura *Autenticazione dei client sui dispositivi mobili.* Questa impostazione non è necessaria per EAP-MSCHAPv2, ma deve avere selezionato qualcosa. I server RADIUS definiti nella gestione utente (*Autenticazione e gestione dell'utente*) possono essere selezionati qui per l'autenticazione degli utenti quando si utilizza EAP-RADIUS.

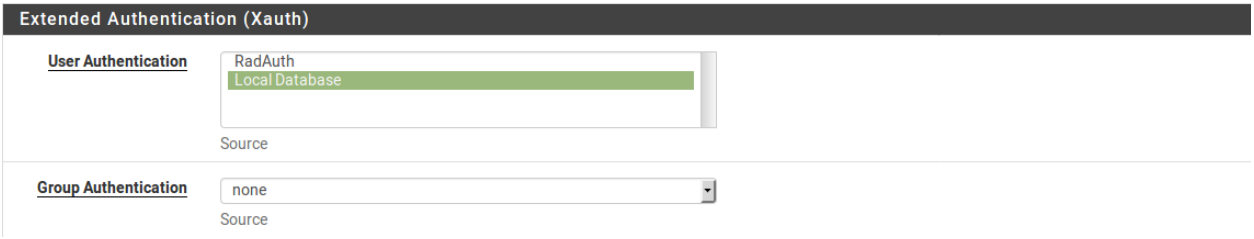


Fig. 18: Autenticazione dei client sui dispositive mobili

Alcune impostazioni possono essere inviate al client, come l'indirizzo IP del client e i server DNS. Queste opzioni sono mostrate nella figura *Impostazioni dei push dei client sui dispositivi mobili*. Il supporto per queste opzioni varia tra i client, ma è comune e ben supportato nella maggior parte dei sistemi operativi attuali.

Pool degli indirizzi virtuali Definisce il pool di indirizzi IP che saranno distribuiti ai clienti. Usare 10.3.200.0/24 in questo esempio.

Pool degli indirizzi virtuali IPv6 Come sopra, ma per gli indirizzi Ipv6.

Elenco di reti Controlla se il client tenterà di inviare tutto il suo traffico attraverso il tunnel, o solo il traffico per reti specifiche. Se questa opzione è selezionata, le reti definite nelle opzioni **Rete Locale** per le definizioni della fase 2 per i dispositivi mobili saranno inviate al client. Se questa opzione è deselezionata, i client tenteranno di inviare tutto il loro traffico, compreso il traffico Internet, attraverso il tunnel. Non tutti i client rispettano questa opzione. Per questo esempio, il client può raggiungere la rete solo nella fase 2, quindi selezionare questa opzione.

Salvare la password di Xauth Quando selezionato, i client che supportano questo controllo permetterà all'utente di salvare le proprie credenziali quando utilizza Xauth. Questo è rispettato principalmente dai client basati su Cisco come quello che si trovano su iOS e Mac OS X. Dal momento che IKEv2 viene utilizzato in questo esempio, non è importante.

Dominio predefinito DNS Quando selezionato, il valore inserito nella casella verrà inviato ai client come suffisso di dominio predefinito per le richieste DNS. Per esempio se questo è impostato su esempio.com e un client richiede l'host, allora la richiesta DNS sarà tentata per host.esempio.com.

DNS diviso Controlla come il client invierà le richieste DNS al server DNS fornito (se presente). Se questa opzione non è selezionata, il client invierà tutte le sue richieste DNS a un server DNS fornito. Se l'opzione è selezionata, ma lasciata vuota, e un **dominio predefinito DNS** è impostato, allora solo le richieste per quel nome di dominio andranno al server DNS fornito. Se è selezionato e viene inserito un valore, allora solo le richieste per il dominio inserito (domini inseriti) nella casella saranno inoltrate al

server DNS fornito. In questo esempio, vengono utilizzati sia esempio.com che esempio.org e le richieste DNS per questi due domini andranno ai server VPN, quindi inserire questi valori separati da uno spazio.

Server DNS Quando viene selezionato **Fornire un elenco di server DNS ai client**, e vengono inseriti indirizzi IP per i server DNS locali, come 10.3.0.1, questi valori vengono inviati ai client per l'uso mentre la VPN è connessa.

Nota:

Se i client mobili si collegano a Internet tramite la VPN, assicurarsi che i client ottengano un server DNS dal firewall utilizzando questa opzione, e che non abbiano il **DNS diviso** abilitato. Se questo non viene fatto, il client tenterà di ottenere il DNS da qualsiasi server sia stato assegnato dal loro ISP, piuttosto che instradare la richiesta attraverso il tunnel e molto probabilmente fallirà.

Server WINS Funziona in modo simile ai server DNS, ma per le WINS. Raramente usato al giorno d'oggi, meglio lasciarlo disattivato.

Gruppo PFS di fase 2 Sovrascrive l'impostazione PFS per tutte le voci della fase 2 per mobili. Generalmente è meglio impostare questo valore sulle voci di P2 singolarmente, quindi lasciarlo deselezionato.

Banner del login Opzionale e funziona solo sui client Xauth. Lasciarlo deselezionato e vuoto.

- Fare clic su **Salvare** e Firew4LL visualizzerà un avviso che non è una definizione di fase 1 per i client mobili
- Fare clic su **Creare la fase 1** per realizzare una nuova voce di fase 1 per i client mobili (Figura *Prompt per la creazione della fase 1 dei client sui dispositivi mobili*)
- Fare clic sulla scheda **Tunnel**

La configurazione della fase 1 per i client mobili è presente e deve essere configurata come segue:

Versione di scambio della chiave Impostare su *V2*

Protocollo Internet Impostare su *IPv4* per questo esempio

Interfaccia Impostare su *WAN*

Descrizione Impostare di IPsec Mobile

Metodo di autenticazione Impostare su *EAP-MSCHAPv2*

Mio identificatore Scegliere il *Distinguished Name* dall'elenco a discesa e quindi inserire l'hostname del firewall, come è stato inserito nel certificato del server, vpn.esempio.com

Identificatore di peer Impostare su *qualsiasi*

Mio certificato Scegliere il certificato del server IPsec creato in precedenza

Mia autorità di certificazione Scegliere l'autorità di certificazione creata in precedenza

Algoritmo di crittografia Impostare su *3DES* (o *AES 256* se non ci sono dispositivi iOS/OS X)

Algoritmo di hash deve essere impostato su *SHA1* (o *SHA256* se non ci sono dispositivi iOS/OS X)

Gruppo di chiavi DH Deve essere impostato a *2 (1024 bit)*

Durata di vita Deve essere impostata su 28800

Disabilitare Rekey Lasciare non selezionato

Disabilitare Reauth Lasciare non selezionato

Solo risponditore Lasciare non selezionato

MOBIKE Impostare su *Abilitare* per consentire ai client di spostarsi tra indirizzi IP, altrimenti impostarlo su *Disabilitare*.

- Fare clic su **Salvare**
- Fare clic su **Mostrare voci di fase 2** per espandere l'elenco delle voci di fase 2 per i dispositivi mobili
- Fare clic su **Aggiungere P2** per aggiungere una nuova fase 3 per i dispositivi mobili.

  La figura *Fase 2 dei client sui dispositivi mobili* mostra le opzioni della fase 2 per questo tunnel mobile.

  Modalità Impostare su *tunnel IPv4*

  Rete locale Impostare su *sottorete LAN* o un'altra rete locale. Per effettuare il tunnel su tutto il traffico attraverso la VPN, utilizzare *Rete* e inserire 0.0.0.0 con una maschera di *0*

  NAT/BINAT Impostare su *nessuno*

  Protocollo impostare su *ESP*, che cripterà il traffico del tunnel

  Algoritmi di crittografia Deve essere impostato su *AES* con *Automatico* selezionato per la lunghezza della chiave. Selezionare anche *3DES* se un client su iOS o OS X si connetterà.

  Algoritmi di hash Selezionare *SHA1* e *SHA256*

  PFS Deve essere impostato su *off*

  Durata di vita Impostare su 3600
- Fare clic su **Salvare**
-

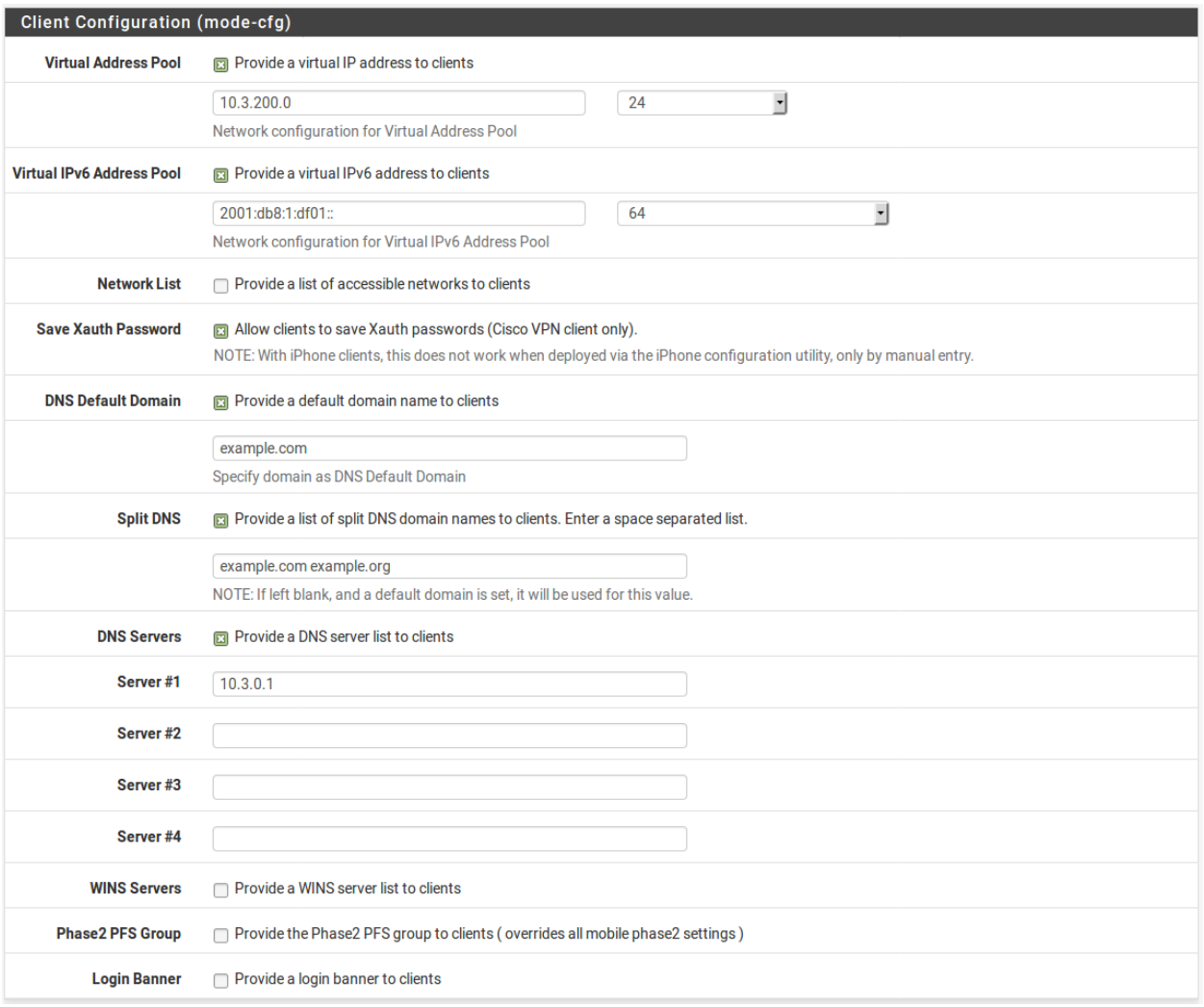


Fig. 19: Impostazioni dei push dei client sui dispositivi mobili

Fig. 20: Prompt per la creazione della fase 1 dei client sui dispositivi mobili

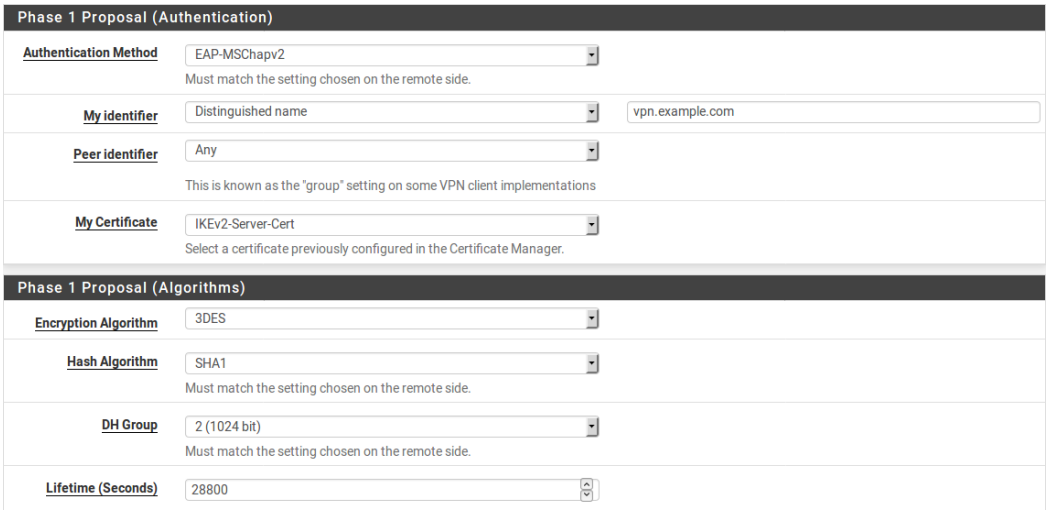


Fig. 21: Fase 1 dei client sui dispositivi mobili

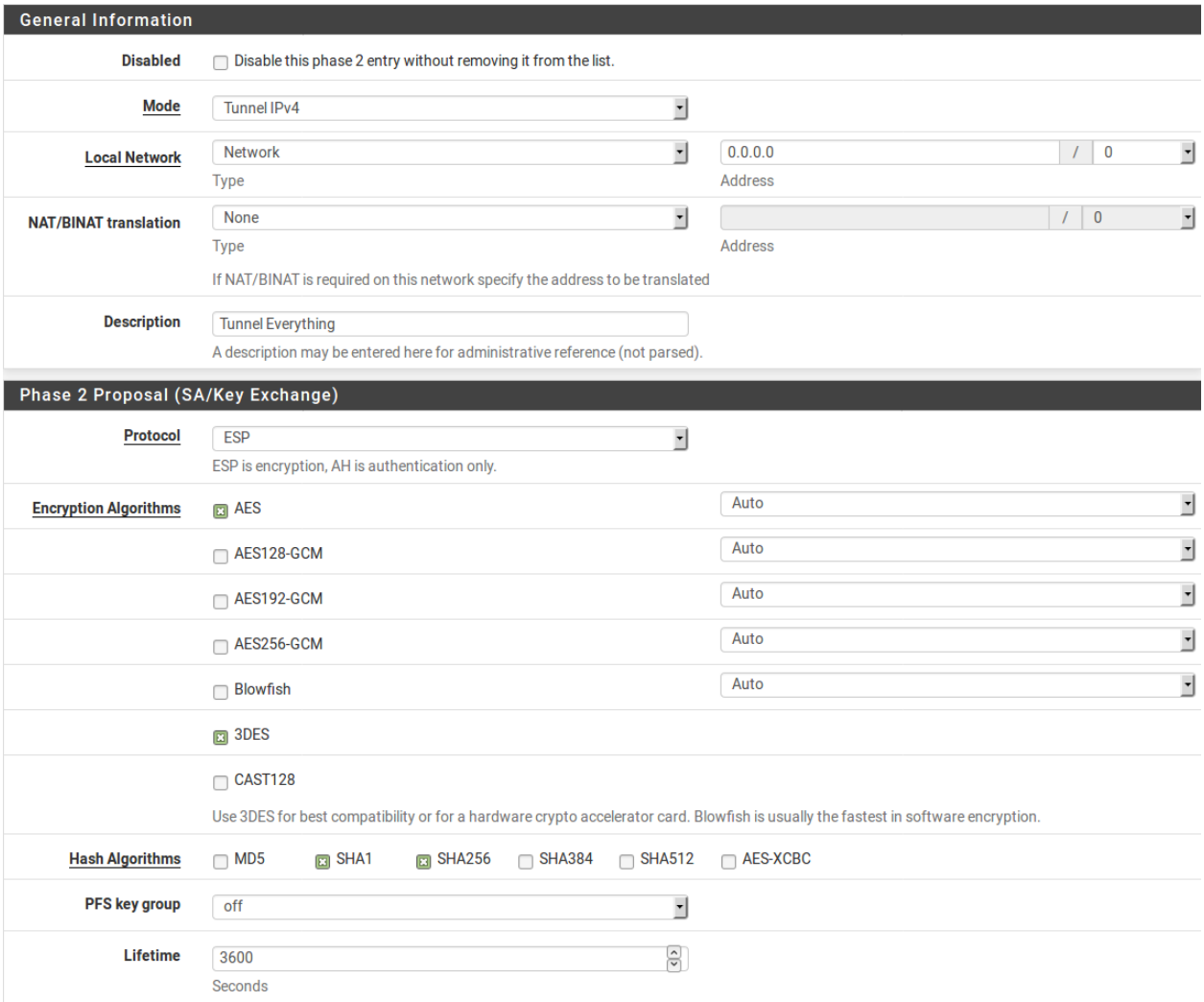


Fig. 22: Fase 2 dei client sui dispositivi mobili

- Fare clic su **Applicare modifiche** (Figura *Applicare le impostazioni del tunnel per i dispositivi mobili*) e quindi

la configurazione tunnel per i client mobili è completa.

Fig. 23: Applicare le impostazioni del tunnel per i dispositivi mobili

Creazione dell'utente su Ipsec per i dispositivi mobili

Il prossimo passo è quello di aggiungere utenti per l'uso da parte di EAP-MSCHAPv2.

- Passare a **VPN>IPsec**, scheda **Chiavi pre-condivise**
- Fare clic su **Aggiungere** per aggiungere una nuova chiave
- Configurare le opzioni come segue:

  Identificatore Il nome utente per il client, può essere espresso in più modi, come ad esempio un indirizzo e-mail come *jimp@esempio.com*

  Tipo segreto Impostare su *EAP* per gli utenti EAP-MSCHAPv2

  Chiave pre-condivisa La password per il client, ad esempio abc123
- Fare clic su **Salvare**
- Ripetere tutte le volte necessarie per gli utenti VPN aggiuntivi.

  Un utente completo è mostrato nella figura *Utente IPsec per dispositivi mobili*.

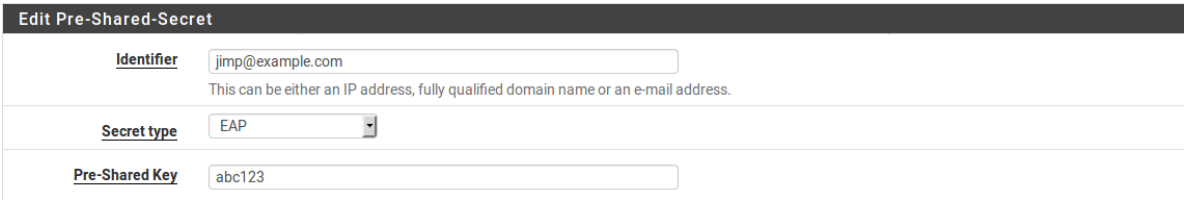


Fig. 24: Utente IPsec per dispositivi mobili

Regole del firewall

Come per i tunnel statici con l'opzione sito-a-sito, anche i tunnel mobili avranno bisogno di regole di firewall aggiunte alla scheda **IPsec** in **Firewall>Regole**. In questo caso la sorgente del traffico sarebbe la sottorete scelta per i client mobili e la destinazione sarà la rete LAN, o *qualsiasi* se tutto il traffico effettua il tunnel. Per maggiori dettagli, *regole di firewall e IPsec*.

Configurazione client

Ogni client mobile dovrà avere un'istanza VPN aggiunta. In alcuni casi può essere richiesto un client Ipsec di terze parti. Ci sono molti client di IPsec diversi disponibili per l'uso, alcuni gratuiti e alcune applicazioni commerciali. Con IKEv2, come usato in questo esempio, molti sistemi operativi hanno client VPN nativi e non hanno bisogno di software extra.

Configurazione del client IKEv2 per windows

Windows 8 e versioni successive supportano facilmente le VPN di IKEv2 e Windows 7 anche se i processi sono leggermente diversi. La procedura in questa sezione è stata eseguita su Windows 10, ma per Windows 8 è quasi identica. La procedura per importare i certificati in Windows 7 può essere trovata sulla Wiki di strongSwan

Importare la CA sul PC del client

- Esportare il certificato CA da Firew4LL e scaricarlo o copiarlo sul PC del client:
  - Passare a **Sistema>Gestione dei certificati**, scheda **Autorità di certificazione** su Firew4LL
  - Cliccare su  dalla CA per scaricare solo il certificato
- Individuare il file scaricato sul PC del client (ad es. VPNCA.crt) come visualizzato dalla figura *Certificato CA scaricato*

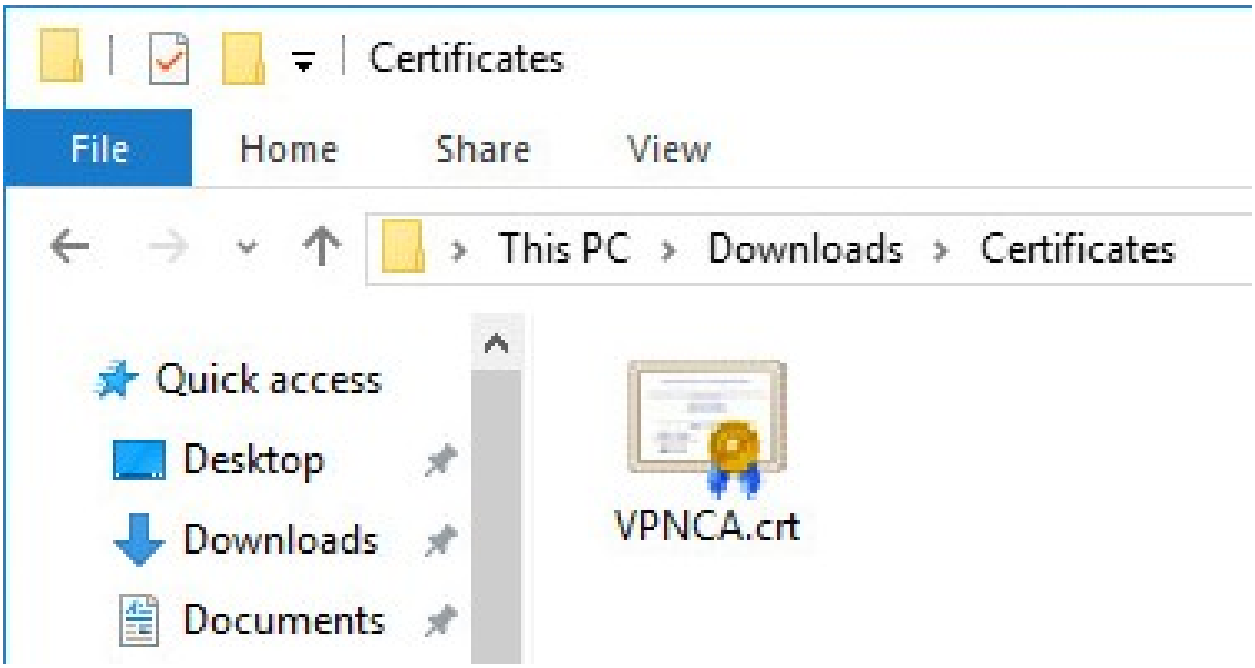


Fig. 25: Certificato CA scaricato

- Fare doppio clic sul file CA
- Fare clic su **Installare certificato**... come mostrato in *proprietà del certificato*
- Selezionare la **macchina locale** come mostrato in *procedura guidata di importazione dei certificati - Posizione negozio*
- Fare clic su **Avanti**
- Fare clic su **Sì** al prompt UAC se appare
- Selezionare **Posizionare tutti i certificati nel seguente negozio**, come mostrato in *procedura guidata di importazione dei certificati – Sfogliare nel negozio*
- Cliccare *Sfogliare*
- Fare clic su **Autorità di certificazione della root fidata** come mostrato in figura *Selezionare il negozio del certificato*

- Fare clic su **Avanti**
- Rivedere i dettagli, dovrebbero corrispondere a quelli in figura *Completare la procedura guidata per l'importazione del certificato *
- Fare clic su **Fine**
- Fare clic su **OK**

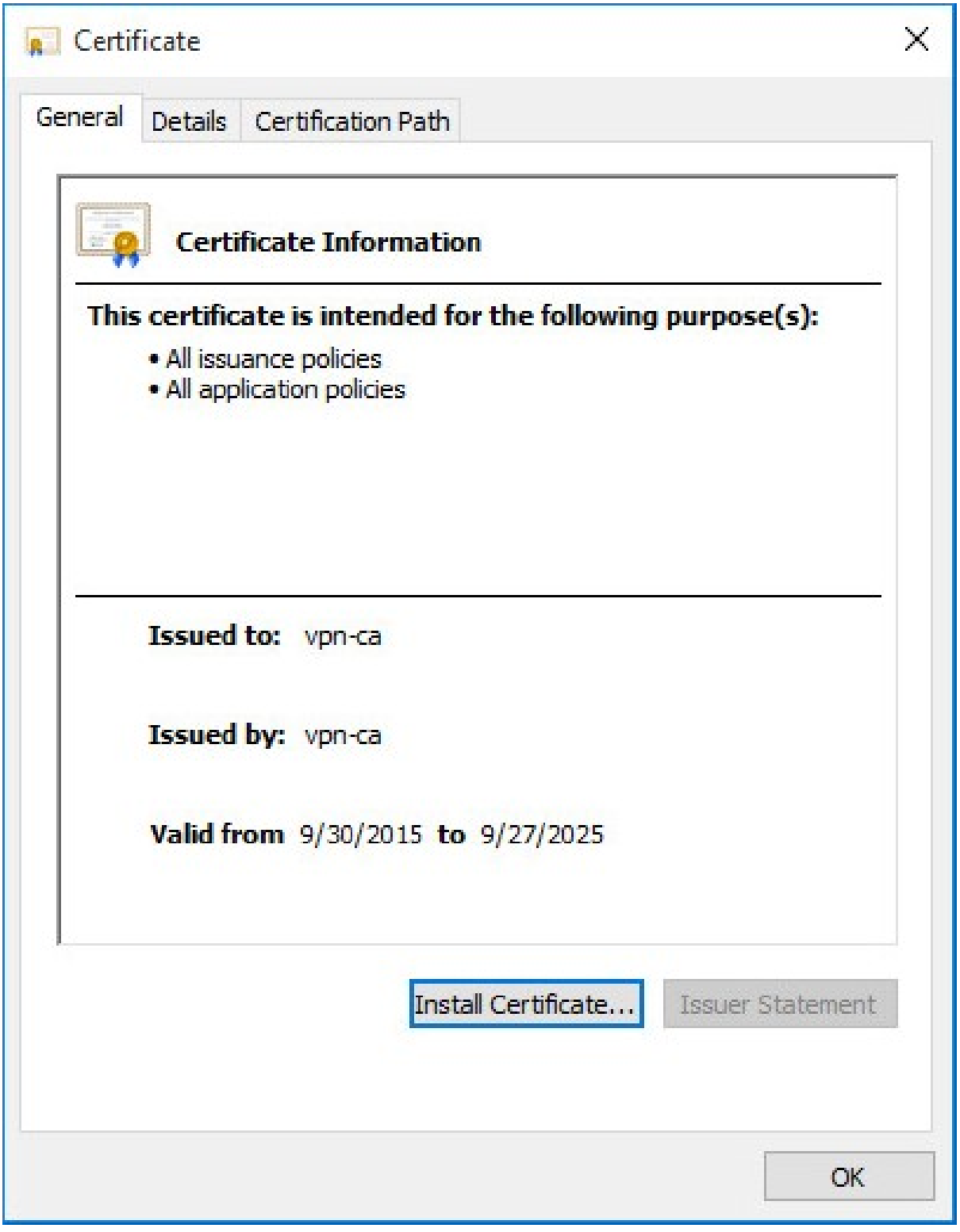


Fig. 26: Proprietà certificato

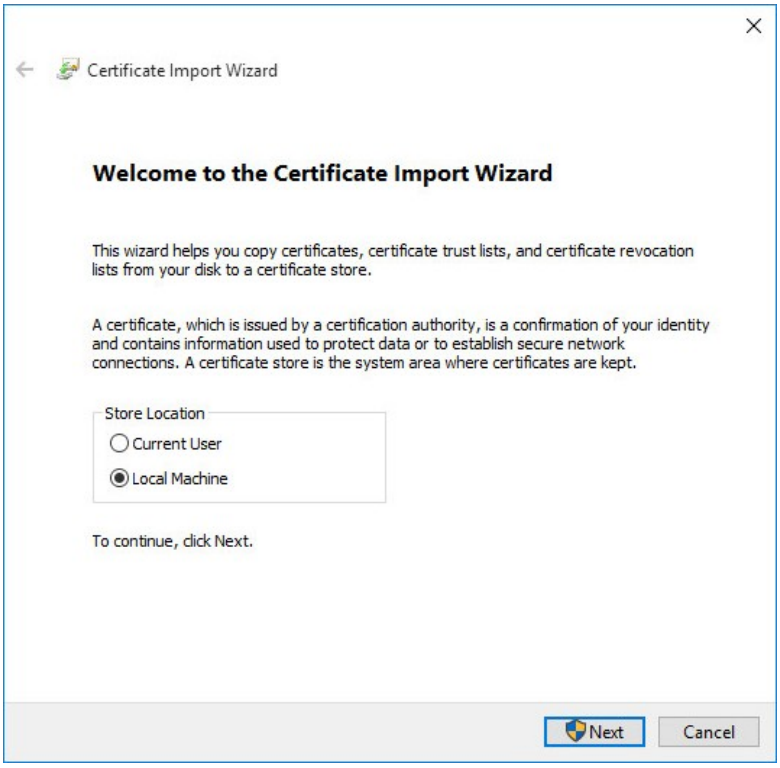


Fig. 27: Procedura guidata di importazione dei certificati - Posizione negoz

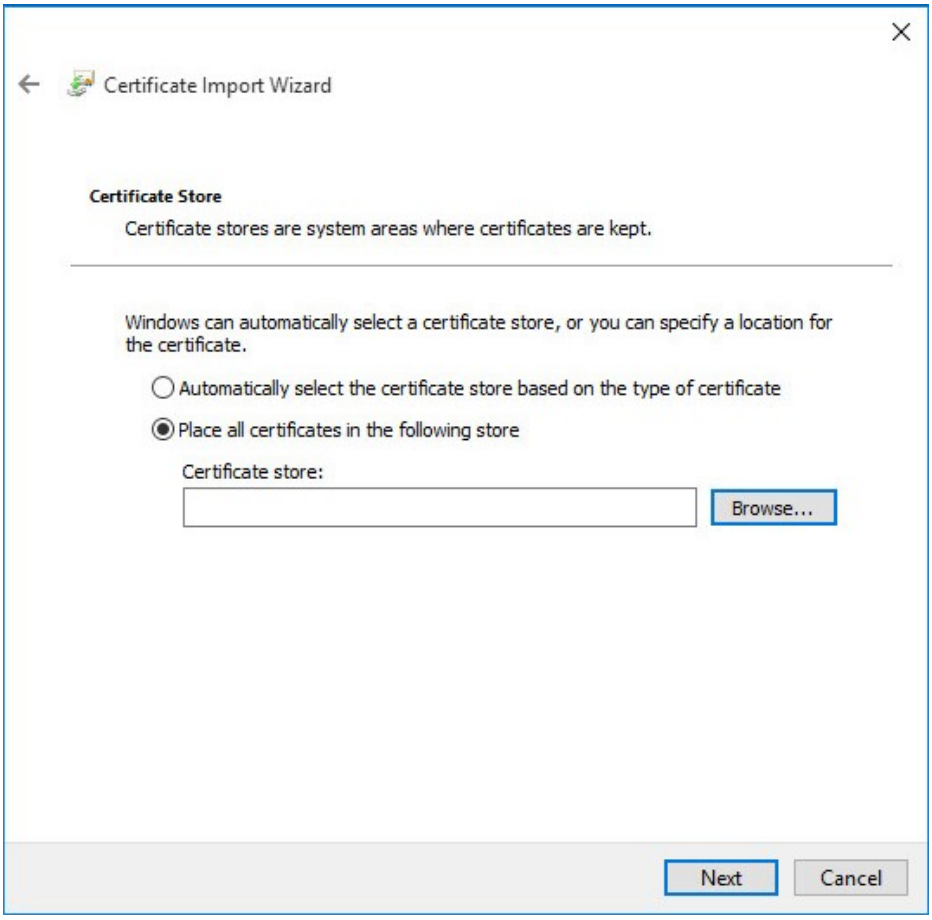


Fig. 28: Procedura guidata di importazione dei certificati – Navigare nel negozio

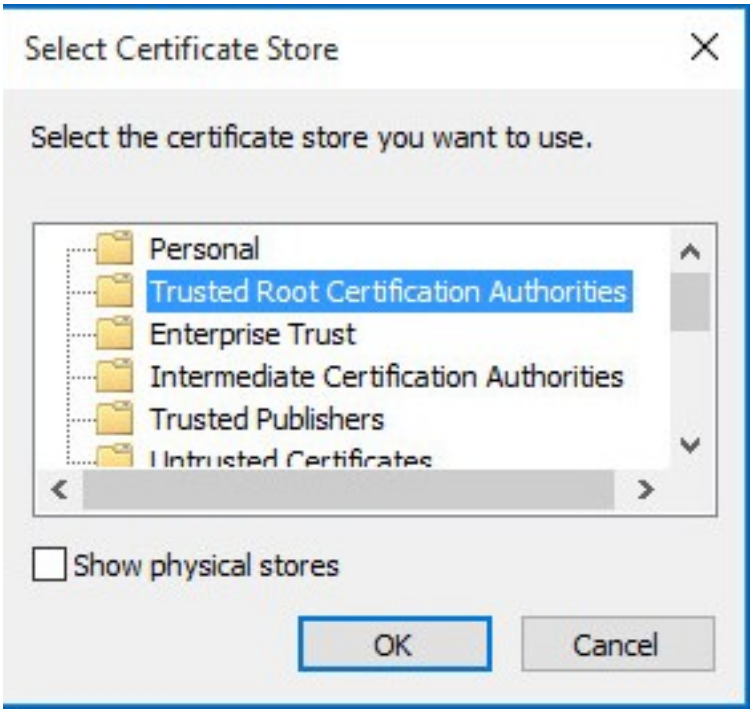


Fig. 29: Selezionare il negozio del certificato

- Fare click su **OK**

Impostare la connessione VPN

Una volta che il certificato è stato correttamente importato è il momento di creare la connessione VPN dei client. I passaggi esatti variano a seconda della versione di Windows utilizzata dal client, ma saranno simili alla seguente procedura.

- Aprire **rete e centro di condivisione** sul PC client
- Fare clic su **Impostare una nuova connessione o rete**
- Seleziona **Connettersi a un posto di lavoro**
- Fare clic su **Avanti**
- Selezionare **No, creare una nuova connessione**
- Fare clic su **Avanti**
- Fare clic su **Usare la mia connessione Internet (VPN)**
- Inserire l'indirizzo IP o l'hostname del server nel campo **Indirizzo Internet**, come mostrato nella figura *Schermata di configurazione della connessione VPN di IKEv2 per Windows*

Nota: Questo deve corrispondere a ciò che è il nome comune nel certificato del server o la denominazione alternativa del soggetto!

- Immettere un **nome di destinazione** per identificare la connessione
- Fare clic su **Creare**

La connessione è stata aggiunta ma con diverse impostazioni predefinite non desiderabili. Ad esempio il tipo predefinito è *automatico*. Alcune impostazioni devono essere impostate a mano prima per garantire che una connessione corretta sia realizzata. Fare riferimento alla figura *Proprietà di connessione VPN di IKEv2 per Windows*

- In **Connessioni di rete/Impostazioni dell'adattatore in Windows**, trovare la connessione creata sopra
- Fare clic con il tasto destro del mouse sulla connessione
- Cliccare su **proprietà**
- Fare clic sulla scheda **Sicurezza**
- Impostare il **tipo di VPN** su *IKEv2*
- Impostare **crittografia dei dati** su *richiedere la crittografia (disconnettere se il server declina)*
- Impostare **Autenticazione/Usare il protocollo di autenticazione estensibile** per *Microsoft: Password sicura (EAP-MSCHAP v2) (crittografia abilitata)*
- Confrontare i valori sullo schermo a quelli nella figura *Proprietà di connessione VPN con IKEv2 per Windows*
- Fare clic su **OK**

La connessione è ora pronta per l'uso.

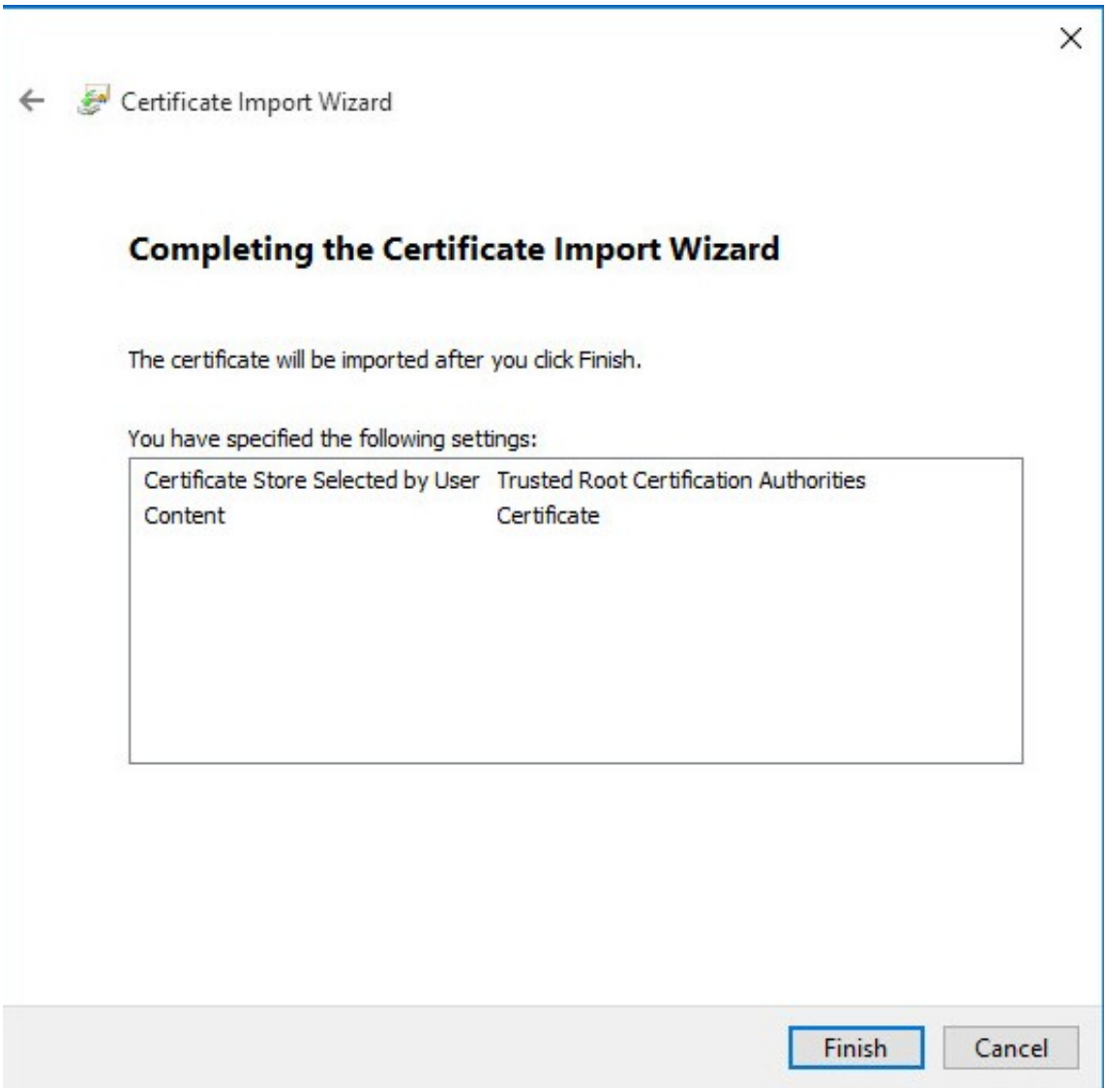


Fig. 30: Completare la procedura guidata per l'importazione del certificato

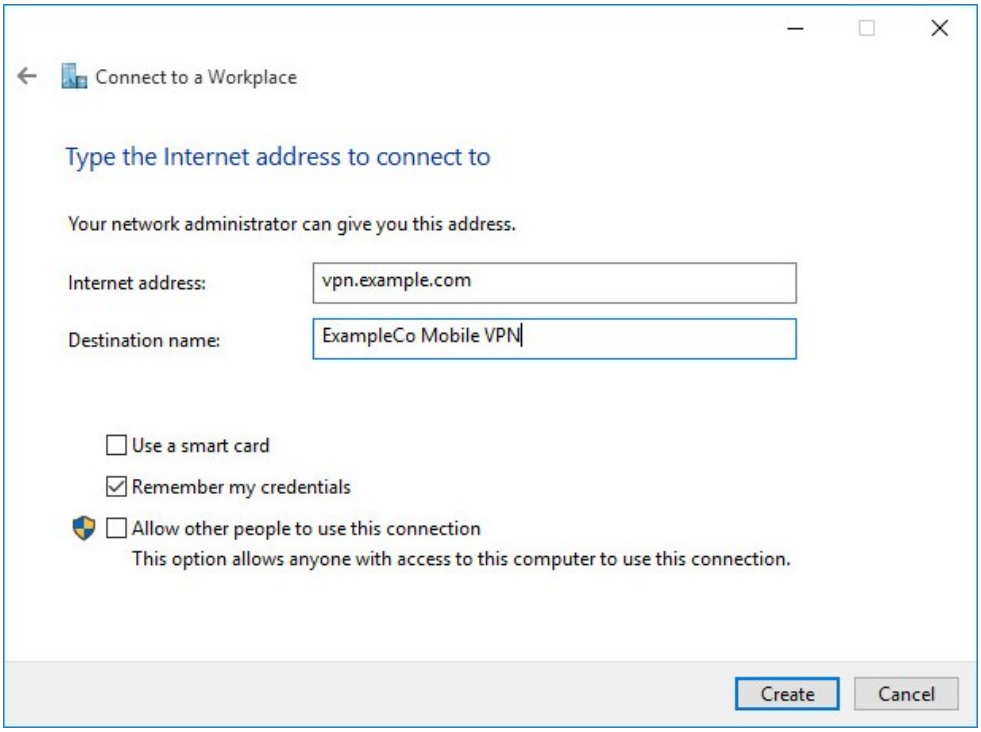


Fig. 31: Schermata di configurazione della connessione VPN di IKEv2 per Windows

Disabilitare il controllo EKU

Quando i certificati CA e del server sono realizzati correttamente su Firew4LL, questo non è necessario. Se un certificato di server generato impropriamente deve essere utilizzato per qualche motivo, allora il controllo di utilizzo della chiave estesa potrebbe essere disabilitato su Windows. Disabilitando questo controllo si disabilita anche la convalida del nome comune del certificato e dei campi SAN, quindi è potenzialmente pericoloso. Qualsiasi certificato della stessa CA potrebbe essere utilizzato per il server quando questo è disabilitato, quindi procedere con cautela. Per disabilitare i controlli di utilizzo della chiave estesa, aprire l'**editor del registro** di sistema sul client Windows e passare alla posizione seguente nel registro client:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasMan\Parameters\
```

Lì dentro, aggiungi una nuova voce **DWORD** chiamata **DisabilitareControlloEkuDelNomeIKE** e impostarla a 1.

Potrebbe essere necessario un riavvio per attivare l'impostazione.

Configurazione del client di IKEv2 basata su Ubuntu

Prima di iniziare, installare **strongswan-gestione-rete** e **strongswan-plugin-eap-mschapv2** usando apt-get o un meccanismo simile.

Impostare la connessione VPN

- Copiare il certificato CA per la VPN dal firewall alla workstation
- Fare clic sull'icona **Gestione di rete** nella barra delle notifiche dell'orologio (l'icona varia a seconda del tipo di rete in uso)

- Fare clic su **connessioni di rete**
- Fare clic su **Aggiungere**
- Selezionare *IPsec/IKEv2 (strongswan)* sotto **VPN** come mostrato in *Aggiungere una VPN con IKEv2 su Ubuntu*

Nota: Se l'opzione non è presente, controllare due volte che sia installato **strongswan-gestione-rete**.

- Fare clic su **Creare**
- Inserire una **descrizione** (ad es. VPN mobile EsempioCo)
- Selezionare la scheda **VPN**
- Inserire l'**indirizzo** del firewall (ad es. vpn.esempio.com)
- Selezionare il controllo accanto a **Certificato** e sfogliare per trovare il certificato CA scaricato
- Selezionare *EAP* per l'**autenticazione**
- Inserire il **nome utente** da usare per questa connessione (ad es. alice)
- Fare click su **Richiedere un indirizzo IP interno**
- Confrontare le impostazioni con quelle mostrate nella figura *Impostazioni del cliente della VPN su Ubuntu*
- Fare clic su **Salvare**
- Fare clic su **Chiudere**

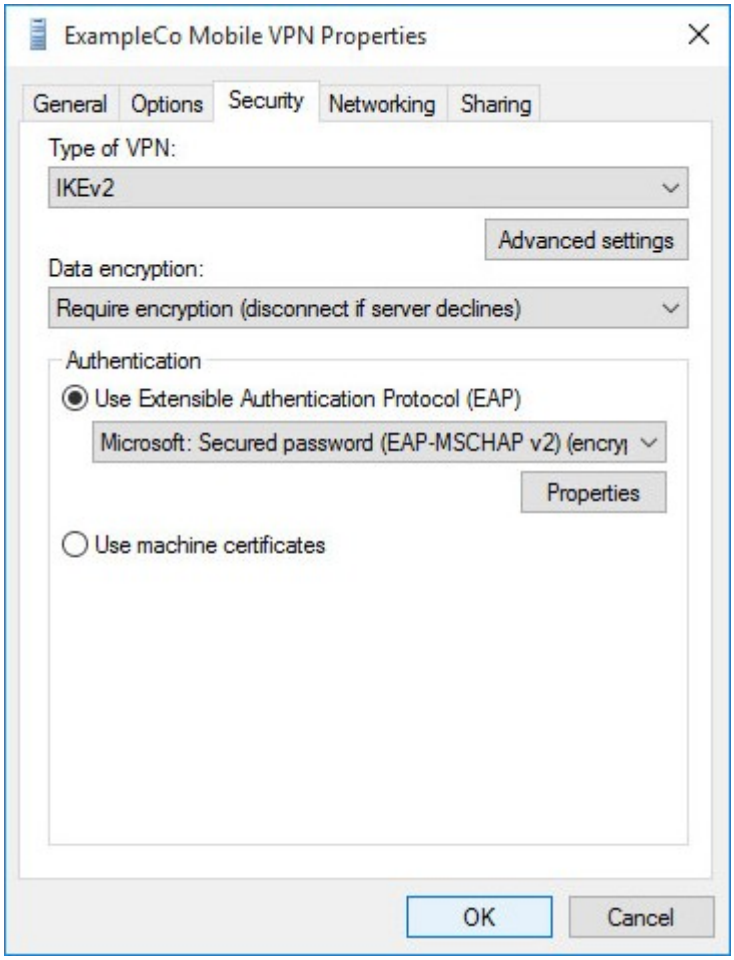


Fig. 32: Proprietà di connessione VPN con IKEv2 per Windows

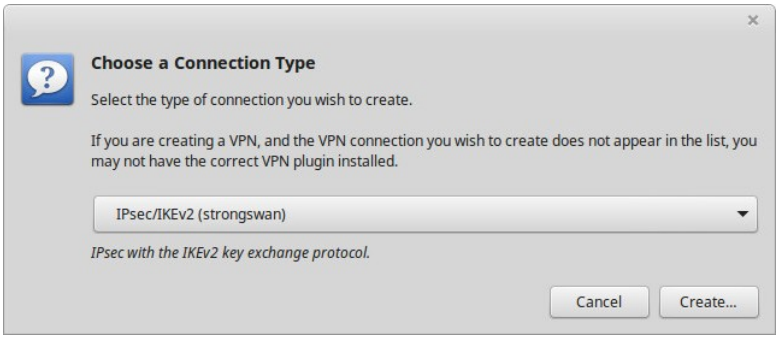


Fig. 33: Aggiungere una VPN con IKEv2 su Ubuntu

Connettersi e disconnettersi

Per connettersi:

- Fare clic sull'icona della **gestione di rete**
- Fare clic sul nome della VPN o su **Connessioni VPN** per spostare il cursore nella posizione *On (1)*

Nota: Se non viene visualizzata una richiesta di password, potrebbe essere necessario riavviare il servizio di gestione di rete o riavviare la stazione di lavoro.

Per disconnettersi:

- Fare clic sull'icona della **gestione di rete**
- Fare clic su **Connessioni VPN** per spostare il cursore nella posizione *Off (0)*

Fig. 34: Impostazioni del cliente della VPN su Ubuntu

1. **Configurazione del client per IKEv2 per strongSwan di Android**

Nota: Android considera l'utilizzo di una VPN un'azione che deve essere sicura. Quando si attiva qualsiasi opzione VPN il sistema operativo costringerà l'utente ad aggiungere una qualche forma di blocco al dispositivo se non è già presente. Non importa quale tipo di blocco è scelto (PIN di blocco, modello di blocco,Password, ecc) purché non si permetta di configurare una VPN fino a quando non è stato aggiunto un blocco sicuro. Su dispositivi Android con il blocco con il viso, non è disponibile come tipo di blocco sicuro.

Prima di iniziare, installare l'app strongSwan dal Play Store:

Impostare la connessione VPN

- Copiare il certificato CA sul dispositivo
- Aprire l'app strongSwan
- Importare la CA:

  - Toccare l'icona delle impostazioni (i tre punti verticali in alto a destra)
  - Toccare i **certificati CA**
  - Toccare l'icona delle impostazioni (i tre punti verticali in alto a destra)
  - Toccare **Importare certificazione**
  - Individuare il certificato CA copiato in precedenza e sfiorarlo.
- Toccare **Aggiungere profilo VPN**
- Immettere un **nome del profilo** (opzionale, se lasciato vuoto, verrà utilizzato l'indirizzo del gateway)
- Immettere l'indirizzo del firewall come **Gateway** (ad es. vpn.esempio.com)
- Selezionare *IKEv2 EAP (nome utente/password)* per il **tipo**
- Inserire il **nome utente**
- Inserire la **password** per ricordarla o lasciarla vuota per chiedere la password su ogni connessione.
- Controllare Selezionare automaticamente sotto Certificato CA
- Confrontare le impostazioni della figura *Impostazioni del client di strongSwan su Android*

Connettersi e disconnettersi

Per connettersi:

- Aprire l'app strongSwan
- Toccare la VPN desiderata
- Selezionare **Mi fido di questa applicazione** sul prompt della sicurezza, come mostrato nella figura *Impostazioni del client di strongSwan su Android*
- Toccare **OK**

  Per disconnettersi:
- Scorrere verso il basso dalla barra di notifica superiore
- Toccare la voce strongSwan nell'elenco delle notifiche
- Toccare Scollegare

  In alternativa:
- Aprire l'app strongSwan
- Toccare **Disconnettere** sulla VPN desiderata

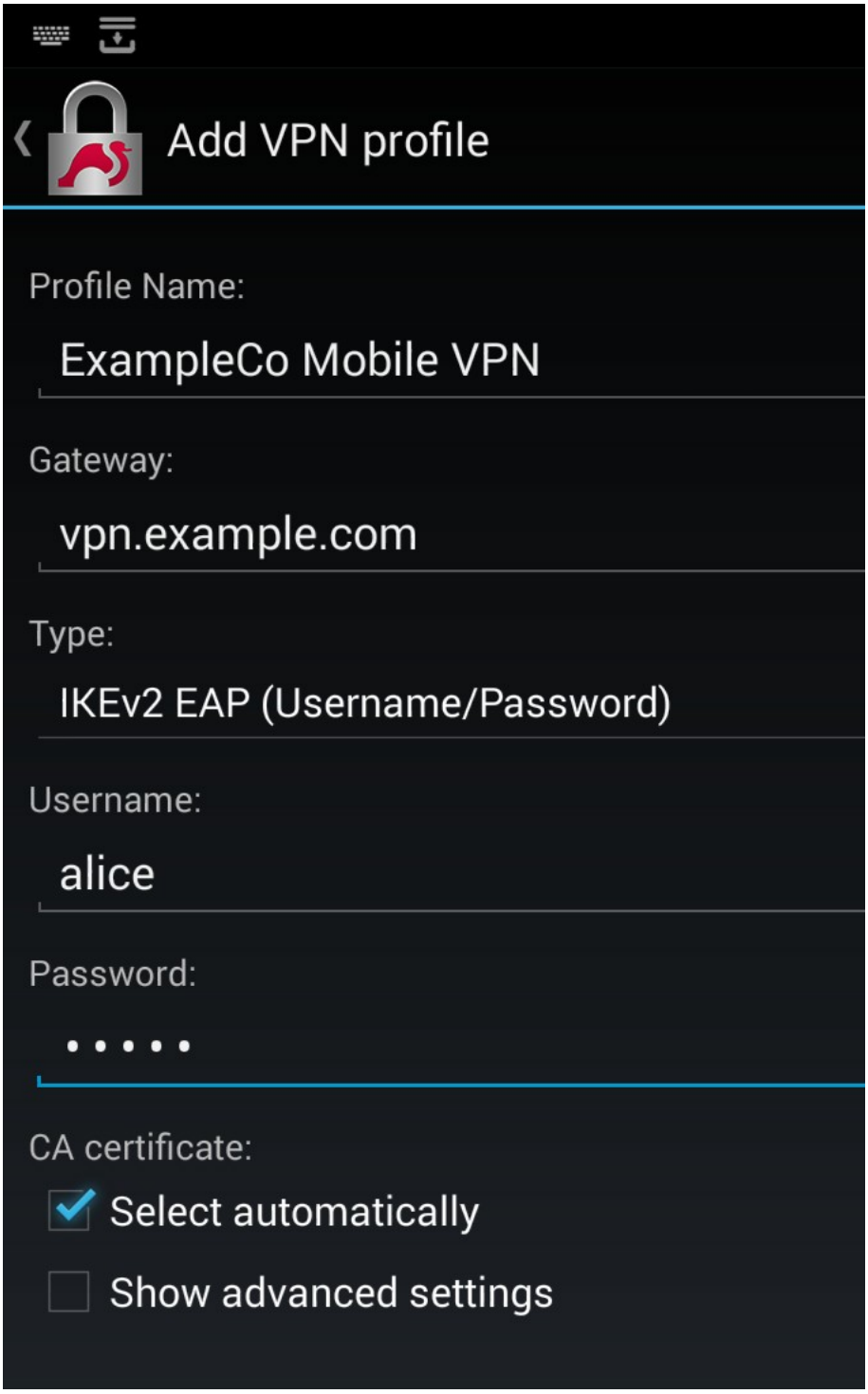


Fig. 35: Impostazioni del client di strongSwan su Android

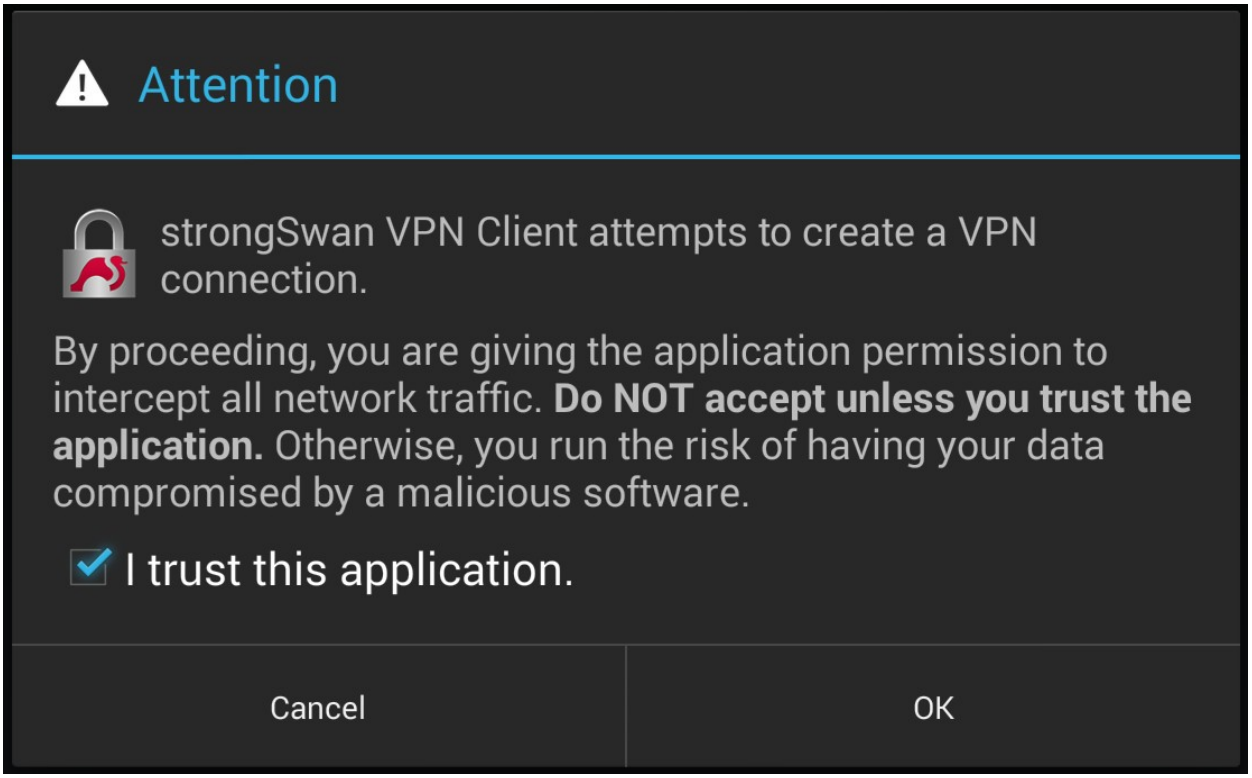


Fig. 36: Impostazioni del client di strongSwan per Android

Configurazione del client con IKEv2 per OS X

A partire da OS X 10.11 (El Capitan) è possibile configurare manualmente una VPN di tipo IKEv2 nella GUI senza bisogno di un file di configurazione del profilo VPN. La configurazione per IKEv2 è integrata nelle impostazioni di gestione della rete come le altre connessioni. Prima che un client possa connettersi, tuttavia, il certificato CA del server VPN deve essere importato.

Importare il certificato CA in OS X

- Copiare il certificato CA sul sistema OS X
- Fare doppio clic sul file del certificato CA in Finder (figura *File del certificato per OS X in Finder*), che apre l'accesso con la chiave
- Individuare il certificato importato sotto **Login**, **Certificati** come mostrato nella figura *Elenco del certificato per l'accesso con la chiave per OS X*
- Trascinare il certificato su **sistema**
- Inserire le credenziali di accesso e fare clic su **Modificare chiavi**
- Individuare il certificato importato in **Sistema**, **Certificati** come mostrato nella figura *Elenco del certificato di sistema per l' accesso con la chiave per OS X*
- Fare clic sul certificato
- Fare clic su **File>Ottienere informazioni**
- Espandere **fiducia**

- Impostare **Quando utilizzare questo certificato** su *Sempre fidato*, come mostrato in figura *Impostazioni della fiducia del certificato su OS X*
- Fare clic sul pulsante rosso di chiusura per chiudere la finestra di informazioni sul certificato, ciò causerà un prompt di autenticazione per consentire la modifica.
- Inserire le credenziali di accesso e fare clic su **Impostazioni di aggiornamento**
- Uscire dall'accesso con le chiavi

Il certificato si trova ora nei certificati di sistema ed è stato contrassegnato come attendibile in modo che possa essere utilizzato per la VPN.

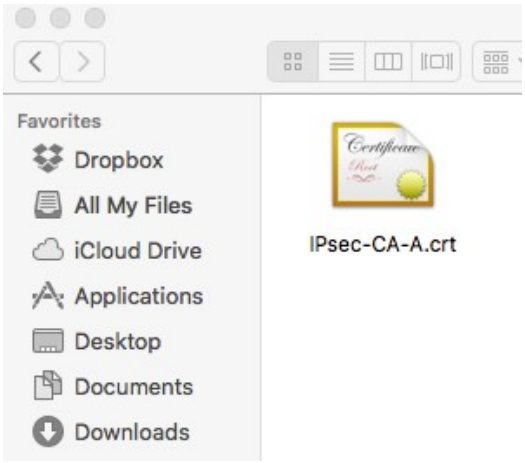


Fig. 37: File del certificato per OS X in Finder

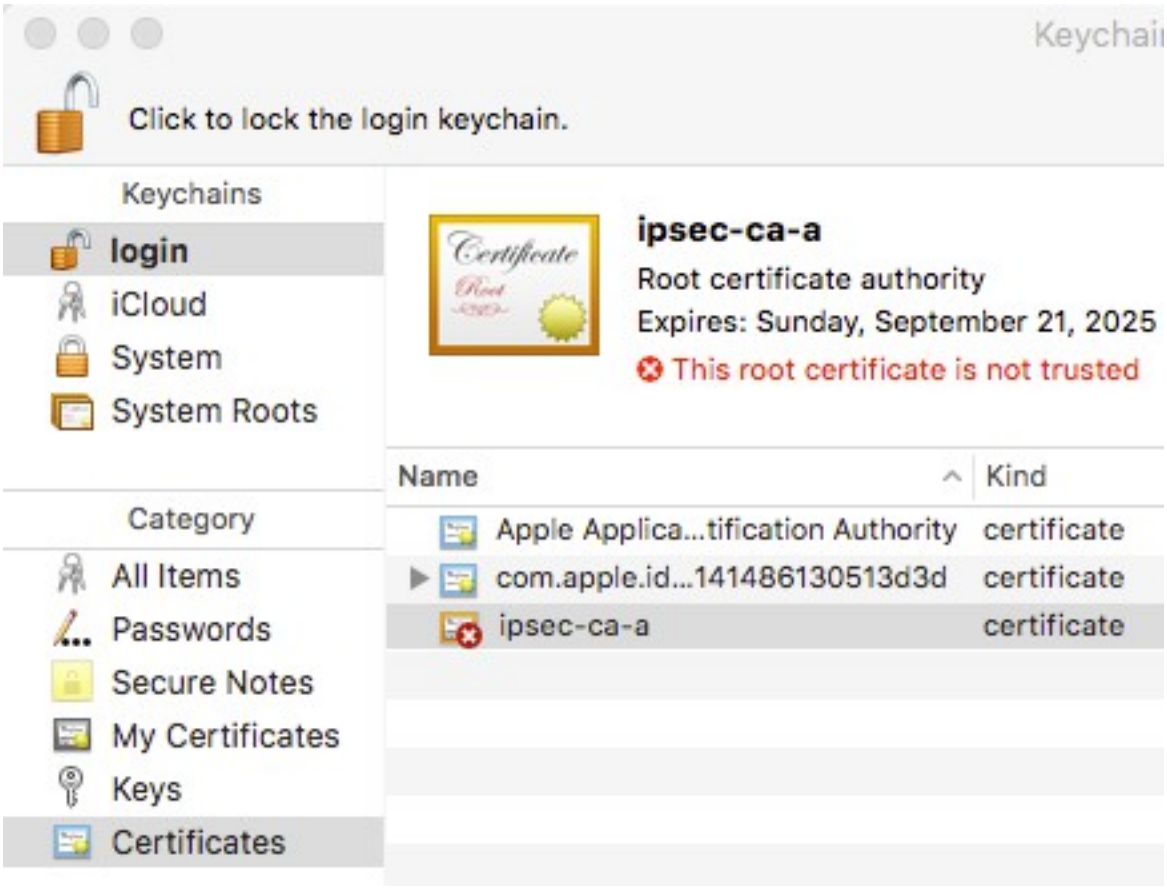


Fig. 38: Elenco del certificato per l'accesso con la chiave per OS X

Impostare la connessione VPN

- Aprire Preferenze di sistema
- Fare clic su **rete**
- Fare clic sull'icona del lucchetto e immettere le credenziali per apportare le modifiche se le impostazioni non sono già state sbloccate
- Fare clic su + per aggiungere una nuova voce VPN, come mostrato nella figura *Pulsante per aggiungere una rete su OS X*
- Selezionare *VPN* per l'interfaccia
- Seleziona IKEv2 per il **tipo di VPN** (predefinito)
- Impostare il **nome del servizio** in una descrizione per la VPN (ad es. VPN Esempi0Co) per completare il modulo, che sarà simile alla figura *Prompt per creare VPN in OS X*
-

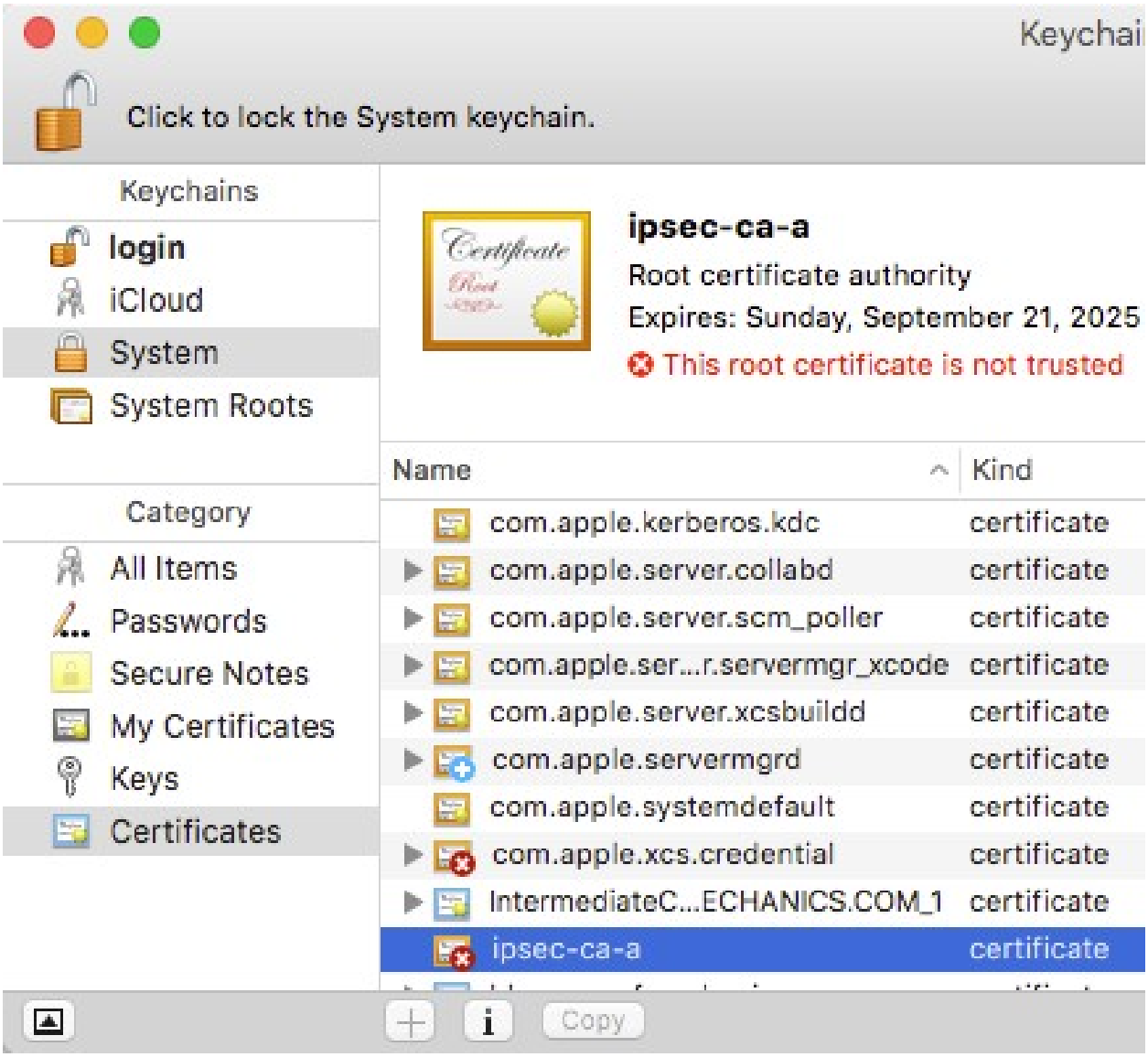


Fig. 39: Elenco del certificato di sistema per l' accesso con la chiave per OS X

Fig. 40: Impostazioni della fiducia del certificato su OS X

Fig. 41: Pulsante per aggiungere una rete su OS X

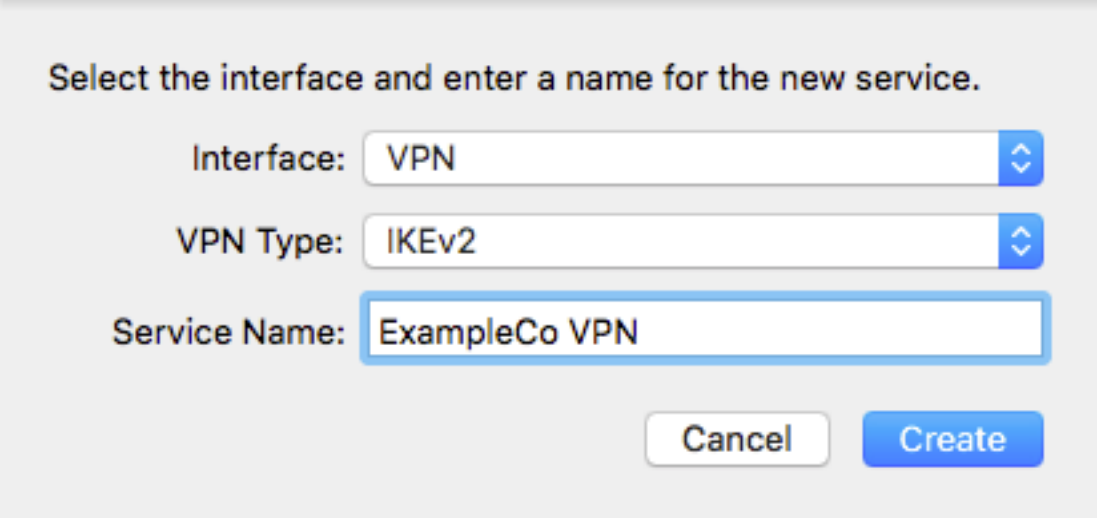


Fig. 42: Prompt per creare VPN in OS X

- Fare clic su **Creare**
- Immettere l'hostname del firewall nel DNS come **indirizzo del server**
- Immettere nuovamente l'hostname del firewall in **ID remoto**

Nota: Questo deve corrispondere al nome comune del certificato del server e alla voce SAN.

- Lasciare **ID locale** vuoto, le impostazioni appariranno come nella figura *Impostazioni della VPN con IKEv2 per OS X*
- Fare clic su **impostazioni dell'autenticazione**
- Selezionare il **nome utente**

Inserire il **nome utente** e la **password**, come mostrato nella figura *Impostazioni di autenticazione della VPN per IKEv2 su OS X*

Nota: Con EAP-MSCHAPv2 il **nome utente** è l'"**Identificatore** configurato per la voce dell'utente nella scheda **Chiavi pre-condivise** in **VPN>IPsec**. Con EAP-RADIUS questo sarebbe il nome utente impostato sul server RADIUS.

- Selezionare **Mostrare lo stato della VPN nella barra del menu** (se desiderato)
- Cliccare su **Applicare**

–

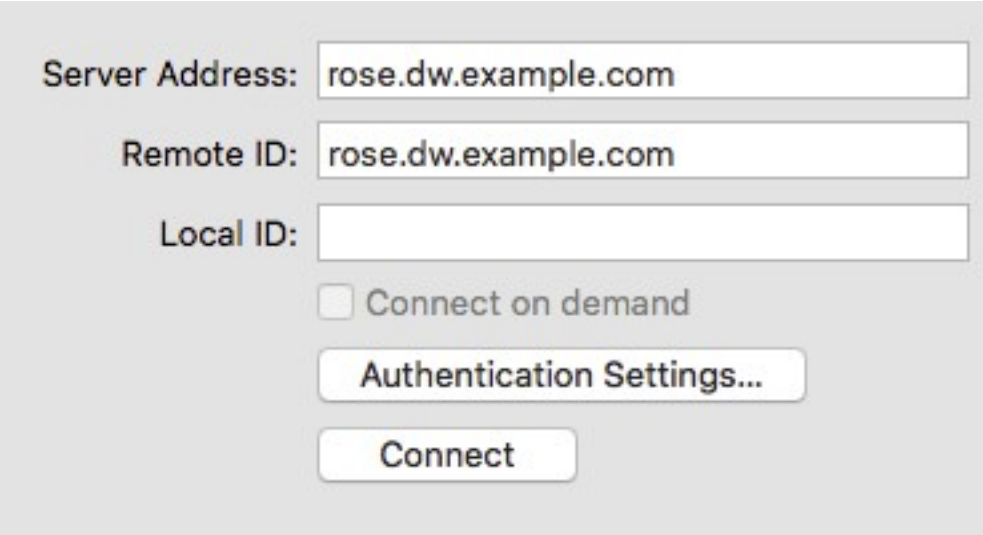


Fig. 43: Impostazioni della VPN con IKEv2 per OS X

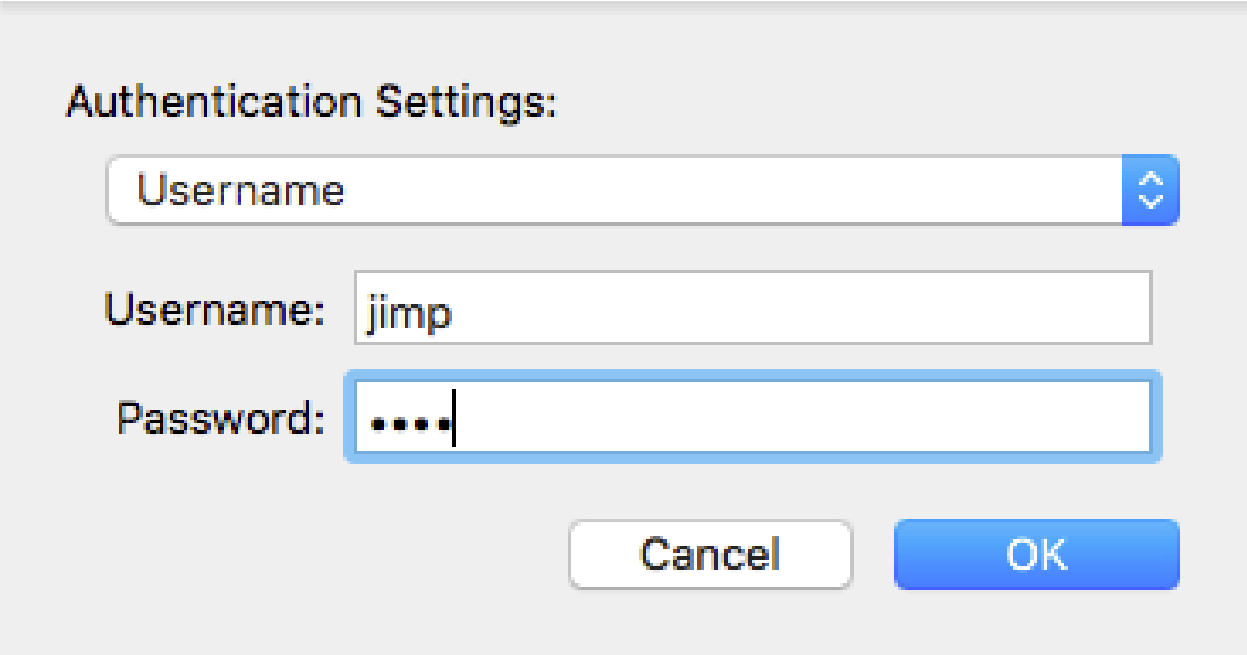


Fig. 44: Impostazioni di autenticazione della VPN per IKEv2 su OS X

Connettersi e disconnettersi

La gestione della connessione può essere effettuata in più modi. Il primo metodo è quello di fare clic su **Connettere** o **Disconnettere** sulla voce VPN nelle impostazioni di rete. Il secondo metodo, più facile, è quello di controllare **Mostrare lo stato della VPN nella barra del menu** nelle impostazioni della VPN e quindi gestire la connessione da tale icona, come mostrato nella figura *Menu dello stato della VPN su OS X.*.

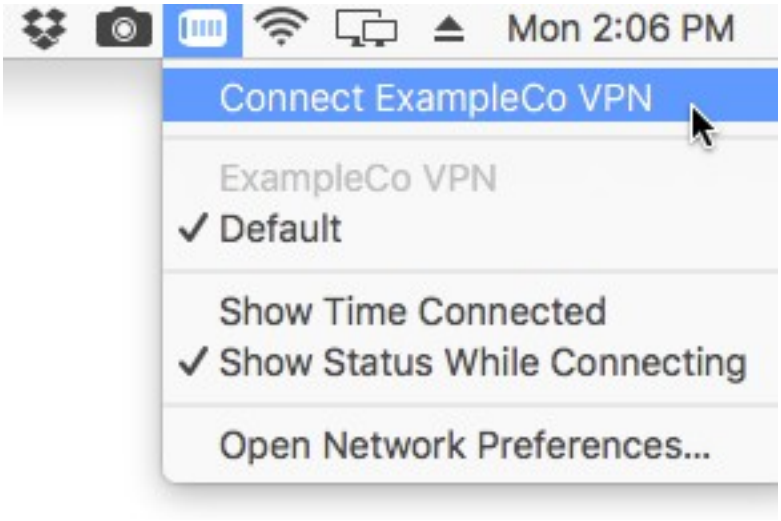


Fig. 45: Menu dello stato della VPN su OS X

Configurazione del client con IKEv2 su iOS

A partire dalla versione 9, iOS ha il supporto integrato per IKEv2 che può essere configurato dalla GUI senza richiedere un profilo VPN. Come per altri client, il certificato CA deve essere installato.

Importare la CA sul dispositivo iOS

L'importazione del certificato CA sul dispositivo del client è un processo relativamente facile. Il primo passo è quello di ottenere il certificato CA sul dispositivo del client. Il modo più semplice per realizzarlo è via e-mail, come mostrato nella figura *Client di posta elettronica per iOS che riceve il certificato CA*

Per installare il certificato da e-mail:

- Inviare solo il certificato CA (non la chiave) a un indirizzo e-mail raggiungibile dal dispositivo client
- Aprire l'app Mail sul dispositivo del client
- Aprire il messaggio contenente il certificato CA
- Toccare l'allegato per installare il certificato CA e il prompt di **Installare il profilo** verrà visualizzato come visto in *Prompt del profilo d'installazione del certificato di CA per iOS*
- Toccare **Installare** in alto a destra e verrà visualizzata una schermata di avviso come mostrato in Avviso di installazione del certificato CA per iOS
- Toccare **Installare** in alto a destra ancora una volta per confermare e poi un prompt finale verrà presentato come visto in *Prompt di conferma del certificato per iOS*
- Toccare **Installare** sul prompt di conferma e il certificato CA è ora memorizzato come una voce attendibile.

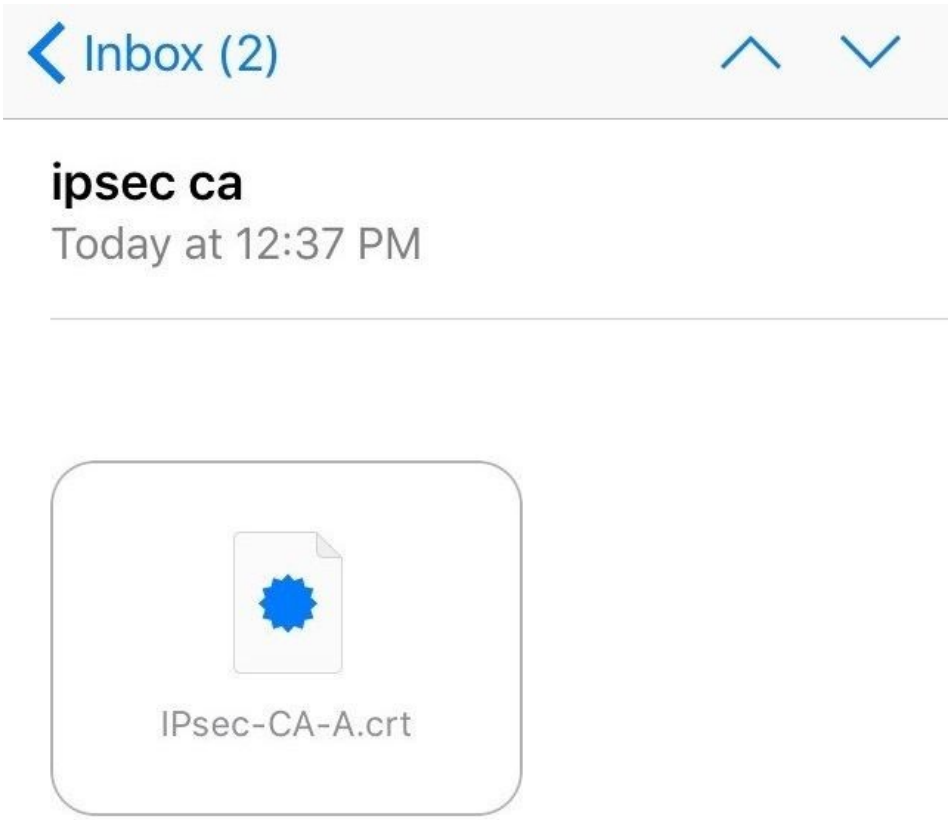


Fig. 46: Client di posta elettronica per iOS che riceve il certificato CA

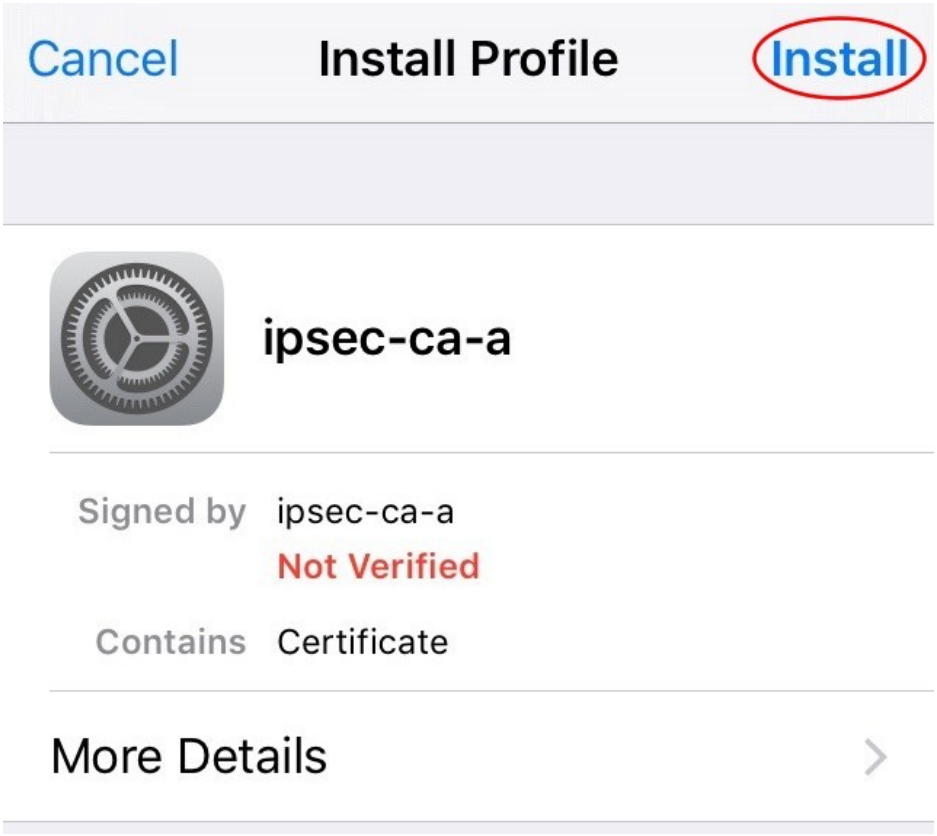


Fig. 47: Prompt del profilo d'installazione del certificato di CA per iOS

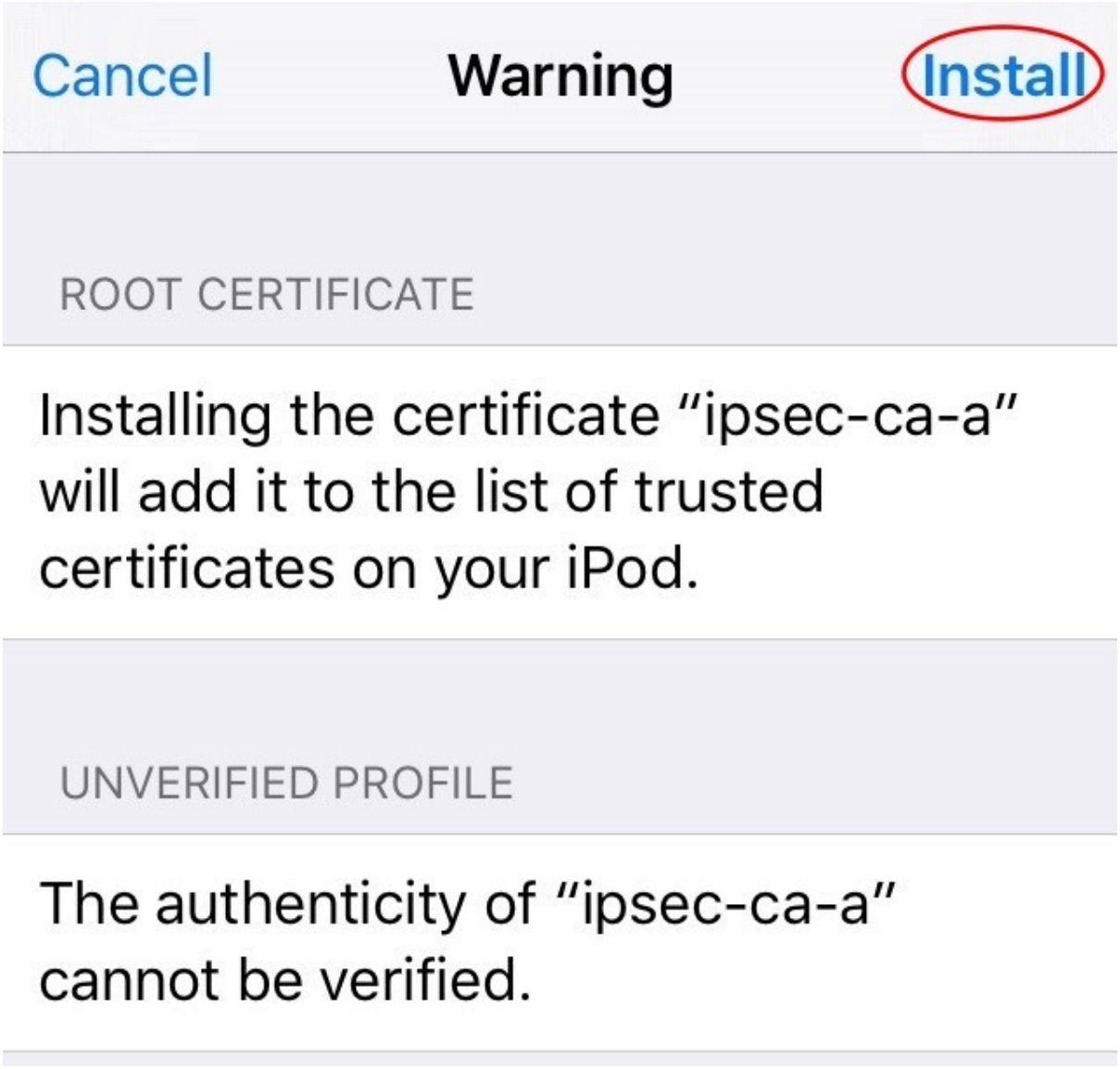


Fig. 48: Avviso di installazione del certificato CA per iOS

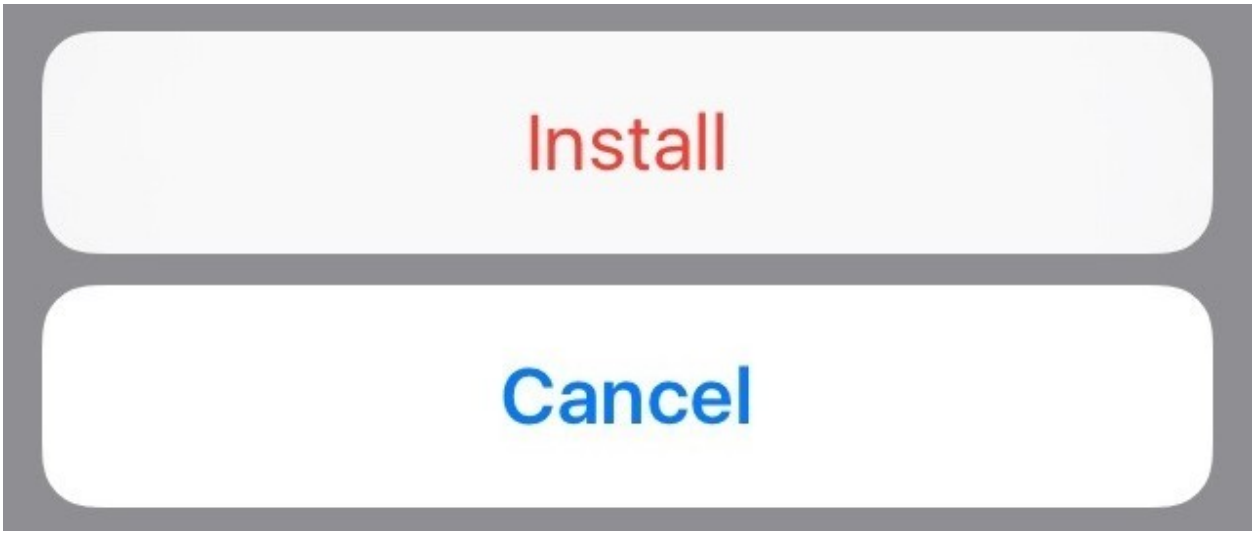


Fig. 49: Prompt di conferma del certificato per iOS

Impostare la connessione VPN

Una volta installato il certificato CA, deve essere configurata una voce VPN:

- Aprire **Impostazioni**
- Toccare **Generale**
- Toccare **VPN**
- Toccare **Aggiungere configurazione VPN**
- Impostare il **tipo** su *IKEv2* (default)
- Inserire un testo per la **descrizione** (ad es. **VPN EsempioCo**)
- Immettere l'hostname del firewall nel DNS come server
- Immettere nuovamente l'hostname del firewall in **ID Remoto**

Nota: Questo deve corrispondere al nome comune e alla voce SAN del certificato del server..

- Lasciare in bianco l'**ID locale**
- Impostare l'**autenticazione utente** su *nome utente*
- Inserire il **nome utente** e la **password**

Nota: Con EAP-MSCHAPv2 il **Nome utente** è l'**Identificatore** configurato per la voce dell'utente nella scheda **Chiavi pre-condivise** in **VPN>IPsec**. Con EAP-RADIUS questo sarebbe il nome utente impostato sul server RADIUS.

- Toccare **Fatto** per completare la voce VPN. Una volta completato, appare simile alla figura *Impostazioni del client per IKEv2 su iOS*

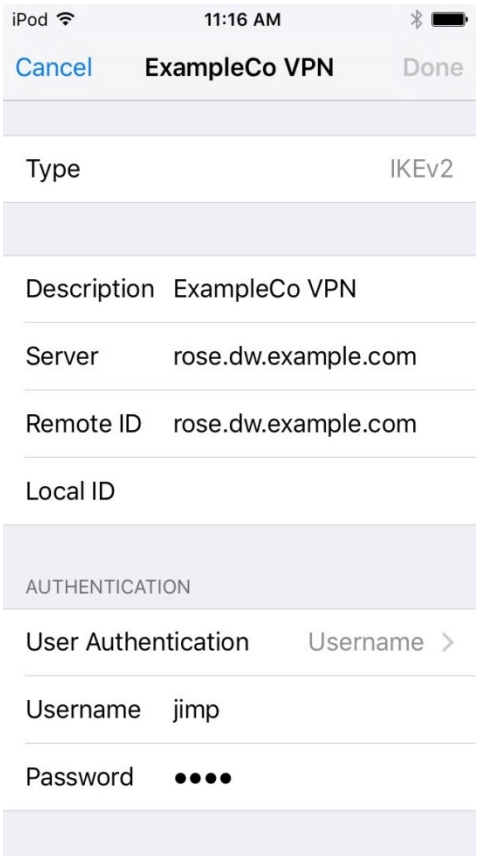


Fig. 50: Impostazioni del client per Ikev2 per iOS

Connettersi e disconnettersi

La VPN può essere collegata o disconnessa visitando le voci VPN in **Impostazioni**. Questo varia un po", ma in genere mostra in almeno due punti:

1. Impostazioni>VPN
2. Impostazioni>Generale>VPN

La voce direttamente sotto **Impostazioni** appare in cima all'elenco con le altre voci di rete (Modalità aereo, Wi-Fi e Bluetooth) una volta che è presente almeno una connessione VPN.

Una volta nell'elenco VPN, la voce VPN deve essere selezionata (mostra un segno di spunta accanto alla sua voce) e quindi il cursore può essere spostato nella posizione "On" per connettersi.

Fig. 51: Elenco delle VPN per iOS

L'IPpsec per dispositivi mobili permette la creazione di una cosiddetta VPN in stile "Road Warrior", che prende il nome dalla natura variabile di chiunque non si trovi nell'ufficio che deve connettersi alla rete principale. Può essere una persona addetta alle vendite che utilizza il Wi-Fi in un viaggio di lavoro, il capo dalla sua limousine tramite modem 3G, o un programmatore che lavora dalla loro linea a banda larga a casa. La maggior parte di questi saranno costretti a trattare con indirizzi IP dinamici, e spesso non conoscono nemmeno l'indirizzo IP che hanno. Senza un router o un firewall che supporta IPsec, un tunnel IPsec tradizionale non funzionerà. Negli scenari di telecomunicazione, di solito è indesiderabile e non necessario collegare l'intera rete domestica dell'utente alla rete dell'ufficio, e così facendo si possono introdurre complicazioni di routing. Questo è dove i client di IPsec per dispositivi mobili sono più utili.

C'è solo una definizione per Ipsec Mobile su Firew4LL, così invece di fare affidamento su un indirizzo fisso per l'estremità remota del tunnel, IPsec Mobile utilizza una qualche forma di autenticazione per consentire un nome utente che deve essere distinto. Questo potrebbe essere un nome utente e password con IKEv2 e EAP o xauth, o un identificatore per utente e una coppia di chiavi pre-condivise, o un certificato.

18.1.6 Testare la connettività di IPsec

Il test più semplice per un tunnel Ipsec è un ping da una stazione client dietro il firewall ad un'altra sul lato opposto. Se funziona, il tunnel funziona correttamente.

Come accennato in *Traffico iniziato da \firew4ll\ e IPsec*, il traffico iniziato dal firewall Firew4LL non attraversa normalmente il tunnel senza un routing extra, ma c'è un modo rapido per testare la connessione dal firewall stesso specificando una sorgente quando si emette un ping.

Ci sono due metodi per eseguire questo test: la GUI e la shell.

Specificare una sorgente del ping nella GUI

Nella GUI, un ping può essere inviato con una sorgente specifica come segue:

- Passare a **diagnostica>Ping**
- Inserire un indirizzo IP sul router remoto all'interno della sottorete remota elencata per il tunnel nel campo **Host** (es. 10.5.0.1)
- Selezionare il **protocollo IP** appropriato, probabilmente *IPv4*
- Selezionare un **indirizzo sorgente** che è un'interfaccia o un indirizzo IP sul firewall locale che si trova all'interno della rete locale della fase 2 (ad es. Selezionare *LAN* per l'indirizzo IP della LAN)
- Impostare un **conteggio** appropriato, come il valore predefinito *3*
- Fare clic su **Ping**

Se il tunnel funziona correttamente, le risposte di ping saranno ricevute dal firewall dall'indirizzo LAN del sito B. Se le risposte non vengono ricevute, passare alla sezione *Risoluzione problemi di IPsec*.

Se il tunnel non è stato creato inizialmente, è comune che alcuni ping vengano persi durante la negoziazione del tunnel, quindi scegliere un conteggio più alto o ripetere il test è una buona pratica se il primo tentativo fallisce.

Specificare una sorgente del ping nella Shell

Usando la shell sulla console o via ssh, il comando ping può essere eseguito manualmente e un indirizzo sorgente può essere specificato con il parametro *-S*. Senza usare - *S* o una route statica, i pacchetti generati da ping non tenteranno di attraversare il tunnel. Questa è la sintassi per un test corretto:

```
#       ping -S <Local LAN IP> <Remote LAN IP>
```

Dove l'*IP della LAN locale* è un indirizzo IP su un'interfaccia interna all'interno della definizione della sottorete locale per il tunnel, e l'*IP della LAN remoto* è un indirizzo IP sul router remoto all'interno della sottorete remota elencata per il tunnel. Nella maggior parte dei casi questo è semplicemente l'indirizzo IP della LAN dei rispettivi firewall di Firew4LL. Dato l'esempio sita-a-sito di sopra, questo è ciò che verrebbe digitato per testare dalla console del firewall del Sita A:

```
#       ping -S 10.3.0.1 10.5.0.1
```

Se il tunnel funziona correttamente, le risposte di ping saranno ricevute dal firewall dall'indirizzo LAN del sito B. Se le risposte non vengono ricevute, passare alla sezione Risoluzione problemi di IPsec.

18.1.7 Risoluzione dei problemi di IPsec

A causa della natura spignola dell'IPsec, non è insolito che sorgano problemi. Per fortuna ci sono alcuni fondamentali (e alcuni non così di base) passaggi di risoluzione dei problemi che possono essere utilizzati per rintracciare potenziali intoppi.

Registrazione di IPsec

> Gli esempi presentati in questo capitolo hanno registri modificati per brevità, ma rimangono messaggi significativi.
>
> La registrazione per IPsec può essere configurata per fornire informazioni più utili. Per configurare la registrazione di IPsec per la diagnosi dei problemi del tunnel di Firew4LL, la seguente procedura fornisce il miglior equilibrio di informazioni:

- Passare a **VPN>IPsec** nella scheda **Impostazioni avanzate**
- Impostare **IKE SA**, **IKE Child SA** e la **backend di configurazione** su *Diag*
- Impostare tutte le altre impostazioni di registro su *controllo*
- Fare clic su Salvare

Nota: La modifica delle opzioni di registrazione non compromette l'attività di IPsec e non c'è bisogno di inserire una specifica "modalità di debug" per IPsec sulle versioni correnti di Firew4LL.

Il tunnel non si stabilisce

Per prima cosa controllare lo stato del servizio in **Stato>Servizi**. Se il servizio di IPsec viene interrotto, ricontrollare che sia abilitato in **VPN>IPsec**. Inoltre, se si utilizzano client mobili, assicurarsi che nella scheda **Client mobili**, la casella di abilitazione è selezionata.

Se il servizio è in esecuzione, controllare i registri del firewall (**Stato>Registro di sistema**, scheda **Firewall**) per vedere se la connessione è bloccata, e se sì, aggiungere una regola per consentire il traffico bloccato. Le regole sono normalmente aggiunte automaticamente per IPsec, ma questa funzione può essere disabilitata.

La causa più comune delle connessioni non riuscite del tunnel IPsec è un disallineamento della configurazione. Spesso si tratta di qualcosa di piccolo, come un gruppo DH impostato a 1 sul lato A e 2 sul lato B, o forse una maschera di rete di /24 da un lato e /32 dall'altro. Ad alcuni router (Linksys, per esempio) piace anche nascondere alcune opzioni dietro i pulsanti "Avanzate" o fare supposizioni. Un sacco di tentativi ed errori possono essere coinvolti, e un sacco di lettura di registro, ma garantire che entrambi i lati corrispondano esattamente aiuterà nella maggior parte dei problemi.

A seconda delle connessioni Internet alle due estremità del tunnel, è anche possibile che un router coinvolto da un lato o dall'altro non gestisca correttamente il traffico IPsec. Questa è una delle preoccupazioni più grandi con i client mobili, e le reti in cui NAT è coinvolto al di fuori degli endpoint di IPsec reali. I problemi si hanno generalmente con il protocollo ESP e che può risultare bloccato o mal gestito lungo la strada. L'NAT Traversal (NAT- T) incapsula l'ESP nel traffico della porta UDP 4500 per risolvere questi problemi.

Il tunnel si stabilisce ma il traffico non passa

Il sospetto principale se un tunnel si stabilisce ma non passa il traffico sono le regole del firewall con IPsec. Se il sito A non può raggiungere il sito B, controllare il registro del firewall del sito B e le regole. Al contrario, se il sito B non può contattare il sito A, controllare il registro del firewall e le regole del sito A. Prima di guardare le regole, ispezionare i registri del firewall in **Stato>Registri di sistema**, nella scheda **Firewall**. Se sono presenti ingressi bloccati che coinvolgono le sottoreti utilizzate nel tunnel IPsec, allora passare al controllo delle regole. Se non ci sono voci di registro che indicano pacchetti bloccati, rivedere la sezione sulle considerazioni del routing IPsec in *Considerazioni su routing e gateway*.

I pacchetti bloccati sull'interfaccia IPsec o *enc0* indicano che il tunnel stesso si è stabilito, ma il traffico è bloccato dalle regole del firewall. I pacchetti bloccati sulla LAN o su un'altra interfaccia interna possono indicare che può essere necessaria un'ulteriore regola in quel gruppo di regole di interfaccia per consentire il traffico dalla sottorete interna all'estremità remota del tunnel IPsec. I pacchetti bloccati sulle interfacce WAN o OPT impedirebbero la creazione di un tunnel. In genere questo accade solo quando le regole VPN automatiche sono disabilitate. L'aggiunta di una regola per consentire il protocollo ESP e la porta UDP 500 da quell'indirizzo IP remoto permetterà al tunnel di stabilirsi. Nel caso di tunnel per dispositivi mobili, consentire al traffico da qualsiasi fonte di connettersi a tali porte.

Le regole per l'interfaccia IPsec possono essere trovate in **Firewall>Regole**, nella scheda **IPsec**. Errori comuni includono l'impostazione di una regola per consentire solo il traffico TCP, il che significa che cose come ping ICMP e DNS non funzionerebbero attraverso il tunnel. Vedere *Firewall* per maggiori informazioni su come creare e risolvere correttamente le regole del firewall.

In alcuni casi è possibile che un disallineamento dell'impostazione possa anche causare il blocco del traffico al passaggio del tunnel. Si consideri il caso in cui una sottorete definita su un firewall non-Firew4LL fosse 192.0.2.1/24, e sul firewall Firew4LL fosse 192.0.2.0/24. Il tunnel si stabilirebbe, ma il traffico non sarebbe passato fino a quando non fosse corretta la sottorete.

I problemi di routing sono un'altra possibilità. Eseguire un traceroute (Tracert su Windows) su un indirizzo IP sul lato opposto del tunnel può aiutare a rintracciare questi tipi di problemi. Ripetere la prova da entrambi i lati del tunnel. Controllare la sezione *Considerazioni su routing e gateway* in questo capitolo per maggiori informazioni. Quando si utilizza traceroute , il traffico che entra e lascia il tunnel IPsec sembrerà mancare alcuni hop provvisori. Questo è normale, e parte di come funziona IPsec. Il traffico che non entra correttamente in un tunnel IPsec sembra lasciare l'interfaccia WAN e la route verso l'esterno attraverso Internet, che indicherebbe ci sia un problema di routing perché Firew4LL non è il gateway (come in *Considerazioni su routing e gateway*), una sottorete remota non correttamente specificata nella definizione del tunnel o al tunnel che è stato disattivato.

Alcuni host funzionano, ma non tutti

Se il traffico tra alcuni host attraverso le VPN funziona correttamente, ma per alcuni host non accade, allora potrebbe essere dovuto a una di queste quattro cose:

Gateway predefinito mancante, errato o ignorato Se il dispositivo non ha un gateway predefinito, o ne ha uno che punta a qualcosa di diverso dal firewall di Firew4LL, non sa come tornare correttamente alla rete remota sulla VPN (vedere *Considerazioni su routing e gateway*). Alcuni dispositivi, anche con un gateway predefinito specificato, non utilizzano quel gateway. Questo è stato visto su vari dispositivi incorporati, tra cui telecamere IP e alcune stampanti. Non c'è nulla che può essere fatto al riguardo, a parte ottenere il software sul dispositivo fisso. Questo può essere verificato eseguendo una cattura di pacchetti sull'interfaccia interna del firewall collegato alla rete che contiene il dispositivo. La risoluzione dei problemi con tcpdump è trattata in *Usare tcpdump dalla riga di comando*, e un esempio specifico di IPsec può essere trovato in *Il tunnel IPsec non si connette*. Se il traffico viene osservato lasciando l'interfaccia interna del firewall, ma nessuna risposta di ritorno, il dispositivo non instrada correttamente il suo traffico di risposta o potrebbe potenzialmente bloccarlo tramite un firewall del client locale.

Maschera di sottorete errata Se la sottorete in uso su un'estremità è 10.0.0.0/24 e l'altra è 10.254.0.0/24, e un host ha una maschera di sottorete errata di **255.0.0.0 o /8**, non sarà mai in grado di comunicare attraverso la VPN perché pensa che la sottorete VPN remota faccia parte della rete locale e quindi il routing non funzionerà correttamente. Il sistema con la configurazione rotta cercherà di contattare il sistema remoto tramite ARP invece di utilizzare il gateway.

Host del firewall Se c'è un firewall sull'host di destinazione, potrebbe non consentire le connessioni. Controllare cose come il firewall di Windows, le tabelle IP, o utilità simili che potrebbero impedire al traffico di essere elaborato dall'host.

Regole del firewall su |firew4ll| Assicurarsi che le regole su entrambe le estremità consentano il traffico di rete desiderato.

La connessione si blocca

IPsec non gestisce con grazia i pacchetti frammentati. Molti di questi problemi sono stati risolti nel corso degli anni, ma ci possono essere alcuni problemi persistenti. Se si bloccano o si perdono pacchetti solo quando si utilizzano protocolli specifici (SMB, RDP, ecc.), può essere necessario il blocco di MSS per la VPN. Il blocco di MSS può essere attivato in **VPN>IPsec** nella scheda **Impostazioni avanzate**. Su quella schermata, selezionare **Abilitare il blocco di MSS sul traffico VPN** e quindi inserire un valore. Un buon punto di partenza sarebbe 1400, e se funziona lentamente aumentare il valore MSS fino a quando il punto di rottura è colpito, quindi indietreggiare un po" da lì.

Disconnessione "casuale" del tunnel/Guasti DPD sul router incorporato

Se i tunnel Ipsec vengono fatto cadere su un ALIX o altro hardware incorporato che sta spingendo i limiti della sua CPU, DPD sul tunnel potrebbe aver bisogno di essere disabilitato. Tali guasti tendono a correlarsi con i tempi di utilizzo della larghezza di banda elevata. Ciò accade quando la CPU su un sistema a bassa potenza è legata all'invio di traffico IPsec o è altrimenti occupata. A causa del sovraccarico della CPU, potrebbe non richiedere tempo per rispondere alle richieste DPD o visualizzare una risposta a una richiesta propria. Di conseguenza, il tunnel fallirà un controllo DPD e verrà disconnesso. Questo è un chiaro segno che l'hardware venga guidato oltre la sua capacità. Se ciò accade, considerare di sostituire il firewall con un modello più potente.

I tunnel si creano e funzionano ma non riescono a rinegoziare

In alcuni casi un tunnel funzionerà correttamente, ma una volta che la durata della fase 1 o della fase 2 scade il tunnel non riuscirà a rinegoziare correttamente. Questo può manifestarsi in diversi modi, ognuno con una risoluzione diversa.

DPD non supportato, un lato cade ma l'altro rimane

Si consideri questo scenario, che DPD è progettato per prevenire, ma può accadere in luoghi in cui DPD non è supportato:

- Un tunnel è stabilito dal sito A al sito B, dal traffico avviato al sito A.
- Per il sito B scade la fase 1 o la fase 2 prima del sito A
- Il sito A crederà che il tunnel sia attivo e continuerà a inviare traffico come se il tunnel stesse funzionando correttamente.
- Solo quando scade la fase 1 o la fase 2 del sito A, verrà rinegoziato come previsto.

In questo scenario, le due probabili risoluzioni sono: abilitare DPD, o il sito B deve inviare traffico al sito A che farà sì che l'intero tunnel rinegozi. Il modo più semplice per farlo accadere è quello di consentire un meccanismo di mantenere vivo su entrambi i lati del tunnel

Il tunnel si stabilisce all'inizio, ma non alla risposta

Se un tunnel si stabilirà a volte, ma non sempre, generalmente c'è una mancata corrispondenza da un lato. Il tunnel può ancora stabilirsi perché se le impostazioni presentate da un lato sono più sicure, l'altro può accettarle, ma non viceversa. Ad esempio, se c'è una mancata corrispondenza della modalità aggressiva/principale su un tunnel IKEv1 e il lato imposta la modalità *Principale* per avviare, il tunnel continuerà a stabilirsi. Tuttavia, se il lato impostato su *aggressivo* tenterà di avviare il tunnel fallirà.

I disallineamenti della durata di vita non causano un guasto nella fase 1 o nella fase 2.

Per rintracciare questi errori, configurare i registri come mostrato nella *registrazione di IPsec* e tentare di avviare il tunnel da ciascun lato, quindi controllare i registri.

Interpretazione del registro di IPsec

I registri IPsec disponibili in **Stato>Registri di sistema**, nella scheda **IPsec** contengono un record del processo di connessione del tunnel e alcuni messaggi provenienti dall'attività di manutenzione del tunnel in corso. Alcune voci di registro tipiche sono elencate in questa sezione, sia buone che cattive. Le cose principali da cercare sono le frasi chiave che indicano quale parte di una connessione ha funzionato. Se » IKE_SA… è stabilito » è presente nel registro, ciò significa che la fase 1 è stata completata con successo e un'associazione di sicurezza è stata negoziata. Se » CHILD_SA … è stabilito » è presente, allora la fase 2 è stata completata e il tunnel è scaduto.

Nei seguenti esempi, i log sono stati configurati come in ascolto in *Registrazione di IPsec* e messaggi irrilevanti possono essere omessi. Tenere presente che questi sono esempi e i numeri ID specifici, gli indirizzi IP e così via varieranno..

Connessioni riuscite

Quando un tunnel è stato stabilito con successo entrambe le parti indicheranno che un IKE SA e un SA secondario sono stati stabiliti. Quando con IKEv1 sono presenti più definizioni di fase 2, viene negoziata un SA secondario per ogni voce di fase 2.

L'output di registro dall'iniziatore:

charon: 09[IKE] IKE_SA con2000[11] established between 192.0.2.90[192.0.2.90]...192.0.2.74[192.0.2.74] charon: 09[IKE] CHILD_SA con2000{2} established with SPIs cf4973bf_i c1cbfdf2_o and TS 192.168.48.0/24|/0 === 10.42.42.0/24|/0

Output del registro dal rispondente:

charon: 03[IKE] IKE_SA con1000[19] established between 192.0.2.74[192.0.2.74]...192.0.2.90[192.0.2.90] charon: 16[IKE] CHILD_SA con1000{1} established with SPIs c1cbfdf2_i cf4973bf_o and TS 10.42.42.0/24|/0 === 192.168.48.0/24|/0

Esempi di connessione non riuscita

Questi esempi mostrano connessioni non riuscite per vari motivi. Nella maggior parte dei casi è chiaro dagli esempi che l'iniziatore non riceve messaggi su elementi specifici che non corrispondono, quindi i registri del rispondente sono molto più informativi. Questo viene fatto per proteggere la sicurezza del tunnel, sarebbe insicuro fornire messaggi a un potenziale attaccante che darebbe loro informazioni su come il tunnel è configurato.

Principale della fase 1/Disadattamento aggressivo

In questo esempio, l'iniziatore è impostato per la modalità aggressiva mentre il rispondente è impostato per la modalità principale. L'output di registro dall'iniziatore:

charon: 15[IKE] initiating Aggressive Mode IKE_SA con2000[1] to 203.0.113.5 charon: 15[IKE] received AUTHENTICATION_FAILED error notify charon: 13[ENC] parsed INFORMATIONAL_V1 request 1215317906 [N(AUTH_FAILED)] charon: 13[IKE] received AUTHENTICATION_FAILED error notify

Output del registro dal rispondente:

charon: 13[IKE] Aggressive Mode PSK disabled for security reasons charon: 13[ENC] generating INFORMATIONAL_V1 request 2940146627 [N(AUTH_FAILED)]

Da notare che i registri del rispondente dichiarano chiaramente che la modalità Aggressiva è disabilitata, il che è un buon indizio che la modalità non sia corretta.

Nel caso inverso, se il lato impostato per la modalità principale inizia, il tunnel verso un firewall di Firew4LL si stabilirà poiché la modalità principale è più sicura.

Disallineamento dell'identificatore di fase 1

Quando l'identificatore non corrisponde, l'iniziatore mostra solo che l'autenticazione non è riuscita, ma non fornisce un motivo. Il rispondente afferma di non essere in grado di individuare un peer, il che indica che non è stato in grado di trovare una fase 1 corrispondente, il che implica che non potrebbe essere individuato alcun identificatore corrispondente.

Output log dall'iniziatore:

charon: 10[ENC] parsed INFORMATIONAL_V1 request 4216246776 [HASH N(AUTH_FAILED)] charon: 10[IKE] received AUTHENTICATION_FAILED error notify

Output del registro dal rispondente:

charon: 12[CFG] looking for pre-shared key peer configs matching 203.0.113.5...198.51.100.3[someid] charon: 12[IKE] no peer config found charon: 12[ENC] generating INFORMATIONAL_V1 request 4216246776 [HASH N(AUTH_FAILED)]

Mancata corrispondenza della chiave pre-condivisa di fase 1

Una chiave pre-condivisa non corrispondente può essere un duro problema da diagnosticare. Un errore che indica il fatto che questo valore non è corretto non è stampato nel registro, invece viene mostrato questo messaggio:

Output del registro dall'iniziatore:

charon: 09[ENC] invalid HASH_V1 payload length, decryption failed? charon: 09[ENC] could not decrypt payloads charon: 09[IKE] message parsing failed

Output del registro dal rispondente:

charon: 09[ENC] invalid ID_V1 payload length, decryption failed? charon: 09[ENC] could not decrypt payloads charon: 09[IKE] message parsing failed

Quando i messaggi di registro di cui sopra sono presenti, controllare il valore della chiave pre-condivisa su entrambi i lati per assicurarsi che corrispondano.

Errore nell'algoritmo di crittografia di fase 1

Output del registro dall'iniziatore:

charon: 14[ENC] parsed INFORMATIONAL_V1 request 3851683074 [N(NO_PROP)] charon: 14[IKE] received NO_PROPOSAL_CHOSEN error notify

Output del registro dal rispondente:

charon: 14[CFG] received proposals: IKE:AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024 charon: 14[CFG] configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024 charon: 14[IKE] no proposal found charon: 14[ENC] generating INFORMATIONAL_V1 request 3851683074 [N(NO_PROP)]

In questo caso, la voce di registro mostra esattamente il problema: l'iniziatore è stato impostato per la crittografia AES 128, e il rispondente è impostato per AES 256. Impostare entrambi su valori corrispondenti e poi riprovare.

Errore nell'algoritmo di hash di fase 1

Output del registro dall'iniziatore:

charon: 10[ENC] parsed INFORMATIONAL_V1 request 2774552374 [N(NO_PROP)] charon: 10[IKE] received NO_PROPOSAL_CHOSEN error notify

Output del registro dal rispondente:

charon: 14[CFG] received proposals: IKE:AES_CBC_256/MODP_1024 charon: 14[CFG] configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024 charon: 14[IKE] no proposal found charon: 14[ENC] generating INFORMATIONAL_V1 request 2774552374 [N(NO_PROP)]

L'algoritmo Hash è indicato dalla parte HMAC delle proposte registrate. Come si può vedere sopra, le proposte ricevute e configurate non hanno voci HMAC corrispondenti.

Disallineamento del gruppo DH di fase 1

Output del registro dall'iniziatore:

charon: 11[ENC] parsed INFORMATIONAL_V1 request 316473468 [N(NO_PROP)] charon: 11[IKE] received NO_PROPOSAL_CHOSEN error notify

Output del registro dal rispondente:

charon: 14[CFG] received proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_8192 charon: 14[CFG] configured proposals: IKE:AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024 charon: 14[IKE] no proposal found charon: 14[ENC] generating INFORMATIONAL_V1 request 316473468 [N(NO_PROP)]

Il gruppo DH è indicato dalla parte «MODP» della proposta elencata. Come indicato dai messaggi di registro, l'iniziatore è stato impostato per 8192 (Gruppo 18) e il rispondente è stato impostato per 1024 (Gruppo 2). Questo errore può essere corretto settando l'impostazione del gruppo DH di entrambe le estremità del tunnel su un valore corrispondente.

Disallineamento della rete nella fase 2

Nell'esempio seguente, la voce di fase 2 sul lato iniziatore è impostata per 10.3.0.0/24 fino a 10.5.0.0/24. Il rispondente non è impostato per corrispondere in quanto elenca invece 10.5.1.0/24.

Output del registro dall'iniziatore:

charon: 08[CFG] proposing traffic selectors for us: charon: 08[CFG] 10.3.0.0/24|/0 charon: 08[CFG] proposing traffic selectors for other: charon: 08[CFG] 10.5.0.0/24|/0 charon: 08[ENC] generating QUICK_MODE request 316948142 [HASH SA No ID ID] charon: 08[NET] sending packet: from 198.51.100.3[500] to 203.0.113.5[500] (236 bytes) charon: 08[NET] received packet: from 203.0.113.5[500] to 198.51.100.3[500] (76 bytes) charon: 08[ENC] parsed INFORMATIONAL_V1 request 460353720 [HASH N(INVAL_ID)] charon: 08[IKE] received INVALID_ID_INFORMATION error notify

Output del registro dal rispondente:

charon: 08[ENC] parsed QUICK_MODE request 2732380262 [HASH SA No ID ID] charon: 08[CFG] looking for a child config for 10.5.0.0/24|/0 === 10.3.0.0/24|/0 charon: 08[CFG] proposing traffic selectors for us: charon: 08[CFG] 10.5.1.0/24|/0 charon: 08[CFG] proposing traffic selectors for other: charon: 08[CFG] 10.3.0.0/24|/0 charon: 08[IKE] no matching CHILD_SA config found charon: 08[IKE] queueing INFORMATIONAL task charon: 08[IKE] activating new tasks charon: 08[IKE] activating INFORMATIONAL task charon: 08[ENC] generating INFORMATIONAL_V1 request 1136605099 [HASH N(INVAL_ID)]

Nei registri del rispondente si elencano sia le reti ricevute (la riga » configurazione secondaria“ nel registro) e ciò che è stato configurato localmente (la riga «proporre Selettori di traffico per...» nel registro). Confrontando i due, una mancata corrispondenza può essere individuata. La riga "nessuna corrispondenza con la configurazione CHILD_SA trovata» nel registro sarà sempre presente quando si verifica questa mancata corrispondenza e ciò indica espressamente che non è stato possibile trovare una definizione di fase 2 che corrisponda a ciò che è stato ricevuto dall'iniziatore.

Disallineamento dell'algoritmo di crittografia di fase 2

Output del registro dall'iniziatore:

charon: 14[CFG] configured proposals: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ charon: 14[ENC] generating QUICK_MODE request 759760112 [HASH SA No ID ID] charon: 14[NET] sending packet: from

198.51.100.3[500] to 203.0.113.5[500] (188 bytes) charon: 14[NET] received packet: from 203.0.113.5[500] to 198.51.100.3[500] (76 bytes) charon: 14[ENC] parsed INFORMATIONAL_V1 request 1275272345 [HASH N(NO_PROP)] charon: 14[IKE] received NO_PROPOSAL_CHOSEN error notify

Output del registro dal rispondente:

charon: 13[CFG] selecting proposal: charon: 13[CFG] no acceptable ENCRYPTION_ALGORITHM found charon: 13[CFG] received proposals: ESP:AES_CBC_128/HMAC_SHA1_96/NO_EXT_SEQ charon: 13[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ charon: 13[IKE] no matching proposal found, sending NO_PROPOSAL_CHOSEN charon: 13[IKE] queueing INFORMATIONAL task charon: 13[IKE] activating new tasks charon: 13[IKE] activating INFORMATIONAL task charon: 13[ENC] generating INFORMATIONAL_V1 request 1275272345 [HASH N(NO_PROP)]

In questo caso, l'iniziatore riceve un messaggio che indica che il rispondente non è riuscito a trovare una proposta adeguata («ricevuto NESSUNA_PROPOSTA_SCELTA_), e dai registri del rispondente è ovvio che ciò è dovuto ai siti impostati per diversi tipi di crittografia, AES 128 da un lato e AES 256 dall'altro.

Errore nell'algoritmo di hash di fase 2

Output del registro dall'iniziatore:

charon: 10[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA2_512_256/NO_EXT_SEQ charon: 10[ENC] generating QUICK_MODE request 2648029707 [HASH SA No ID ID] charon: 10[NET] sending packet: from 198.51.100.3[500] to 203.0.113.5[500] (188 bytes) charon: 10[NET] received packet: from 203.0.113.5[500] to 198.51.100.3[500] (76 bytes) charon: 10[ENC] parsed INFORMATIONAL_V1 request 757918402 [HASH N(NO_PROP)] charon: 10[IKE] received NO_PROPOSAL_CHOSEN error notify

Output del registro dal rispondente:

charon: 11[CFG] selecting proposal: charon: 11[CFG] no acceptable INTEGRITY_ALGORITHM found charon: 11[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA2_512_256/NO_EXT_SEQ charon: 11[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ charon: 11[IKE] no matching proposal found, sending NO_PROPOSAL_CHOSEN charon: 11[IKE] queueing INFORMATIONAL task charon: 11[IKE] activating new tasks charon: 11[IKE] activating INFORMATIONAL task charon: 11[ENC] generating INFORMATIONAL_V1 request 757918402 [HASH N(NO_PROP)]

Analogamente a un disallineamento dell'algoritmo di hash di fase 1, i valori HMAC nelle voci di registro non si allineano. Tuttavia il rispondente registra anche un messaggio più chiaro "Nessun accettabile ALGORITMO_INTEGRITA trovato" quando questo accade nella fase 2.

Disallineamento di PFS di fase 2 PFS

Output del registro dall'iniziatore:

charon: 06[ENC] generating QUICK_MODE request 909980434 [HASH SA No KE ID ID] charon: 06[NET] sending packet: from 198.51.100.3[500] to 203.0.113.5[500] (444 bytes) charon: 06[NET] received packet: from 203.0.113.5[500] to 198.51.100.3[500] (76 bytes) charon: 06[ENC] parsed INFORMATIONAL_V1 request 3861985833 [HASH N(NO_PROP)] charon: 06[IKE] received NO_PROPOSAL_CHOSEN error notify

Output del registro dal rispondente:

charon: 08[CFG] selecting proposal: charon: 08[CFG] no acceptable DIFFIE_HELLMAN_GROUP found charon: 08[CFG] received proposals: ESP:AES_CBC_256/HMAC_SHA1_96/MODP_2048/NO_EXT_SEQ charon: 08[CFG] configured proposals: ESP:AES_CBC_256/HMAC_SHA1_96/NO_EXT_SEQ charon: 08[IKE] no matching proposal found, sending NO_PROPOSAL_CHOSEN charon: 08[ENC] generating INFORMATIONAL_V1 request 3861985833 [HASH N(NO_PROP)]

La perfetta segretezza di forward (PFS) funziona come i gruppi DH nella fase 1, ma è opzionale. Quando le opzioni PFS scelte non corrispondono, viene registrato un messaggio chiaro che indica questo fatto: «nessun accettabile DIFFIE_HELLMAN_GROUP trovato".

Nota: In In alcuni casi, se un lato ha PFS impostato su off , e

l'altro lato ha un valore impostato, il tunnel può ancora stabilirsi e lavorare. La mancata corrispondenza mostrata sopra può essere vista solo se i valori non corrispondono, per esempio *1* e *5*.

Identificatore non corretto con NAT

In questo caso, Firew4LL è configurato per un **identificatore Peer** di *indirizzo IP del Peer*, ma il dispositivo remoto è in realtà dietro il NAT. In questo caso strongSwan si aspetta che l'indirizzo IP prima del NAT privato effettivo sia l'identificatore. Il demone racoon utilizzato nelle versioni precedenti era molto più rilassato e corrispondeva a entrambi gli indirizzi, ma strongSwan è più formale e richiede una corrispondenza corretta.

Output del registro dal rispondente:

charon: 10[IKE] remote host is behind NAT charon: 10[IKE] IDir "192.0.2.10" does not match to "203.0.113.245" [...] charon: 10[CFG] looking for pre-shared key peer configs matching 198.51.100.50...203.0.113.245[192.0.2.10]

Per correggere questa condizione, modificare l'impostazione dell'**identificatore Peer** all'*indirizzo IP* e quindi inserire l'indirizzo IP prima del NAT, che in questo esempio è 192.0.2.10.

Traffico che scompare

Se il traffico IPsec arriva ma non viene mai visualizzato sull'interfaccia IPsec (*enc0*), verificare la presenza di percorsi/indirizzi IP d'interfaccia in conflitto. Ad esempio, se un tunnel IPsec è configurato con una rete remota di 192.0.2.0/24 e c'è un server OpenVPN locale con una rete tunnel di 192.0.2.0/24, allora il traffico ESP potrebbe arrivare, strongSwan può elaborare i pacchetti, ma non vengono mai visualizzati su *enc0* perché stanno arrivando al sistema operativo per la consegna.

Risolvere l'interfaccia/percorso duplicato e il traffico inizierà a fluire.

Problemi della pagina sullo stato di IPsec

Se la pagina di stato di IPsec stampa errori come:

```
Warning:  Illegal string offset 'type' in /etc/inc/xmlreader.inc on line 116
```

Questo è un segno che il decodificatore di XML XmlReader incompleto è attivo, il quale viene attivato dalla presenza del file */cf/conf/use_xmlreader*. Questo decodificatore alternativo può essere più veloce nel leggere file *config.xml* di grandi dimensioni, ma manca di alcune caratteristiche necessarie in altre aree per funzionare bene. Rimuovere */cf/conf/use_xmlreader* restituirà immediatamente il sistema al decodificatore predefinito, che correggerà la visualizzazione della pagina di stato di IPsec.

18.1.8 Configurare l dispositive Ipsec di terze parti

Qualsiasi dispositivo VPN che supporti IPSec standard può essere collegato a un dispositivo che esegue Firew4LL. Firew4LL viene utilizzato in produzione in combinazione con attrezzature di numerosi fornitori, e molto probabilmente funziona bene con tutti i dispositivi capaci di supportare IPsec incontrati in altre reti. Il collegamento di dispositivi di due diversi fornitori può essere problematico indipendentemente dai fornitori coinvolti a causa delle differenze di

configurazione tra i fornitori, in alcuni casi per i bug nelle implementazioni e per il fatto che alcuni di essi utilizzano estensioni proprietarie. Alcuni esempi sono forniti alla fine di questo capitolo per diversi dispositivi Cisco comuni.

Per configurare un tunnel IPsec tra Firew4LL e un dispositivo di un altro fornitore, la preoccupazione principale è garantire che i parametri di fase 1 e 2 corrispondano su entrambi i lati. Per le opzioni di configurazione su Firew4LL, dove si consente di selezionare più opzioni, selezionare solo una di queste opzioni e assicurarsi che l'altro lato sia impostato allo stesso modo. Gli endpoint tenteranno di negoziare un'opzione compatibile quando vengono selezionate più opzioni, tuttavia ciò è spesso fonte di problemi durante la connessione a dispositivi di terze parti. Configurare entrambe le estremità a quelle che si ritiene siano le impostazioni corrispondenti, quindi salvare e applicare le modifiche su entrambi i lati.

Una volta che le impostazioni corrispondono su entrambe le estremità del tunnel, tentare di far passare il traffico sopra la VPN per attivare la sua iniziazione, quindi controllare i registri IPsec su entrambe le estremità per rivedere la negoziazione. A seconda della situazione, i registri di un'estremità possono essere più utili di quelli dell'estremità opposta, quindi è bene controllare entrambi e confrontare. Il lato Firew4LL in genere fornisce informazioni migliori in alcuni scenari, mentre in altre occasioni l'altro dispositivo fornisce un registro più utile. Se la negoziazione fallisce, determinare se è stata la fase 1 o 2 che ha fallito e rivedere accuratamente le impostazioni di conseguenza, come descritto nella *risoluzione dei problemi di IPsec*. Il lato che inizia spesso non riesce a capire perché, quindi controllare prima i registri sul lato che risponde.

Differenze terminologiche

Un'altra fonte frequente di guasti sono le differenze nella terminologia tra i fornitori. Qui ci sono alcune cose comuni da tenere presente:

VPN/IPsec basato sulla politica Il tipo di IPsec utilizzato da Firew4LL. I criteri sono definiti, ad esempio le voci di fase 2, che controllano il traffico che entra nel tunnel.

VPN/IPsec basato sulla route Questo stile di IPsec non è supportato da Firew4LL, ma alcuni fornitori o apparecchiature possono richiederlo. Esiste un'interfaccia IPsec che instrada in modo simile ad altre interfacce e obbedisce alla tabella di routing, piuttosto che basarsi sulla politica.

S2S o L2L Abbreviazione di Sita-a-Sito o LAN-a-LAN, distinto da una VPN in stile client mobile.

Segretezza privata forward (PFS) Alcuni fornitori hanno diversi controlli per PFS. Può essere solo un interruttore che utilizza lo stesso valore del **gruppo DH** di fase 1, altri lo etichettano con il testo completo o l'acronimo, altri lo etichettano **gruppo DH**.

Trasformare il set Sui dispositivi Cisco, un insieme di parametri che definiscono la gestione di fase 2, come la crittografia e gli algoritmi di hash.

Politica ISAKMP Sui dispositivi Cisco, un insieme di parametri che definiscono la gestione della fase 1 come autenticazione, crittografia e algoritmi hash e altri.

Proposte Su Juniper e Fortigate, set di opzioni che definiscono i parametri per la gestione della fase 1 (IKE) o della Fase 2 (IPsec).

Esenzione NAT o nessun nat Su Juniper e Cisco, eccezioni al NAT che devono essere fatte per garantire che il traffico che attraversa una VPN non abbia il NAT applicato.

Byte di vita o durata di vita del traffico Limiti sulla quantità di traffico inviato su una VPN prima che sia rinegoziato. Attualmente non supportato nella GUI di Firew4LL, se presente su un dispositivo remoto potrebbe essere necessario disabilitarlo.

Dominio o politica di crittografia Una definizione di rete utilizzata nella fase 2 per controllare quale traffico verrà gestito da IPsec.

Esempi di firewall di terze parti

I seguenti esempi sono per i dispositivi Cisco di terze parti che eseguono un tunnel ipotetico per un esempio leggermente diverso da quello in questo capitolo. I dettagli dell'indirizzo sono gli stessi di *Sito-a-Sito*, ma ci sono alcune differenze in questi esempi:

Crittografia di fase 1 e fase 2 3DES Hash di fase 1 e fase 2 SHA1 Durata della fase 1 86400

Cisco PIX OS 6.x

La seguente configurazione è per un Cisco PIX in esecuzione su 6.x come sito B dall'esempio di configurazione sito-a-sito precedente nel capitolo.

sysopt connection permit-ipsec isakmp enable outside

!— Phase 1 isakmp identity address isakmp policy 1 encryption 3des isakmp policy 1 hash sha isakmp policy 1 group 2 isakmp policy 1 lifetime 86400 isakmp policy 1 authentication pre-share isakmp key aBc123%XyZ9$7qwErty99 address 198.51.100.3 netmask 255.255.255.255 no- →xauth no-config-mode

!— Phase 2 crypto ipsec transform-set 3dessha1 esp-3des esp-sha-hmac access-list PFSVPN permit ip 10.5.0.0 255.255.255.0 10.3.0.0 255.255.255.0 crypto map dyn-map 10 ipsec-isakmp crypto map dyn-map 10 match address PFSVPN crypto map dyn-map 10 set peer 198.51.100.3 crypto map dyn-map 10 set transform-set 3dessha1 crypto map dyn-map 10 set security-association lifetime seconds 3600 crypto map dyn-map interface outside

!— no-nat to ensure it routes via the tunnel access-list nonat permit ip 10.5.0.0 255.255.255.0 10.3.0.0 255.255.255.0 nat (inside) 0 access-list nonat

Cisco PIX OS 7.x, 8.x, eASA

La configurazione sulle revisioni più recenti del sistema operativo PIX e per i dispositivi ASA è simile a quella dei più vecchi, ma presenta alcune differenze significative. L'esempio seguente sarebbe per l'utilizzo di un PIX con OS versione 7.x o 8.X, o un dispositivo ASA, come sito B nell'esempio da sito-a-sito precedente in questo capitolo.

crypto isakmp enable outside

!— Phase 1 crypto isakmp policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400

tunnel-group 198.51.100.3 type ipsec-l2l tunnel-group 198.51.100.3 ipsec-attributes pre-shared-key aBc123%XyZ9$7qwErty99

!— Phase 2 crypto ipsec transform-set 3dessha1 esp-3des esp-sha-hmac access-list PFSVPN extended permit ip 10.5.0.0 255.255.255.0 10.3.0.0 255.255.255.0 crypto map outside_map 20 match address PFSVPN crypto map outside_map 20 set peer 198.51.100.3

crypto map outside_map 20 set transform-set 3dessha1 crypto map outside_map interface outside

!— no-nat to ensure it routes via the tunnel access-list nonat extended permit ip 10.5.0.0 255.255.255.0 10.3.0.0 255.255.255.0 nat (inside) 0 access-list nonat

Router per iOS di Cisco

Questo mostra un router basato su Cisco per IOS come sito B dall'esempio di configurazione sito-sito precedente nel capitolo.

```
!--- Phase 1
```

crypto isakmp policy 10 encr 3des authentication pre-share group 2 crypto isakmp key aBc123%XyZ9$7qwErty99 address 198.51.100.3 no-xauth

!— Phase 2 access-list 100 permit ip 10.3.0.0 0.0.0.255 10.5.0.0 0.0.0.255 access-list 100 permit ip 10.5.0.0 0.0.0.255 10.3.0.0 0.0.0.255 crypto ipsec transform-set 3DES-SHA esp-3des esp-sha-hmac crypto map PFSVPN 15 ipsec-isakmp set peer 198.51.100.3 set transform-set 3DES-SHA match address 100

!— Assign the crypto map to the WAN interface interface FastEthernet0/0 crypto map PFSVPN

!— No-Nat so this traffic goes via the tunnel, not the WAN ip nat inside source route-map NONAT interface FastEthernet0/0 overload access-list 110 deny ip 10.5.0.0 0.0.0.255 10.3.0.0 0.0.0.255 access-list 110 permit ip 10.5.0.0 0.0.0.255 any route-map NONAT permit 10 match ip address 110

IPsec fornisce un'implementazione standard basata sulla VPN compatibile con una vasta gamma di client per la connettività mobile e altri firewall e router per la connettività sito-a-sito. Supporta numerosi dispositivi di terze parti e viene utilizzato in produzione con dispositivi che vanno dai router Linksys di tipo consumatore fino ai computer centrali IBM z/OS e tutto ciò che si possa immaginare in mezzo. Questo capitolo descrive le opzioni di configurazione disponibili e come configurare vari scenari comuni.

Vedi anche:

Per la discussione generale dei vari tipi di VPN disponibili nel software Firew4LL e dei loro pro e contro, vedere *reti private virtuali*.

Il software Firew4LL supporta IPsec con IKEv1 e IKEv2, più definizioni di fase 2 per ogni tunnel, così come l'NAT Traversal, NAT sulle definizioni di fase 2, un gran numero di opzioni di crittografia e hash, e molte altre opzioni per i client mobili, tra cui xauth e EAP.

18.1.9 Terminologia di IPsec

Prima di approfondire troppo la configurazione, ci sono alcuni termini che vengono utilizzati in tutto il capitolo che richiedono spiegazioni. Altri termini sono spiegati in modo più dettagliato sul loro utilizzo nelle opzioni di configurazione.

IKE

IKE sta per *Scambio di chiavi per interne (Internet Key Exchange)*, ed è disponibile in due diverse varietà: IKEv1 e IKEv2. Quasi tutti i dispositivi che supportano IPsec utilizzano IKEv1. Un numero crescente di dispositivi supporta anche il nuovo protocollo IKEv2 che è una versione aggiornata di IKE che risolve alcune delle difficoltà presenti nella versione precedente. Ad esempio, IKEv2 ha MOBIKE, che è uno standard per i client mobili che consente loro di cambiare gli indirizzi in modo dinamico. Ha anche l'NAT Traversal incorporato, e meccanismi standard per l'affidabilità simile a DPD. In generale IKEv2 fornisce un'esperienza più stabile e affidabile, a condizione che entrambe le estremità lo supportino sufficientemente.

Associazione per la sicurezza dell'ISAKMP

ISAKMP sta per *Associazione per la sicurezza di internet e protocollo di gestione delle chiavi (Internet Security Association and Key Management Protocol).* Fornisce a entrambe le parti un meccanismo attraverso il quale possono impostare un canale di comunicazione sicuro, incluso lo scambio di chiavi e la fornitura di autenticazione.

Un'associazione di sicurezza ISAKMP (ISAKMP SA) è una politica a senso unico che definisce come il traffico verrà crittografato e gestito. Ogni tunnel IPsec attivo avrà due associazioni di sicurezza, una per ogni direzione. Le associazioni di sicurezza ISAKMP vengono impostate tra gli indirizzi IP pubblici per ciascun endpoint. La conoscenza di queste associazioni di sicurezza attive è conservata nel database dell'associazione di sicurezza (Security Association Database , SAD).

Politica di sicurezza

Una politica di sicurezza gestisce le specifiche complete del tunnel IPsec. Come per le associazioni di sicurezza, queste sono a senso unico, quindi per ogni tunnel ce ne sarà una in ogni direzione. Queste voci sono conservate nel database delle politiche di sicurezza (Security Policy Database, SPD). L'SPD è popolato da due voci per ogni connessione tunnel non appena viene aggiunto un tunnel. Al contrario, le voci SAD esistono solo al successo della negoziazione della connessione.

Nel software di Firew4LL, le politiche di sicurezza controllano quale traffico verrà intercettato dal kernel per la consegna tramite IPsec.

Fase 1

Ci sono due fasi di negoziazione per un tunnel IPsec. Durante la fase 1, i due endpoint di un tunnel impostano un canale sicuro tra t'utilizzo di ISAKMP per negoziare le voci SA e le chiavi di scambio. Ciò include anche l'autenticazione, il controllo degli identificatori e il controllo delle chiavi pre-condivise (PSK) o dei certificati. Quando la fase 1 è completa, le due estremità possono scambiare informazioni in modo sicuro, ma non hanno ancora deciso quale traffico attraverserà il tunnel o la sua crittografia.

Fase 2

Nella fase 2, i due endpoint negoziano su come crittografare e inviare i dati per gli host privati in base alle politiche di sicurezza. Questa parte crea il tunnel utilizzato per il trasferimento dei dati tra gli endpoint e i client il cui traffico è gestito da tali endpoint. Se le politiche da entrambe le parti sono d'accordo e la fase 2 è stata stabilita con successo, il tunnel sarà pronto per l'uso per il traffico che corrisponde alle definizioni di fase 2.

18.2 OpenVPN

18.2.1 OpenVPN e IPv6

OpenVPN può collegare un tunnel sito-a-sito a un indirizzo IPv4 o a un indirizzo IPv6 e il traffico IPv4 e IPv6 può essere passato contemporaneamente all'interno di un tunnel OpenVPN. IPv6 è supportato sia in client sito-a-sito e mobile, e può essere utilizzato per fornire IPv6 a un sito che ha solo connettività IPv4. Al fine di garantire il supporto al client mobile per IPv6, ottenere il software del client dal pacchetto di esportazione del client OpenVPN o scaricare un client basato su OpenVPN 2.3 o più recente.

18.2.2 Opzioni di configurazione di OpenVPN

Questa sezione descrive tutte le opzioni disponibili con OpenVPN e quando vengono utilizzate in genere. Le sezioni successive coprono esempi di configurazione di VPN con sito-a-sito e accesso remoto con OpenVPN, utilizzando le opzioni più comuni e una configurazione minima.

Opzioni di configurazione del server

Queste opzioni sono disponibili in una o più modalità per le istanze del server OpenVPN, gestite in **VPN>OpenVPN**, nella scheda **Server**.

Disabilitare questo server

Selezionare questa casella e fare clic su Salvare per mantenere la configurazione, ma non abilitare il server. Il processo per questa istanza verrà interrotto e tutti i peer/client verranno disconnessi da questo server. Tutti gli altri server attivi non sono interessati.

Modalità del server

Questo è il ruolo per il server, che specifica come i router o gli utenti si connetteranno a questa istanza del server. La modifica di questo influenzerà anche quali opzioni appariranno sul resto della pagina, quindi vengono visualizzate solo le scelte rilevanti.

Peer a Peer (SSL/TLS) Una connessione tra reti locali e remote che è protetta da SSL/TLS. Questa scelta offre una maggiore sicurezza e la possibilità per il server di spingere i comandi di configurazione al router del peer remoto quando si utilizza una configurazione 1:molti stili. I router del peer remoti possono anche avere certificati revocati per rimuovere l'accesso se vengono compromessi.

Peer a Peer (chiave condivisa) Una connessione tra reti locali e remote che è protetta da una singola chiave condivisa configurata su entrambi i nodi. Questa scelta è più facile da configurare, ma è meno sicura. Se una chiave condivisa è compromessa, una nuova chiave deve essere generata e quindi copiata su qualsiasi router o client utilizzando la vecchia chiave condivisa. In questa modalità, è necessaria un'istanza server separata per ciascun client.

Accesso remoto (SSL/TLS) Questa scelta è una configurazione client mobile con certificati X.509 per utente. Come per il tipo di connessione peer-a-peer con SSL/TLS, l'utilizzo di questo metodo offre una maggiore sicurezza e la possibilità per il server di spingere i comandi di configurazione ai client. I client mobili possono anche avere chiavi revocate per rimuovere l'accesso se una chiave è compromessa, ad esempio un laptop rubato o smarrito.

Accesso remoto (autenticazione utente) Un server di accesso client che non utilizza i certificati, ma richiede all'utente finale di fornire un nome utente e una password quando si effettua una connessione. Questo non è raccomandato a meno che l'autenticazione non sia gestita esternamente da LDAP o RADIUS.

Accesso remoto (SSL/TLS + Autenticazione utente) La scelta più sicura offerta. Non solo ottiene i vantaggi di altre scelte SSL/TLS, ma richiede anche un nome utente e una password dal client quando si connette. L'accesso al client può essere rimosso non solo revocando il certificato, ma anche modificando la password. Inoltre, se una chiave compromessa non viene immediatamente scoperta, il pericolo viene diminuito perché è improbabile che l'attaccante abbia le chiavi e la password. Quando si utilizza la procedura guidata OpenVPN, questa è la modalità configurata durante tale processo.

Protocollo

TCP o UDP possono essere selezionati, o le loro controparti con IPv6 abilitato, TCP6 o UDP6. Un'istanza del server OpenVPN può attualmente associare solo a IPv4 o IPv6, ma non entrambi allo stesso tempo. UDP è la scelta più affidabile e veloce per l'esecuzione di OpenVPN e dovrebbe essere sempre utilizzata quando possibile. In alcuni rari casi TCP può essere utilizzato per aggirare le limitazioni, ad esempio bypassando alcuni firewall eseguendo un server OpenVPN sulla porta TCP 443.

I protocolli senza connessione come UDP sono sempre preferibili quando si esegue il tunnel del traffico. TCP è orientato alla connessione con la consegna garantita, quindi tutti i pacchetti persi vengono ritrasmessi. Questo suona come una buona idea in superficie, ma le ritrasmissioni TCP causeranno una significativa degradazione delle prestazioni su connessioni Internet pesantemente caricate o su quelle con una perdita di pacchetti coerente.

Il traffico TCP esiste spesso all'interno dei tunnel ed è indesiderabile ritrasmettere i pacchetti persi dal traffico VPN incapsulato. Nei casi in cui TCP è avvolto attorno a TCP, ad esempio un tunnel VPN che utilizza TCP come protocollo di trasporto, quando un pacchetto viene perso, i pacchetti TCP persi esterni e interni verranno ritrasmessi. Le occorrenze rare di questo saranno impercettibili ma la perdita ricorrente causerà prestazioni significativamente inferiori rispetto a UDP. Se il traffico all'interno del tunnel richiede una consegna affidabile, utilizzerà un protocollo come TCP che lo assicura e gestirà le proprie ritrasmissioni.

Modalità dispositivo

OpenVPN può essere eseguito in una delle due modalità del dispositivo: *tun* o *tap*:

tun Funziona su OSI di livello 3 ed esegue il routing su interfacce punto-a-punto.

tap Può funzionare su OSI di livello 2 e può eseguire sia il routing che il bridging se necessario.

Nota: Non tutti i client supportano la modalità tap, l'utilizzo di tun è più stabile e più ampiamente supportato. In particolare, i client come quelli trovati su Android e iOS supportano solo la modalità tun nelle app che la maggior parte delle persone può utilizzare. Alcune app OpenVPN Android e iOS che richiedono il rooting o il jailbreaking di undispositivo supportano tap, ma le conseguenze del suo utilizzo possono essere un po" troppo pesanti per la maggior parte degli utenti.

Interfaccia

Selezionare il gruppo di interfaccia, VIP o failover che l'istanza del server OpenVPN ascolterà per le connessioni in entrata. Questo controlla anche da quale interfaccia uscirà il traffico dal server.

Diversi tipi di opzioni sono elencati nel menu a discesa di **Interfaccia**, e alcuni hanno un comportamento speciale o casi d'uso:

Interfacce OpenVPN si legherà all'indirizzo dell'interfaccia. Se l'interfaccia è dinamica, come DHCP, OpenVPN si legherà automaticamente al nuovo indirizzo se cambia.

VIP OpenVPN si legherà solo al VIP specificato (Alias di IP o tipo CARP)

Gruppi di gateway Da utilizzare con i gruppi di failover, OpenVPN si legherà all'indirizzo dell'interfaccia attualmente attiva nel gruppo. Se quel gateway di interfaccia diventa irraggiungibile, verrà utilizzato il successivo e così via.

Host locale Utile per le distribuzioni Multi-WAN, l'associazione a host locali e l'utilizzo di porte forward per accettare connessioni da diverse interfacce e/o porte è un modo versatile per fornire connettività OpenVPN ridondante per la connessione dei client.

Qualsiasi Si lega a ogni indirizzo su ogni interfaccia. Anche se allettante, questa opzione non è raccomandata. Quando viene utilizzato con UDP, le risposte ai client Internet usciranno sempre di nuovo dalla WAN del gateway predefinito, il che potrebbe essere indesiderabile.

Porta locale

La porta locale è il numero di porta che OpenVPN utilizzerà per ascoltare. Le regole del firewall devono consentire il traffico verso questa porta e devono essere specificate nella configurazione del client. La porta per ogni server deve essere univoca per ogni interfaccia.

Descrizione

Immettere una descrizione per questa configurazione del server, per riferimento.

Impostazioni crittografiche

Questa sezione controlla come il traffico da e verso i client viene crittografato e convalidato.

Chiave condivisa

Quando si utilizza un'istanza di chiave condivisa, selezionare la casella **Generare automaticamente una chiave condivisa** per creare una nuova chiave o deselezionare la casella per incollare una chiave condivisa da un tunnel OpenVPN esistente. Quando si genera automaticamente la chiave, tornare alla schermata di modifica per questo tunnel in seguito per ottenere la chiave che può essere copiata sul router remoto.

Autenticazione TLS

TLS, o Sicurezza del livello di trasporto (Transport Layer Security), fornisce l'autenticazione della sessione per garantire la validità sia del client che del server. Selezionare la casella **Abilitare l'autenticazione dei pacchetti TLS** se lo si desidera. Se non esiste una chiave TLS esistente, lasciare **Generare automaticamente una chiave di autenticazione TLS condivisa** selezionata. Se la chiave esiste già, deselezionare l'opzione e quindi incollarla nella casella di immissione fornita. Quando si genera automaticamente la chiave, tornare alla schermata di modifica per questo tunnel in seguito per ottenere la chiave che può essere copiata sul router o sul client remoto.

Avvertimento: Quando si utilizza una modalità SSL/TLS, si consiglia vivamente di utilizzare pure l'autenticazione TLS. Oltre al vantaggio di sicurezza aggiunto dal requisito chiave, una chiave TLS aiuta anche a proteggere da alcuni attacchi basati su SSL come Heartbleed.

Autorità del certificazione del Peer

Selezionare l'autorità di certificazione utilizzata per firmare il certificato server per questa istanza del server OpenVPN qui. Se nulla appare in questo elenco, prima importare o generare un'autorità di certificazione in **Sistema>Gestione dei certificati**, nella scheda **CA**.

Elenco di revoca dei certificati dei peer

Questo campo ipzionale indica l'elenco di revoca dei certificati (Certificate Revocation List, CRL) che deve essere utilizzato da questo tunnel. Un CRL è un elenco di certificati ottenuti da una determinata CA che non sono più considerati validi. Ciò potrebbe essere dovuto a un certificato compromesso o perso, ad esempio da un laptop rubato, infezione da spyware, ecc. Un CRL può essere creato o gestito da **Sistema>Gestione dei certificati**, nella scheda **Revoca dei certificati**.

Certificato del server

Un certificato del server deve essere scelto per ogni istanza del server OpenVPN. Se nulla appare in questo elenco, prima importare o generare un'autorità di certificazione in **Sistema>Gestione dei certificati**, nella scheda **Certificati**.

Lunghezza dei parametri DH

I parametri dello scambio di chiave Diffie-Hellman (DH) vengono utilizzati per stabilire un canale di comunicazione sicuro. Possono essere rigenerati in qualsiasi momento e non sono specifici per un'istanza OpenVPN. Cioè, quando si importa una configurazione OpenVPN esistente, questi parametri non devono essere copiati dal server precedente. La lunghezza dei parametri DH desiderati può essere scelta dalla casella del menu a discesa, 1024, 2048 o 4096.

Nota: a causa del calcolo pesante coinvolto nella generazione di chiavi DH, viene utilizzato un set pre-generato per ogni tipo di chiave. I nuovi parametri DH possono essere generati manualmente utilizzando i seguenti comandi della shell:: # /usr/bin/openssl dhparam 1024 > /etc/dh-parameters.1024 # /usr/bin/openssl dhparam 2048 > /etc/dh-parameters.2048 # /usr/bin/openssl dhparam 4096 > /etc/dh-parameters.4096

Algoritmo di crittografia

Il cifrario crittografico da utilizzare per questa connessione. Il valore predefinito è *AES-128-CBC*, che è il concatenamento del blocco del cifrario (Cipher Block Chaining) di AES 128 Bit. Questa è una buona scelta per la maggior parte degli scenari.

Vedi anche:

Crittografia dell'hardware per ulteriori informazioni sull'utilizzo di acceleratori crittografici e sulla scelta di un algoritmo di crittografia.

Algoritmo Digest Auth

Selezionare l'algoritmo digest del messaggio da utilizzare per l'autenticazione HMAC dei pacchetti in arrivo.

Nota: OpenVPN è impostasto in maniera predefinita su SHA1 quando questa opzione non è specificata altrimenti, quindi a meno che entrambi i lati non siano impostati su un valore noto, utilizzare qui SHA1.

Crittografia Hardware

Se disponibile, questa opzione controlla quale acceleratore crittografico dell'hardware verrà utilizzato da OpenVPN. Quando è lasciato non specificato, OpenVPN sceglierà automaticamente in base a ciò che è disponibile nel sistema operativo.

Se questo dispositivo firewall dispone di un acceleratore crittografico hardware, scegliere la **macchina per la crittografia di BSD (BSD Cryptodev Engine)** o selezionare il dispositivo specifico se appare nell'elenco. La maggior parte delle schede dell'acceleratore utilizza la macchina per la crittografia di BSD, quindi in caso di dubbio, selezionarla. Questa impostazione consentirà a OpenVPN di sfruttare l'accelerazione hardware. È inoltre necessario selezionare un algoritmo di crittografia supportato dall'acceleratore. Fare riferimento alla documentazione dell'hardware per informazioni sui cifrari supportati dall'acceleratore.

Profondità del certificato

Questa opzione limita la lunghezza di una catena di certificati prima che fallisca la convalida. Questo valore predefinito è *Uno (Client + Server)* in modo che se in qualche modo viene generata una CA intermedia non autorizzata, i

certificati firmati da un intermediario rude falliranno la convalida. Nei casi in cui è richiesto il concatenamento con gli intermediari, questo limite può essere aumentato.

Corrispondenza con un utente-CN rigorosa

Per un server con SSL/TLS+Autenticazione dell'utente, se abilitata, questa opzione impone una corrispondenza tra il nome utente fornito dall'utente e il nome comune del certificato utente. Se i due non corrispondono, la connessione viene rifiutata. Ciò impedisce agli utenti di utilizzare le proprie credenziali con il certificato di un'altra persona e viceversa.

Impostazioni del tunnel

La sezione delle impostazioni del tunnel regola il modo in cui il traffico scorre tra il server e i client, tra cui il routing e la compressione.

La rete del tunnel IPv4/IPv6

Questi sono i pool di indirizzi da assegnare ai client al momento della connessione. La fine del server della configurazione OpenVPN utilizzerà il primo indirizzo in questo pool per la fine della connessione e assegnerà indirizzi aggiuntivi ai client connessi in base alle esigenze. Questi indirizzi sono utilizzati per la comunicazione diretta tra gli endpoint del tunnel, anche quando si collegano due reti remote esistenti. Qualsiasi sottorete può essere scelta a condizione che non sia in uso localmente o in qualsiasi sito remoto. Uno o entrambe la **rete del tunnel IPv4** e la **rete del tunnel IPv6** possono essere inserite, o nel caso di un ponte con il tap, nessuna delle due.

> **Avvertimento:** attualmente, le limitazioni in OpenVPN impediscono l'esecuzione solo con una configurazione per la rete del tunnel IPv6. Quando viene definita una rete del tunnel IPv6, è necessario specificare anche una rete del tunnel IPv4, anche se non viene utilizzata.

Per un server SSL/TLS con sito-a-sito che utilizza IPv4, la dimensione della **rete del tunnel IPv4** può modificare il comportamento del server. Se x.x.x. x/30 viene inserito per la **rete del tunnel IPv4**, il server utilizzerà una modalità peer-a-peer in modo molto simile a come funziona la chiave condivisa: può avere solo un client, non richiede sostituzioni specifiche del client o *iroute*, ma non può anche spingere percorsi o impostazioni ai client. Se viene utilizzata una **rete del tunnel IPv4** più grande di quella utilizzata, ad esempio x.x.x.x/24, il server accetterà più client e potrà spingere le impostazioni, ma richiede *iroute*.

Vedi anche:

Vedere *Configurazione di esempio con sito-a-sito (SSL/TLS)* per ulteriori informazioni su un esempio da sito-a-multi-sito utilizzando una grande rete di tunnel e *iroute*.

Opzioni di bridging

Quando si utilizza la modalità tap, vengono mostrate opzioni aggiuntive che controllano il comportamento di bridging in OpenVPN e l'assegnazione degli indirizzi del client. Questi sono coperti in *Connessioni OpenVPN con il ponte*

Gateway per il reindirizzamento

Quando viene selezionata l'opzione **Gateway per il reindirizzamento**, il server invierà un messaggio ai client che li istruiranno per inoltrare tutto il traffico, incluso il traffico Internet, attraverso il tunnel VPN. Funziona solo in modalità SSL/TLS con una rete del tunnel più grande di una sottorete a / 30.

Rete locale IPv4/IPv6

Questi campi specificano quali reti locali sono raggiungibili dai client VPN, se presenti. Un percorso per queste reti viene spinto ai client che si connettono a questo server. Se sono necessari più percorsi per le sottoreti di una particolare famiglia, immettere le sottoreti separate da una virgola, ad esempio 192.168.2.0/24, 192.168.56.0/24.

Questa funzione si basa sulla capacità di spingere i percorsi al client, quindi per IPv4 è valida solo in un contesto SSL/TLS quando è in uso una rete tunnel più grande di a /30. Funzionerà sempre per IPv6 a condizione che una maschera troppo piccola simile non sia impostata.

Rete remota IPv4/IPv6

Questa opzione viene visualizzata solo quando viene utilizzata una connessione di tipo Peer-a-Peer e non è disponibile per i client mobili. Le voci della tabella delle route vengono aggiunte al firewall per le sottoreti specificate, che consegnano il traffico a questa istanza OpenVPN per l'elaborazione. Se è necessaria più di una sottorete di rete remota, immettere le sottoreti separate da una virgola, ad esempio 192.168.2.0/24, 192.168.56.0/24..

Connessioni simultanee

Specifica il numero di client che possono essere collegati simultaneamente a questa istanza del server OpenVPN in un dato momento. Questo è un limite collettivo per tutti i client connessi, non un'impostazione per utente.

Compressione

Quando la compressione è abilitata, il traffico che attraversa la connessione OpenVPN verrà compresso prima di essere crittografato. Ciò consente di risparmiare sull'utilizzo della larghezza di banda per molti tipi di traffico a scapito di un maggiore utilizzo della CPU sia sul server che sul client. Generalmente questo impatto è minimo e l'abilitazione della compressione è utile per quasi tutti gli usi di OpenVPN su Internet.

Per le connessioni ad alta velocità, come ad esempio l'utilizzo di OpenVPN attraverso una LAN, WAN ad alta velocità e bassa latenza WAN, o rete wireless locale, questo può essere indesiderabile, come il ritardo aggiunto dalla compressione può essere più che il ritardo salvato nella trasmissione del traffico. Se quasi tutto il traffico che attraversa la connessione OpenVPN è già crittografato (come SSH, SCP, HTTPS, tra molti altri protocolli), non abilitare la compressione LZO perché i dati crittografati non sono comprimibili e la compressione LZO causerà un po" più di dati da trasferire di quanto sarebbero senza compressione. Lo stesso vale se il traffico VPN presenta quasi interamente dati già compressi.

Questo selettore controlla la gestione della compressione LZO per questa istanza OpenVPN. Ci sono quattro possibili impostazioni ciascuna con un comportamento leggermente diverso.

> **Nessuna preferenza** Omette completamente le direttive di compressione dalla configurazione OpenVPN. Non verrà eseguita alcuna compressione, ma questa opzione potrebbe essere sovrascritta da altri metodi come le sostituzioni specifiche del client o le opzioni avanzate.
>
> **Disabilitata - nessuna compressione** Disabilita esplicitamente la compressione nella configurazione

Abilitata con compressione adattiva Consente la compressione con un test periodico per garantire che il traffico sia in grado di essere compresso. Se la compressione non è ottimale, verrà disabilitata fino a quando non verrà nuovamente testata. Questa opzione ottine il miglior equilibrio dal momento che comprimerà i dati quando è utile, ma non comprime i dati quando ne ostacola le prestazioni.

Abilitato senza compressione adattiva Consente esplicitamente la compressione in ogni momento ma senza testare il traffico.

Tipo di servizio

Quando questa opzione è abilitata, OpenVPN imposterà il valore di intestazione IP per il tipo di servizio (Type-of-Service, TOS) dei pacchetti del tunnel in modo che corrisponda al valore del pacchetto incapsulato. Ciò può causare un traffico importante da gestire più velocemente attraverso il tunnel dall'hot intermediario, al costo di alcune informazioni di divulgazione di meno.

L'esempio più comune è il traffico VoIP o video. Se il bit TOS è impostato per riflettere la priorità del traffico, può aiutare QoS lungo il percorso, ma qualcuno che intercetta il traffico potrebbe vedere il bit TOS e acquisire alcune conoscenze sul contenuto del traffico all'interno del tunnel. Per coloro che si affidano a bit TOS per QoS, il vantaggio potrebbe superare la perdita di informazioni.

Comunicazione tra client

Questa opzione controlla se i client connessi sono in grado di comunicare tra loro o meno. Per consentire questo comportamento, selezionare l'opzione. Se deselezionata, i client possono inviare solo traffico al server o destinazioni oltre il server, ad esempio le reti instradate o Internet.

In genere nelle distribuzioni con stile di accesso remoto non è necessario che i client si raggiungano a vicenda, ma ci sono alcuni casi limite in cui può essere utile. Un esempio è che gli sviluppatori Web remoti lavorino insieme e eseguano server di test sui loro sistemi locali. Con questa opzione attivata, possono raggiungere l'altro server del test per lo sviluppo collaborativo.

Duplicare le connessioni

Per impostazione predefinita, OpenVPN assocerà un indirizzo IP dalla sua rete tunnel con un certificato o un nome utente specifico per una determinata sessione. Se lo stesso certificato si connette di nuovo, verrà assegnato lo stesso indirizzo IP e disconnetterà il primo client o causarà un conflitto IP in cui nessuno dei due client riceverà dati corretti. Questo è principalmente per motivi di sicurezza, quindi lo stesso certificato non può essere utilizzato da più persone contemporaneamente. Si consiglia di utilizzare un certificato univoco per ogni utente che si connette. Altrimenti, se un client è compromesso, non è possibile revocare solo un client, i certificati dovrebbero essere ristampati a tutti i client che condividono lo stesso certificato.

Se una configurazione che utilizza lo stesso certificato in più posizioni è un requisito assoluto e non può essere evitata, controllare **Duplicare le connessioni** per consentire il comportamento non standard di più client che utilizzano lo stesso certificato o nome utente.

Disabilitare IPv6

Quando selezionato, l'inoltro del traffico IPv6 è disabilitato per questa istanza OpenVPN.

Impostazioni del client

Queste impostazioni riguardano il comportamento dei client che si connettono a questa istanza del server.

IP dinamico

Selezionando questa casella si aggiunge l'opzione di configurazione *dinamica (float)* alla configurazione OpenVPN. Ciò consente ai client di mantenere la loro connessione se il loro indirizzo IP cambia. simile a MOBIKE per IKEv2 in IPsec. Per i client su connessioni Internet in cui l'IP cambia frequentemente o gli utenti mobili che si spostano comunemente tra diverse connessioni Internet, selezionare questa opzione per consentire una connettività stabile. Quando l'IP client è statico o raramente cambia, non utilizzare questa opzione offre un piccolo miglioramento della sicurezza.

Pool degli indirizzi

Quando questa opzione è abilitata, il server assegnerà gli indirizzi IP dell'adattatore virtuale ai client dalla sottorete specificata dall'opzione **Rete del tunnel**. Quando è deselezionata gli indirizzi IP non verranno assegnati automaticamente e i client dovranno impostare manualmente i propri indirizzi IP statici nei file di configurazione del client. Tranne in rari casi, questa opzione è quasi sempre abilitata.

Topologia

Per impostazione predefinita OpenVPN su Firew4LL 2.3 e successivi preferisce uno stile di topologia di *sottorete* quando si utilizza una **Modalità dispositivo** *tun*. Questo stile alloca solo un indirizzo IP per client piuttosto che una sottorete isolata per client. Questo è l'unico stile disponibile quando si utilizza la **modalità dispositivo** *tap*.

Quando viene scelta la topologia *net30* più vecchia per *tun*, OpenVPN assegna una rete CIDR /30 (quattro indirizzi IP, due utilizzabili) a ciascun client di connessione. Questo stile ha una storia più lunga, ma può essere fonte di confusione per gli amministratori e gli utenti.

L'opzione **topologia** è rilevante solo quando si fornisce un indirizzo IP dell'adattatore virtuale ai client che utilizzano la modalità *tun* su IPv4. Alcuni client potrebbero richiederlo anche per IPv6, come OpenVPN Connect, anche se in realtà IPv6 viene sempre eseguito con una topologia di *sottorete* anche quando IPv4 utilizza *net30*. OpenVPN versione 2.1.3 o successive è necessario per utilizzare una topologia di *sottorete*, e ci sono pure state correzioni significative ad essa in OpenVPN 2.3, allo stesso modo è importante utilizzare una versione corrente del client di OpenVPN.

Avvertimento: il valore predefinito in pfSense è stato modificato in sottorete perché il progetto OpenVPN ha dichiarato lo stile net30 come deprecato, indicando che verrà rimosso nelle versioni future. Tenere presente, tuttavia, che alcuni client molto vecchi potrebbero rompersi se questa opzione viene utilizzata, come le versioni precedenti di OpenVPN (prima di 2.0.9, rilasciate quasi 10 anni fa), le versioni di Windows con driver tun/tap precedenti o client come i telefoni Yealink. Assicurarsi sempre che il client e i driver associati siano completamente aggiornati quando si utilizza una topologia di sottorete.

Dominio predefinito del DNS

Una volta selezionato, apparirà un campo per specificare il nome di dominio del DNS da assegnare ai client. Per garantire che la risoluzione dei nomi funzioni correttamente per gli host della rete locale in cui viene utilizzata la risoluzione dei nomi DNS, specificare qui il nome di dominio del DNS interno. Per gli ambienti con Directory attiva di Microsoft, questo di solito sarebbe il nome di dominio della directory attiva.

Server del DNS

Una volta selezionato, è possibile immettere fino a quattro server DNS per l'utilizzo da parte del client mentre è connesso alla VPN. Per gli ambienti con Directory attiva di Microsoft, in genere si tratta dei controllori del dominio della directory attiva o dei server DNS per la risoluzione e l'autenticazione dei nomi corretti quando si è connessi tramite OpenVPN.

Forzare l'aggiornamento della cache del DNS

Una volta selezionata, questa opzione spingerà una serie di comandi ai client di Windows che scaricheranno il loro DNS e riavvieranno la cache per migliorare la gestione dei client dei server DNS aggiornati dalla VPN.

Server NTP

Una volta selezionato, è possibile impostare uno o due server NTP per la sincronizzazione degli orologi sui client. Può essere un indirizzo IP o FQDN.

Opzioni del NetBIOS

Quando si attiva NetBIOS su TCP/IP, verranno visualizzate diverse altre opzioni relative a NetBIOS e WINS. Se la casella è deselezionata, queste impostazioni saranno disabilitate.

Tipo di nodo

Il tipo di nodo del NetBIOS controlla il funzionamento dei sistemi Windows durante la risoluzione dei nomi del NetBIOS. Di solito va bene lasciare questo a *nessuno* per accettare l'impostazione predefinita di Windows.

Le opzioni disponibili includono:

Nodo-B Utilizza le trasmissioni per la risoluzione dei nomi del NetBIOS. Questa non va usata se non nel caso di un ponte tap.

Nodo-P Il nome con punto-a-punto richiede un server WINS. WINS è stato per lo più deprecato, quindi questa opzione non è utile nelle moderne reti Windows.

Nodo-M La trasmissione interroga il server dei nomi. Simile a nodo-B ma ricadrà sul DNS.

Nodo-H Richiede prima il nome del server, poi utilizza la trasmissione. Questa opzione è quella con maggiore probabilità di successo in una rete corrente con DNS corretto, funzionale.

ID dell'ambito

Un ID dell'ambito di NetBIOS fornisce un servizio di denominazione esteso per NetBIOS su TCP/IP. L'ID dell'ambito di NetBIOS isola il traffico NetBIOS su una singola rete solo a quei nodi con lo stesso ID dell'ambito di NetBIOS.

Server WINS

Selezionando questa casella è possibile definire due server WINS che forniscono la risoluzione dei nomi per i client che accedono e navigano nelle risorse del NetBIOS attraverso la VPN. WINS è stato ampiamente deprecato e rimosso dall'uso, quindi è improbabile che ciò sia necessario nella maggior parte degli ambienti moderni.

Abilitare una porta personalizzata

Una volta selezionata, è possibile specificare una **porta di gestione** non predefinita da utilizzare con la funzione Gestione della OpenVPN del pacchetto di esportazione dei client della OpenVPN. Se vengono utilizzati più profili di connessioni su un singolo client che utilizza tale interfaccia, ciascuno deve utilizzare una porta di gestione univoca.

Opzioni personalizzate

Mentre l'interfaccia web di Firew4LL supporta le opzioni più comunemente utilizzate, OpenVPN è molto potente e flessibile e, occasionalmente, le opzioni che non sono disponibili nell'interfaccia web potrebbero essere necessarie. Tali opzioni personalizzate possono essere aggiunte utilizzando questa casella di immissione. Queste opzioni sono descritte ulteriormente nelle opzioni di configurazione personalizzate.

Livello di dettaglio (verbosità)

Configura la quantità di dettagli mostrata nei registri OpenVPN per questa istanza, utile per la risoluzione dei problemi. Numeri più alti si tradurranno in maggiori quantità di dettagli nel registro. Durante il normale funzionamento la selezione *predefinita* è la migliore.

Nota: Se impostato su livelli più alti, la pagina di stato di OpenVPN e il widget della dashboard causeranno una registrazione aggiuntiva mentre interagiscono con il processo di gestione per sondare le informazioni dai demoni di OpenVPN.

Opzioni di configurazione del client

Queste opzioni sono disponibili in una o più modalità per le istanze dei client di OpenVPN, gestite da **VPN>OpenVPN**, nella scheda **Client**.

Molte di queste opzioni sono identiche alle opzioni del server sopra menzionate, quindi verranno notate solo le differenze.

Modalità del server

Per le istanze del client, le scelte della modalità del server sono limitate a *Peer a Peer (SSL/TLS)* e *Peer a Peer (chiave condivisa)*, che si accoppiano con le opzioni del server con lo stesso nome e tipo.

Interfaccia

Questa opzione seleziona l'interfaccia, VIP o il gruppo di failover che l'istanza client OpenVPN utilizzerà per le connessioni in uscita.

Quando viene selezionato un VIP di tipo CAP per l'Interfaccia nelle istanze client di OpenVPN, l'istanza OpenVPN verrà interrotta quando il VIP CARP si trova in uno stato di backup. Ciò viene fatto per impedire al nodo HA secondario di mantenere percorsi non validi o tentare di effettuare connessioni in uscita che possono interferire con la connessione attiva sul nodo HA primario.

Porta locale

Per i client, la porta locale viene lasciata vuota in quasi tutti i casi in modo da utilizzare una porta locale randomizzata. Questo è più sicuro, ma alcune implementazioni potrebbero richiedere una porta sorgente specifica. Se è richiesta una porta sorgente specifica, riempire secondo necessità.

Indirizzo o host del server

L'indirizzo IP o il nome di dominio completo per il server.

Porta del server

La porta su cui il server è in ascolto, in genere 1194

Impostazioni del proxy

Host o indirizzo del proxy L'indirizzo IP o il nome di dominio completo per un server proxy attraverso il quale questo client deve connettersi.

Opzioni extra per l'autenticazione de proxy Opzioni dell'autenticazione extra. Se impostato su *base* o *ntlm*, i campi **Nome Utente** e **Password** vengono presentati in modo che l'autenticazione proxy possa essere configurata.

Risoluzione del hostname del server

Quando viene selezionato **Server per risolvere infinitamente**, il nome host del server verrà risolto ad ogni tentativo di connessione. Quando deselezionato, OpenVPN tenterà solo di risolverlo una volta. Quando si utilizza un hostname per l'indirizzo del server remoto, questa opzione deve essere selezionata.

Impostazioni di autenticazione utente

Quando si utilizza la modalità *Peer a Peer SSL/TLS*, è possibile specificare un **Nome utente** e una **Password** in aggiunta o al posto di un certificato utente, a seconda dei requisiti configurati sul server.

Impostazioni crittografiche

Le impostazioni di questa sezione sono identiche a quelle delle opzioni corrispondenti sul lato server, ad eccezione dell'opzione nuovo **Certificato del client**, in cui il certificato è selezionato per l'uso da parte di questo client. Questo certificato (e la chiave associata e il certificato CA) devono essere importati in questo firewall prima di poter essere scelti.

Chiave condivisa/autenticazione TLS

Queste opzioni funzionano in modo simile alle controparti del lato server, ma tieni presente che la chiave dal server deve essere copiata qui, piuttosto che generare una nuova chiave sul client.

Limitare la larghezza di banda in uscita

Il valore in questa casella, specificato in **byte al secondo**, viene utilizzato per limitare la velocità del traffico VPN in uscita. Quando lasciato vuoto, non c'è limite. Il valore deve essere compreso tra *100* e *100000000*.

Non estrarre le route

Una volta selezionato, il client ignorerà i percorsi spinti dal server. Questo è utile nei casi in cui il server spinge un reindirizzamento del gateway predefinito quando questo client non ne ha bisogno.

Non aggiungere/rimuovere le route

Una volta selezionato, OpenVPN non gestirà le voci della tabella di route per questa VPN. In questo caso, devono essere gestite manualmente. I percorsi che normalmente verranno aggiunti vengono invece passati a `--route-upscript` utilizzando variabili ambientali.

18.2.3 Procedura guidata server OpenVPN per accesso remoto

La procedura guidata di OpenVPN è un modo conveniente per impostare una VPN di accesso remoto per i client mobili. Configurare tutti i prerequisiti necessari per un server di accesso remoto OpenVPN:

- Una sorgente di autenticazione (server locale, RADIUS o server LDAP)
- Un'autorità di certificazione
- Un certificato server
- Un'istanza server OpenVPN.

Entro la fine della procedura guidata un server completamente funzionante sarà configurato e pronto per gli utenti. Una configurazione di esempio verrà utilizzata per aiutare a spiegare le opzioni disponibili nella procedura guidata.

Prima di iniziare la procedura guidata

Prima di avviare la procedura guidata per configurare il server di accesso remoto, ci sono alcuni dettagli che devono essere pianificati.

Determinare uno schema di indirizzamento IP

Una sottorete IP deve essere scelta per l'uso dai client OpenVPN stessi. Questa è la sottorete compilata nella **Rete del tunnel** nella configurazione del server. I client connessi riceveranno un indirizzo IP all'interno di questa sottorete e l'estremità del server della connessione riceve anche un indirizzo IP utilizzato dal client come gateway per le reti sul lato server.

Come sempre quando si scelgono le sottoreti interne per una singola posizione, idealmente la sottorete scelta verrà progettata in modo che possa essere riassunta con CIDR con altre sottoreti interne. La rete di esempio qui descritta utilizza 10.3.0.0 / 24 per la LAN e 10.3.201.0 / 24 per OpenVPN. Queste due reti possono essere riassunte con 10.3.0.0/16, rendendo il routing più facile da gestire. La sintesi di CIDR è discussa ulteriormente nella Sintesi di CIDR.

Esempio di rete

La figura *Rete di accesso remoto dell'esempio OpenVPN* mostra la rete configurata in questo esempio.

Scegliere il tipo di autenticazione

Nella prima schermata della procedura guidata del server di accesso remoto OpenVPN, scegliere un metodo per l'autenticazione dell'utente. Le scelte disponibili per il **Tipo di backend di autenticazione** sono *Accesso dell'utente locale*, *LDAP* e *RADIUS*.

Se è già in atto un sistema di autenticazione esistente, ad esempio Directory attiva, scegliere *LDAP* o *RADIUS* in base alla configurazione del sistema. È possibile selezionare l'"*accesso dell'utente locale* per gestire gli utenti, le password e i certificati sul firewall Firew4LL. Quando si utilizza l'"*accesso dell'utente locale*, i certificati per utente possono essere utilizzati facilmente, gestiti completamente nella GUI di Firew4LL. Questo è molto più sicuro, ma a seconda del numero di utenti che accederanno al servizio, potrebbe essere meno conveniente rispetto all'utilizzo di un sistema di autenticazione centrale.

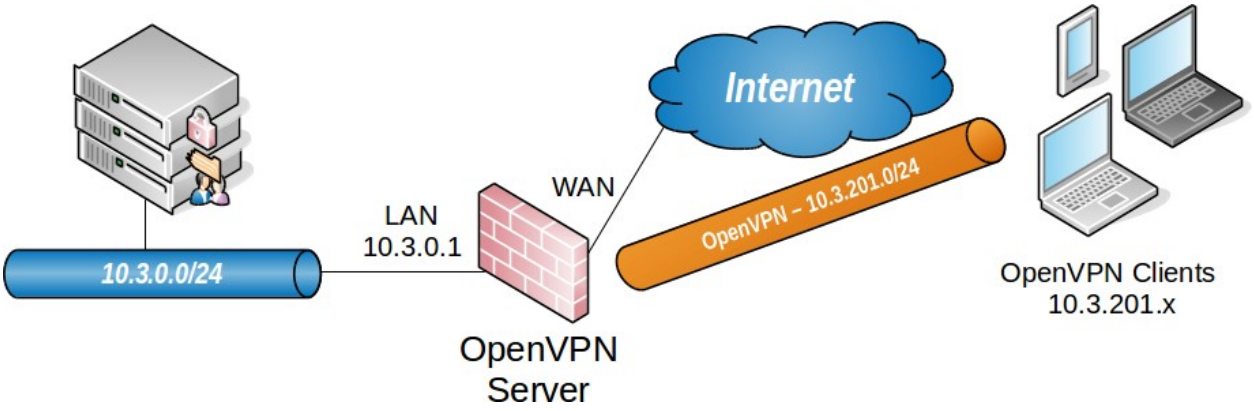


Fig. 1: Rete di accesso remoto dell'esempio OpenVPN

Nota: per LDAP o RADIUS, i certificati per utente non possono essere utilizzati senza generarli manualmente

La scelta di *Accesso dell'utente locale* è l'equivalente della scelta di *Accesso remoto (SSL/TLS + Autenticazione utente)* menzionata in precedenza in questo capitolo. *LDAP* e *RADIUS* sono equivalenti ad *Accesso remoto (autenticazione utente)*.

Dopo aver selezionato il tipo di server di autenticazione, fare clic su *Avanti*. Se *LDAP* o *RADIUS* sono stati scelti la configurazione del server per tali scelte sarà il passo successivo. Se è stato scelto *Accesso dell'utente locale*, i passaggi della procedura guidata per LDAP e RADIUS vengono saltati. Per questo esempio, verrà scelto *Accesso dell'utente locale*, ma le altre opzioni sono discusse per completezza.

Scelta di un server LDAP

Se un server LDAP è già definito sul firewall Firew4LL, può essere scelto dall'elenco. Per utilizzare un server LDAP diverso, scegliere **Aggiungere un nuovo server LDAP**. Se non sono definiti server LDAP, questo passaggio viene saltato.

Aggiunta di un server LDAP

Se non esistono server LDAP o viene scelto **Aggiungere un nuovo server LDAP**, verrà visualizzata una schermata con le opzioni necessarie per aggiungere un nuovo server. Molte di queste opzioni dipenderanno dalla specifica configurazione e struttura della directory di LDAP. In caso di incertezza sulle impostazioni, consultare l'amministratore del server LDAP, il fornitore del software o la documentazione.

Nota:

i dettagli dei server LDAP sono coperti nei *Server di autenticazione*. Alcuni dettagli sono omessi qui poiché le opzioni sono discusse in modo approfondito altrove. Per ulteriori informazioni sulle opzioni elencate in questa sezione, fare riferimento lì.

Nome Nome descrittivo per questo server LDAP, per riferimento.

Hostname o indirizzo IP L'hostname o l'indirizzo IP del server LDAP.

Porta La porta su cui può essere contattato il server LDAP. La porta predefinita è 389 per le connessioni TCP standard e 636 per SSL.

Trasporto Questo può essere impostato su *TCP-Standard* per le connessioni non crittografate, o *SSL-crittografato* per le connessioni sicure. Una connessione standard può essere sufficiente almeno per i server locali o i test iniziali. Se il server è remoto o attraversa collegamenti di rete non attendibili, SSL è una scelta più sicura. Se si desidera utilizzare SSL, il certificato CA dal server LDAP deve essere importato in Firew4LL e il **Hostname o l'indirizzo IP** di cui sopra deve corrispondere al valore nel campo **Nome comune** del certificato server.

Livello di ambito di ricerca Seleziona la profondità di ricerca nella directory LDAP, in *un livello* o *intero sottoalbero*. Spesso, *intero sottoalbero* è la scelta corretta.

DN di base dell'ambito della ricerca Il nome distinto su cui si baserà la ricerca. Per esempio DC=esempio,DC=com

Contenitori di autenticazione Questi valori specificano dove nella directory vengono trovati gli utenti. Per l'esempio, può essere CN=utenti;DC=esempio.

DN dell'utente associato a LDAP Il Nome distinto per un utente che può essere utilizzato per associarsi al server LDAP ed eseguire l'autenticazione. Se questo viene lasciato vuoto, verrà eseguita un'associazione anonima e l'impostazione della password di seguito verrà ignorata.

Password per l'associazione LDAP La password da utilizzare con il DN dell'utente associato a LDAP.

Attributo di denominazione dell'utente Varia a seconda del software e della struttura della directory LDAP. Tipicamente è cn per OpenLDAP e Novell eDirectory e samNomeAccount per la Directory attiva di Microsoft.

Attributo di denominazione del gruppo Varia a seconda del software e della struttura della directory LDAP, ma è in genere cn.

Attributo di denominazione dei membri Varia a seconda del software e della struttura della directory LDAP. Tipicamente membro su OpenLDAP, membroDi per la Directory attiva di Microsoft e unicoMembro su novell eDirectory.

Scelta di un server RADIUS

Se sul firewall Firew4LL è definito un server RADIUS esistente, selezionarlo dall'elenco. Per utilizzare un server RADIUS diverso, scegliere **Aggiungere un nuovo server RADIUS**. Se su Firew4LL non sono definiti server RADIUS, questo passaggio viene saltato.

Aggiunta di un server RADIUS

Se non esistono server RADIUS o è stato selezionato **Aggiungere un nuovo server RADIUS**, viene visualizzata una schermata con le opzioni necessarie per aggiungere un nuovo server. In caso di incertezza sulle impostazioni, consultare l'amministratore del server RADIUS, il fornitore del software o la documentazione.

Nota:

I dettagli dei server RADIUS sono coperti in *Server di autenticazione*. Alcuni dettagli sono omessi qui poiché le opzioni sono discusse in modo approfondito altrove. Per ulteriori informazioni sulle opzioni elencate in questa sezione, fare riferimento lì.

Nome Nome descrittivo per questo server RADIUS, per riferimento.

Hostname o indirizzo IP L'hostname o indirizzo IP del server RADIUS.

Porta di autenticazione Porta utilizzata dal server RADIUS per accettare le richieste di autenticazione, in genere è 1812.

Segreto condiviso Il **Segreto condiviso** è la password configurata sul server RADIUS per accettare le richieste di autenticazione dall'indirizzo IP del firewall Firew4LL.

Scelta di un'autorità di certificazione

Se esiste un'autorità di certificazione esistente definita sul firewall Firew4LL, può essere scelta dall'elenco. Per creare una nuova autorità di certificazione, scegliere **Aggiungere una nuova CA**. Se non sono definite autorità di Certificazione, questo passaggio viene saltato.

Creazione di un'autorità di certificazione

Questo passaggio presenta tutti i campi necessari per creare una nuova autorità di certificazione (CA). Ogni opzione in questa pagina è necessaria e tutti i campi devono essere compilati correttamente per procedere. La CA viene utilizzata per stabilire una base di fiducia da cui i certificati del server possono essere generati e ritenuti "affidabili" dai client. Poiché questa CA è auto-generata, sarà attendibile solo dai client che vengono forniti anche con una copia di questo certificato CA.

Vedi anche:

Per ulteriori informazioni sulla creazione e la gestione di CA, vedere *Gestione delle autorità di certificazione*.

Nome descrittivo Un nome per riferimento per identificare questo certificato. Questo è lo stesso campo del Nome comune per altri certificati. Per questo esempio CA, viene utilizzato CAEsempioCo. Sebbene sia consentito l'utilizzo di spazi in questo campo, sconsigliamo vivamente l'utilizzo di spazi nel campo Nome comune perché alcuni client hanno problemi a gestirli correttamente.

Lunghezza della chiave Dimensione della chiave che verrà generata. Più grande è la chiave, maggiore è la sicurezza che offre, ma le chiavi più grandi sono generalmente più lente da usare. 2048 è una buona scelta.

Durata di vita Il tempo in giorni durante il quale questa CA sarà valida. Su una CA auto-generata come questa, è comunemente impostata su 3650, che è di circa 10 anni.

Codice del paese Codice del paese ISO a due lettere (ad esempio US, AU, CA). Se il codice del paese ISO a due lettere è sconosciuto, individuarlo sul sito della piattaforma di navigazione online ISO. Dal momento che l'azienda EsempioCo si trova negli Stati Uniti, inserire per questo esempio.

Stato o provincia Nome dello Stato o della Provincia completo e non abbreviato (ad esempio Texas, Indiana, California). EsempioCo si trova in Texas per questo esempio.

Città Città o altro nome di località (ad esempio Austin, Indianapolis, Toronto). La sede di EsempioCo è a Austin.

Organizzazione Nome dell'organizzazione, spesso il nome della società o del gruppo. EsempioCo va qui per questo esempio. **Non utilizzare caratteri speciali in questo campo, nemmeno la punteggiatura come un punto o una virgola**.

E-Mail Indirizzo e-Mail per il contatto del certificato. Spesso l'e-mail della persona che genera il certificato, come ad esempio vpnadmin@esempio.com.

Fare clic su **Aggiungere una nuova CA** per completare il processo di creazione della CA

Scelta di un certificato server

Se è presente un certificato esistente definito sul firewall Firew4LL, può essere scelto dall'elenco. Per creare un nuovo certificato, scegliere **Aggiungere un nuovo certificato**. Se non vengono definiti Certificati, questo passaggio viene saltato.

Aggiunta di un certificato server

Questa schermata crea un nuovo certificato server che verrà utilizzato per verificare l'identità del server ai client. Il certificato server verrà firmato dall'autorità di certificazione scelta o creata in precedenza nella procedura guidata. Nella maggior parte dei casi, come con questo esempio, vengono utilizzate le stesse informazioni del passaggio precedente e verranno pre-compilate automaticamente sul modulo.

Nome descrittivo Questo è il campo Nome comune (CN) per il certificato server e viene utilizzato anche per fare riferimento al certificato in Firew4LL. L'utilizzo del hostname del firewall è una scelta comune per un certificato server, ad esempio vpn.esempio.com. Sebbene sia consentito l'utilizzo di spazi in questo campo, sconsigliamo vivamente l'utilizzo di spazi in un campo Nome comune perché i client tendono ad avere problemi a gestirli correttamente

L**unghezza chiave** Dimensione della chiave che verrà generata. Più grande è la chiave, maggiore è la sicurezza che offre, ma le chiavi più grandi sono generalmente più lente da usare. 2048 è una buona scelta.

Durata di vita Durata di vita in giorni. Questa è comunemente impostato su 3650 (circa 10 anni).

Codice del paese Codice del paese ISO a due lettere (ad es.)

Stato o provincia Nome dello Stato o della Provincia completo e non abbreviato (ad esempio Texas, Indiana, Ontario).

Città Città o altro nome di località (ad esempio Austin, Indianapolis, Toronto).

Organizzazione Nome dell'organizzazione, spesso il nome della società o del gruppo. **Non utilizzare caratteri speciali in questo campo, nemmeno la punteggiatura come un punto o una virgola**.

E-Mail Indirizzo e-Mail per il contatto del certificato. Spesso l'e-mail della persona che genera il certificato (ad esempio vpnadmin@esempio.com)

Fare clic su **Creare un nuovo certificato** per memorizzare le impostazioni e continuare con la fase successiva della procedura guidata.

Configurazione delle impostazioni del server OpenVPN

Le opzioni di questo passaggio della procedura guidata configurano ogni aspetto di come si comporterà il server OpenVPN e le opzioni che vengono trasmesse ai client. Le opzioni presentate qui sono le stesse discusse in precedenza nelle *opzioni di configurazione OpenVPN*, fare riferimento a tale sezione per i dettagli. Poiché le opzioni sono trattate in dettaglio in quella sezione, verranno menzionate solo le impostazioni per questo esempio.

Informazioni generali sul server OpenVPN

Queste opzioni controllano il funzionamento dell'istanza OpenVPN.

Interfaccia Poiché le connessioni in entrata saranno dal lato WAN, selezionare *WAN*.

Protocollo L'impostazione predefinita di *UDP* è accettabile.

Porta locale Questa sarà la prima istanza del server OpenVPN, quindi è preferibile l'impostazione predefinita di 1194. Se c'è una OpenVPN esistente su quella porta, utilizzare un numero di porta diverso. La procedura guidata suggerirà un numero di porta inutilizzato.

Descrizione Siccome questo sarà per l'accesso remoto dell'utente, Client VPN Mobile EsempioCo è una descrizione adatta.

Impostazioni crittografiche

Queste opzioni controllano il modo in cui il traffico nel tunnel viene crittografato e autenticato.

Autenticazione TLS TLS è altamente desiderabile, quindi selezionare **Abilitare l'autenticazione dei pacchetti TLS**.

Generare chiave TLS Non esiste una chiave TLS esistente, quindi selezionare **Generare automaticamente una chiave di autenticazione TLS condivisa**.

Chiave condivisa TLS Poiché non esiste una chiave TLS esistente, lasciare vuoto.

Lunghezza dei parametri Selezionare quanto è un buon equilibrio di velocità e forza.

Algoritmo di crittografia Questo può essere lasciato al valore predefinito di *AES-128-CBC*, ma anche qualsiasi altra opzione funzionerebbe fino a quando i client sono impostati in modo da corrispondere.

Algoritmo digest d autenticazione Lasciare al *SHA1 (160-bit)* predefinito

Crittografia dell'hardware Il dispositivo di destinazione non ha acceleratore, quindi lasciare settato su *Nessun acceleratore della crittografia dell'hardware*

Impostazioni del tunnel

Queste opzioni controllano come verrà instradato il traffico proveniente dai client remoti.

Rete del tunnel Come nel diagramma all'inizio di questo esempio, la sottorete 10.3.201.0/24 è stata scelta per i client VPN.

Gateway per il reindirizzamento Per l'"installazione di EsempioCo, la VPN trasporterà solo traffico destinato alle sottoreti presso l'ufficio principale, quindi questa casella *non è selezionata*.

Rete locale Questa è la sottorete principale dell'ufficio, che in questo esempio è 10.3.0.0/24.

Connessioni simultanee EsempioCo non vuole limitare il numero di client che possono connettersi contemporaneamente, quindi questo viene lasciato vuoto.

Compressione Per migliorare il throughput del traffico sul tunnel VPN a scapito di una certa potenza della CPU, questo è impostato su *abilitato con compressione adattiva*.

Tipo di servizio Questa casella è deselezionata, in quanto non vi è traffico su questa VPN che richiede priorità/QoS.

Comunicazione tra client Poiché i client di questa VPN non hanno bisogno di connettersi ad altre macchine client, questa casella è deselezionata.

Duplicare le connessioni Poiché esistono certificati univoci per ogni client, questo è deselezionato.

Impostazioni del client

Queste opzioni controllano le impostazioni specifiche fornite ai client quando viene stabilita una connessione.

IP dinamico I client si connetteranno da tutto il paese e le reti mobili sconosciute e i loro indirizzi IP potrebbero cambiare senza preavviso, quindi questa opzione è selezionata.

Pool di indirizzi Ai client verranno assegnati indirizzi dalla rete tunnel di sopra, quindi questa casella è selezionata.

Topologia Il metodo utilizzato per assegnare indirizzi IP ai client. Il valore predefinito della *Sottorete* è la scelta migliore.

Diminio predefinito del DNS Immettere il dominio per EsempioCo qui, esempio.com.

Server DNS Qualsiasi server DNS interno potrebbe essere utilizzato qui. EsempioCo ha il controllore della directory attiva di Windows che è configurato per agire come un server DNS, 10.3.0.5.

Server NTP Il server di sopra, 10.3.0.5, viene utilizzato anche per sincronizzare gli orologi PC del client.

Opzioni del NetBIOS I client avranno bisogno di accedere alle condivisioni di Windows dietro la VPN, quindi selezionare **Abilitare il NET-BIOS su TCP/IP**.

Tipo di nodo del NetBIOS Poiché il DNS viene utilizzato principalmente, selezionare *nodo-H*.

ID dell'ambito del NetBIOS Questo verrà lasciato vuoto, poiché l'ambito del NetBIOS non è limitato.

Server WINS WINS è stato deprecato, quindi questo è lasciato vuoto.

Avanzate In questo momento non sono necessari ulteriori ritocchi, quindi questo è lasciato vuoto.

Configurazione delle regole del firewall

Come per altre parti del firewall, per impostazione predefinita tutto il traffico è bloccato dalla connessione alle VPN o dal passaggio sul tunnel VPN. Questo passaggio della procedura guidata aggiunge automaticamente le regole del firewall per consentire al traffico di connettersi alla VPN e anche i client connessi possono far passare il traffico sulla VPN.

Traffico da client a server

Selezionare questa casella per aggiungere una regola firewall sull'interfaccia scelta per il tunnel (ad esempio *WAN*) che consente ai client di connettersi. Consente a tutti i client di qualsiasi indirizzo sorgente di connettersi per impostazione predefinita. Per consentire connessioni da un set limitato di indirizzi IP o sottoreti, creare una regola personalizzata o selezionare questa casella e modificare la regola che crea. Poiché in questo esempio i client si connettono da tutto il paese, la regola creata da questa casella di controllo è l'ideale, quindi la casella è selezionata.

Traffico dai client attraverso il tunnel VPN

Questa impostazione consente a tutto il traffico di attraversare il tunnel OpenVPN, che è desiderabile per questo esempio, quindi questa casella è selezionata.

Completamento della procedura guidata

Fare clic su **Finire** e la procedura guidata è ora completa; il tunnel è completamente configurato e pronto per le connessioni dei client. Da qui i passi successivi saranno quelli per aggiungere utenti e configurare i dispositivi client. Se sono necessarie modifiche alle regole del firewall generate automaticamente, bisogna farlo ora.

18.2.4 Configurazione degli utenti

A questo punto il server VPN è configurato ma potrebbe non esserci alcun client che possa connettersi. Il metodo per aggiungere utenti alla VPN dipenderà dal metodo di autenticazione scelto durante la creazione del server OpenVPN.

Vedi anche:

Maggiori dettagli sull'aggiunta di utenti possono essere trovati in *Gestione e autenticazione degli utenti*. Maggiori informazioni sulla gestione dei certificati utente possono essere trovate in *Certificati utente*.

Utenti locali

Per aggiungere un utente che può connettersi a OpenVPN, devono essere aggiunti alla Gestione utente come segue:

- Passare a **Sistema>Gestione utenti**
- Fare clic su  **Aggiungere** per creare un nuovo utente
- Inserire un **Nome utente**, una **Password** e confermare la password
- Compilare il **Nome completo** (opzionale)
- Selezionare **Fare clic per creare un certificato utente**, che aprirà il pannello delle opzioni del certificato
- Inserire il nome dell'utente o altre informazioni pertinenti nel campo **Nome descrittivo**
- Scegliere la stessa **Autorità di certificazione** utilizzata sul server OpenVPN
- Scegliere una **Lunghezza della chiave** (può essere lasciato su default)
- Inserire una **Durata di vita** (può essere lasciato su default)
- Fare clic su **Salvare**

  Per visualizzare o modificare l'utente:

- Passare a **Sistema>Gestione utenti**
- Fare clic su  accanto alla riga contenente l'utente per vedere/modificare

Per esportare il certificato e la chiave di un utente:

Nota: questa parte può essere saltata se si utilizza il pacchetto di esportazione del client di OpenVPN, descritto in *Pacchetto di esportazione del client di OpenVPN*. Il pacchetto di esportazione del client è un modo molto più semplice per scaricare configurazioni del client e il file di installazione.

- Passare **a Sistema>Gestione utenti** nella scheda **Certificati**
- Individuare il certificato utente nell'elenco
- Fare clic su  per scaricare i certificati utente
- Fare clic su  per scaricare la chiave per il certificato
- **Fare clic su**  **per scaricare un pacchetto PKCS#12 che include** il certificato utente e la chiave e il certificato CA (opzionale).

Nella maggior parte dei casi, il certificato CA deve essere scaricato anche con il certificato utente. Questo può essere fatto dalla sua voce su **Sistema>Gestione utenti**, scheda **CA** o utilizzando il pacchetto PKCS#12 menzionato in precedenza.

Utenti LDAP o RADIUS

L'aggiunta di utenti LDAP e RADIUS dipenderà completamente dagli strumenti di implementazione e gestione del server, che vanno oltre lo scopo di questo libro. Contattare l'amministratore del server o il fornitore del software per l'assistenza. I certificati per gli utenti LDAP o RADIUS non possono essere creati dall'interfaccia web del firewall in modo da riflettere una relazione del certificato utente. Tuttavia, è possibile creare i certificati da soli utilizzando la gestione dei certificati come descritto nei *Certificati utente*

18.2.5 Installazione del client di OpenVPN

Pacchetto di esportazione del client di OpenVPN

Il modo più semplice per configurare un client OpenVPN sulla maggior parte delle piattaforme è utilizzare il pacchetto di esportazione del client OpenVPN sul firewall Firew4LL.

Installare il pacchetto di utilità di esportazione del client OpenVPN come segue:

- Passare a **Sistema>Pacchetti**
- **Individuare il Pacchetto di esportazione del client OpenVPN** nell'elenco
- **Fare clic su** **Installare accanto all'elenco di pacchetti** da installare

Una volta installato, può essere trovato in **VPN>OpenVPN**, nella scheda **Esportazione del client**.

Le opzioni per il pacchetto includono:

Server di accesso remoto Selezionare l'istanza del server OpenVPN per la quale verrà esportato un client. Se c'è solo un server di accesso remoto OpenVPN ci sarà solo una scelta nella lista. L'elenco sarà vuoto se non ci sono server OpenVPN in modalità di accesso remoto.

Risoluzione del hostname Controlla come viene formattata la voce "remoto" del client.

Indirizzo IP dell'interfaccia Quando viene scelto, l'indirizzo IP dell'interfaccia viene utilizzato direttamente. Questa è la scelta migliore per le installazioni con un indirizzo IP statico sulla WAN

IP automatico delle Multi-WAN Questa opzione è utile quando si reindirizzano più porte utilizzando la porta forward per le distribuzioni che utilizzano Multi-WAN o più porte sulla stessa WAN. Cercherà e farà voci per tutte le porte forward che mirano al server e utilizzerà l'indirizzo IP di destinazione utilizzato sulla porta forward nella configurazione del client.

Nomi host automatici di DDNS per le Multi-WAN Simile all'opzione precedente, ma utilizza la prima voce DNS dinamica che trova corrispondente alla destinazione scelta.

Hostname di installazione Inserisce l'hostname del firewall, definito in **Sistema>Configurazione generale**, nella configurazione del client. L'hostname deve esistere nel DNS pubblico in modo che possa essere risolto dai client.

Voci del hostname del DNS dinamico Ogni hostname del DNS dinamico configurato sul firewall è elencato qui. Questi sono in genere la scelta migliore per l'esecuzione di un server su una singola WAN con un indirizzo IP dinamico.

Altro Presenta una casella di testo in cui è possibile inserire un hostname o un indirizzo IP per il client da utilizzare.

CN del server per la verifica Specifica come il client verificherà l'identità del certificato del server. Il CN del certificato del server viene inserito nella configurazione client, in modo che se un altro certificato valido finge di essere il server con un CN diverso, non corrisponderà e il client rifiuterà di connettersi.

Automatico – Usare verify-509-name dove possibile Questa è la migliore scelta per i client attuali. I metodi più vecchi sono stati deprecati poiché questo metodo è più accurato e flessibile.

Utilizzare TLS remoto Questo può funzionare su client più vecchi (OpenVPN 2.2.x o precedente) ma interromperà i client più recenti poiché l'opzione è stata deprecata.

Utilizzare TLS remoto e citare il server CN Funziona allo stesso modo di TLS-remoto ma aggiunge citazioni in tutto il CN per aiutare alcuni client a far fronte agli spazi nel CN.

Non verificare il server CN Disabilita la verifica client del nome comune del certificato server.

Utilizzare la porta locale casuale Per i client correnti, l'impostazione predefinita (selezionata) è la migliore, altrimenti due connessioni OpenVPN non possono essere eseguite contemporaneamente sul dispositivo client. Alcuni client più anziani non la supportano, tuttavia.

Utilizzare l'archiviazione dei certificati di Microsoft In opzioni di esportazione dei certificati, per i client di installazione esportati verrà inserito il certificato CA e dell'utente nell'archiviazione dei certificati di Microsoft anziché utilizzare direttamente i file.

Utilizzare una password per proteggere il contenuto del file pkcs12 Quando è selezionato, inserire una password e confermarla, quindi i certificati e le chiavi fornite al client saranno protetti con una password. Se il server Open-VPN è configurato per l'autenticazione dell'utente, questo farà sì che gli utenti vedano due diversi prompt di password durante il caricamento del client: uno per decifrare le chiavi e i certificati e un altro per l'autenticazione dell'utente del server al momento della connessione.

Utilizzare il proxy Se il client si trova dietro un proxy, controllare *Usare il proxy per comunicare con il server* e quindi fornire un **tipo** di proxy**, indirizzo IP**, **porta** e **Autenticazione del proxy** con le credenziali, se necessario.

Gestione di OpenVPN Quando è selezionata, questa opzione raggrupperà il programma di installazione di Windows con la GUI della gestione di OpenVPN oltre al normale client di Windows. Questa GUI alternativa gestisce il servizio OpenVPN in modo tale da non richiedere privilegi a livello di amministratore una volta installato.

Opzioni di configurazione aggiuntive Ciascuna delle opzioni di configurazione aggiuntive necessarie per il client possono essere inserite in questa casella di immissione. Questa è approssimativamente equivalente alla casella **Opzioni avanzate** nelle schermate di configurazione di OpenVPN, ma dal punto di vista del client.

Nota: non esiste alcun meccanismo per salvare queste impostazioni, quindi devono essere controllate e impostate ogni volta che la pagina viene visitata.

Lista dei pacchetti di installazione del client

Sotto **Pacchetti di installazione del client** c'è un elenco di potenziali client da esportare. Il contenuto dell'elenco dipende da come viene configurato il server e da quali utenti e certificati sono presenti sul firewall.

L'elenco seguente descrive come lo stile di configurazione del server influisce sull'elenco nel pacchetto:

Accesso remoto (SSL/TLS) Sono elencati i certificati utente realizzati dalla stessa CA del server OpenVPN

Accesso remoto (SSL/TLS + Autenticazione utente – Utenti locali) Le voci utente di sono elencate per gli utenti locali che dispongono anche di un certificato associato realizzato dalla stessa CA del server OpenVPN.

Accesso remoto (SSL/TLS + Autenticazione utente – Autenticazione remota) Poiché gli utenti sono remoti, vengono elencati i certificati utente realizzati dalla stessa CA del server OpenVPN. Si presume che il nome utente sia lo stesso del nome comune del certificato.

Accesso remoto (Autenticazione utente - Utenti locali o Autenticazione remota) Viene visualizzata una singola voce di configurazione per tutti gli utenti poiché non ci sono certificati per utente.

L'impostazione dell'esempio dalla procedura guidata fatta in precedenza in questo capitolo era per SSL/TLS + Autenticazione utente con utenti locali, quindi viene mostrata una voce per utente sul sistema che ha un certificato creato dalla stessa CA del server OpenVPN.

Nota: se non vengono visualizzati utenti o se manca un utente specifico nell'elenco, l'utente non esiste o l'utente non dispone di un certificato appropriato. Vedere *Utenti locali* per la procedura

---

corretta per creare un utente e un certificato.

Tipi di pacchetto di installazione del client

Sono elencate numerose opzioni per ogni client che esporta la configurazione e i file associati in modi diversi. Ognuno può ospitare un diverso tipo di client potenziale.

Configurazioni standard

Archivio Scarica un archivio ZIP contenente il file di configurazione, la chiave TLS del server se definita e un file PKCS#12 contenente il certificato CA, la chiave client e il certificato client. Questa opzione è utilizzabile con i client Linux o Tunnelblick, tra gli altri.

Solo file Scarica solo il file di configurazione di base, senza certificati o chiavi. Questo sarebbe principalmente usato per vedere il file di configurazione stesso senza scaricare le altre informazioni.

Configurazioni in linea

Questa scelta scarica un singolo file di configurazione con i certificati e le chiavi in linea. Questo formato è ideale per l'uso su tutte le piattaforme, in particolare i client di Android e iOS o per copiare manualmente una configurazione su un sistema che ha già installato un client. Questa opzione funzionerà per qualsiasi tipo di client basato su OpenVPN versione 2.1 o successiva.

Android Utilizzato con il client OpenVPN di Android menzionato in *Android 4.x e versioni successive*.

OpenVPN Connect (iOS/Android) Utilizzato con il client di OpenVPN Connect su iOS o Android descritto in *iOS*.

Altri Utilizzabili da qualsiasi client OpenVPN standard su piattaforme come Windows, OS X o BSD/Linux. Funziona anche bene con Tunnelblick su OS X, è sufficiente scaricare la configurazione in linea e trascinarla nella cartella di configurazioni per Tunnelblick.

Archivio telefonico SIP

Se il server OpenVPN è configurato come SSL/TLS solo *senza* autenticazione, appariranno opzioni per esportare le configurazioni del client per diversi modelli di telefoni SIP che supportano OpenVPN. Esempi notevoli sono i

telefoni Yealink T28 e T38G e SNOM. L'installazione del client sul telefono varia in base al modello, controllare la documentazione del produttore per ulteriori informazioni.

Nota: Assicurarsi che il telefono abbia una corretta configurazione dell'orologio e/o server NTP, altrimenti i certificati non verranno convalidati e la VPN non si connetterà.

Avvertimento: In genere questi telefoni supportano solo l'uso di SHA1 come hash del certificato. Assicurarsi che i certificati CA, il certificato del server e client siano tutti generati utilizzando SHA1 o potrebbero non riuscire. Essi possono anche supportare solo un insieme limitato di algoritmi di crittografia come AES-128-CBC. Consultare la documentazione del telefono per i dettagli

Programma d'installazione di Windows

Le opzioni del programma di installazione di Windows creano un file di installazione eseguibile semplice da usare che contiene il client OpenVPN con i dati di configurazione incorporati. Il programma di installazione viene eseguito come il normale programma di installazione del client di OpenVPN di Windows, ma copia anche tutte le impostazioni e i certificati necessari. Vedere *Installazione di Windows* qui sotto per alcune note su come installare ed eseguire il client di Windows.

Attualmente, ci sono quattro opzioni disponibili:

x86-xp Programma di installazione a 32-bit utilizzabile su Windows XP e versioni successive

x64-xp Programma di installazione a 64-bit utilizzabile su Windows XP e versioni successive

x86-win6 Programma di installazione a 32-bit utilizzabile su Windows Vista e versioni successive e include un driver tap più recente

x64-win6 Programma di installazione a 64-bit utilizzabile su Windows Vista e versioni successive e include un driver tap più recente

Nota: Assicurarsi di fare clic su avanti/finire in fondo al processo

di installazione. Non fare clic su Annullare o X per uscire dall'installazione in qualsiasi fase, o il sistema client può essere lasciato con il client installato, ma nessuna configurazione importata

Pacchetto di viscosity

Questo funziona come l'archivio di configurazione di cui si è parlato sopra, ma per il client OpenVPN di viscosity è utilizzato in OS X e Windows. Se il client di viscosity è già installato, scaricare questo pacchetto e fare clic su di esso per importarlo nel client.

Avvertimento: in Windows Vista, 7, 8, 10 e versioni successive con UAC (Controllo dell'account dell'utente, User Account Control) abilitato, il client deve essere eseguito come amministratore. Cliccare con il tasto destro sull'icona della GUI di OpenVPN e fare clic su Eseguire come amministratore per farlo funzionare. Può connettersi senza diritti amministrativi, ma non può aggiungere il percorso necessario per dirigere il traffico sulla connessione OpenVPN, lasciandolo inutilizzabile. Le proprietà del collegamento possono essere impostate per avviare sempre il programma come Amministratore. Questa opzione si trova nella scheda Compatibilità delle proprietà di scelta

rapida. Un modo per aggirare questo requisito è controllare la gestione di OpenVPN prima di esportare per utilizzare una GUI di gestione OpenVPN alternativa su Windows. Il client di viscosity è disponibile anche per Windows e non richiede privilegi amministrativi per funzionare correttamente.

Installazione di Windows

Il progetto OpenVPN fornisce un programma di installazione per Windows 2000 tramite Windows 10, scaricabile dalla pagina di download della comunità OpenVPN. Al momento della stesura di questo articolo, la versione migliore per la maggior parte degli utenti Windows è il programma di installazione 2.4.x-i60x. La serie 2.4 è la versione stabile più attuale

L'installazione è semplice, accettare tutti i valori predefiniti. L'installazione creerà una nuova **connessione locale** sul sistema client per l'interfaccia *tun*. Questa interfaccia apparirà collegata quando viene stabilita la VPN e si mostrerà altrimenti come disconnessa. Nessuna configurazione di questa interfaccia è necessaria in quanto la sua configurazione verrà estratta dal server OpenVPN o dalla configurazione del client.

Avvertimento: In Windows Vista, 7, 8, 10 e versioni successive con UAC (Controllo dell'account dell'utente) abilitato, il client deve essere eseguito come amministratore. Fare clic con il tasto destro sull'icona della GUI di OpenVPN e fare clic su Eseguire come amministratore per farlo funzionare. Può connettersi senza diritti amministrativi, ma non può aggiungere il percorso necessario per dirigere il traffico sulla connessione OpenVPN, lasciandolo inutilizzabile. Le proprietà del collegamento possono essere impostate per avviare sempre il programma come amministratore. Questa opzione si trova nella scheda compatibilità delle proprietà di scelta rapida. Un modo per aggirare questo requisito è controllare la gestione di OpenVPN prima di esportare per utilizzare una GUI di gestione OpenVPN alternativa su Windows. Il client di viscosity è disponibile anche per Windows e non richiede privilegi amministrativi per funzionare correttamente.

Installazione Client Mac OS X

Opzioni client OpenVPN

- **Il client della riga di comando OpenVPN. La maggior parte degli** utenti preferisce un client grafico, quindi questa opzione non sarà coperta.
- **Tunnelblick, un'opzione gratuita disponibile per il download sul sito** Web di Tunnelblick.
- **Il client di viscosity commerciale. Al momento della stesura di** questo documento, costa $ 9 USD per un singolo posto. Se OpenVPN viene utilizzato frequentemente, viscosity rende un client molto più bello e vale il costo.

Sia Tunnelblick che viscosity sono facilmente installati, senza opzioni di configurazione durante l'installazione.

Installare viscosity

Quando si utilizza il client di viscosity, può essere configurato manualmente o il pacchetto di esportazione del client OpenVPN può essere utilizzato per importare la configurazione.

Nota: Viscosity fornisce uno strumento di configurazione della GUI che può essere utilizzato per generare la configurazione del client di OpenVPN sottostante. La CA e i certificati possono essere importati manualmente e tutti i parametri possono essere impostati manualmente.

Importazione configurazione di «Viscosity»

- Scaricare una copia del **pacchetto viscosity** per il client dal pacchetto di esportazione del client di OpenVPN
- Individuare il file salvato, che si concluderà in .visc.zip che indica che si tratta di un archivio compresso
- Copiare questo pacchetto esportato in una cartella sul Mac
- Fare doppio clic su questo file e si espanderà a viscosity.visc
- Fare doppio clic su **viscosity.visc** e viscosità aprirà e importerà la connessione come mostrato in figura *Importazione di viscosity*
-

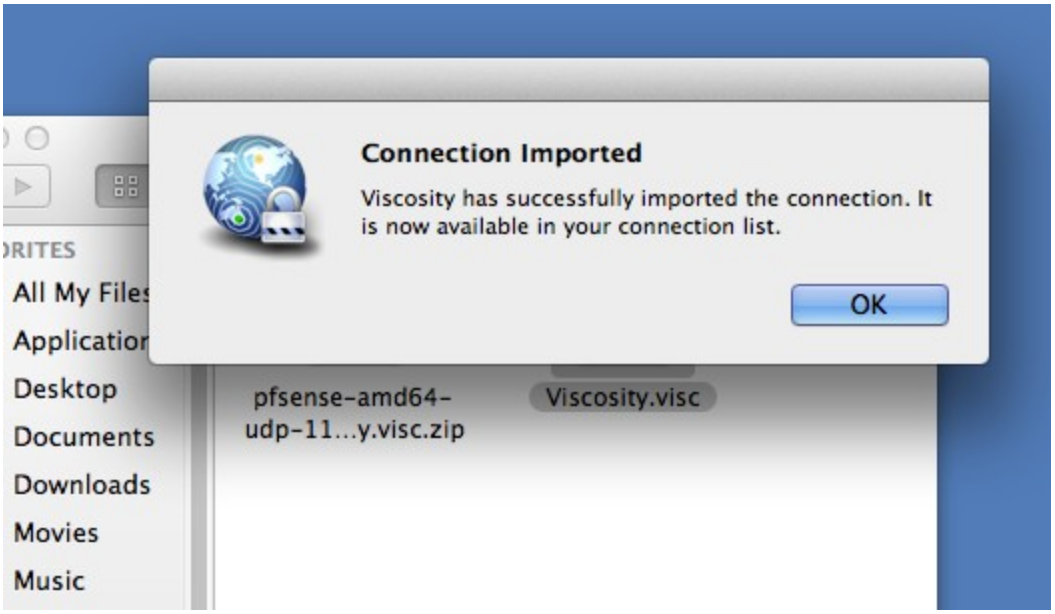


Fig. 2: Importazione di viscosity

- Eliminare la directory viscosity.visc e l'archivio .zip
- Viscosity sarà in esecuzione dopo l'importazione, e può essere trovato nella barra dei menu

Verificare importazione

- Fare clic sull'icona di blocco aggiunto alla barra dei menu nella parte superiore dello schermo
- Fare clic su **Preferenze** per verificare che la configurazione sia stata importata come mostrato in figura *Preferenze per viscosity*

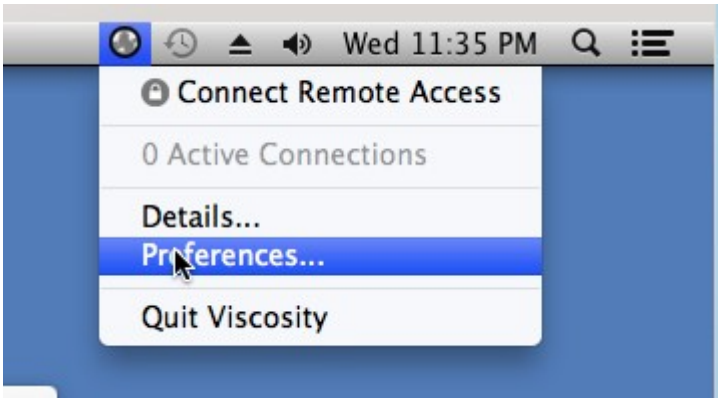


Fig. 3: Preferenze per viscosity

- Controllare l'area delle **connessioni** per verificare se la connessione è stata importata correttamente, come mostrato in figura *Connessioni viste da viscosity*.
- Chiudere la schermata Preferenze

Collegati alla VPN

- Fare clic sull'icona lucchetto nella barra dei menu
- Fare clic sul nome della connessione VPN per connettersi come mostrato in figura *Collegare viscosity*. Dopo alcuni secondi, il blocco nella barra dei menu diventerà verde per mostrarlo collegato correttamente.

Controlla dettagli connesione

- Fare clic sull'icona lucchetto nella barra dei menu
- Fare clic su **Dettagli** come mostrato nella figura *Menu di viscosity* per vedere le informazioni di connessione

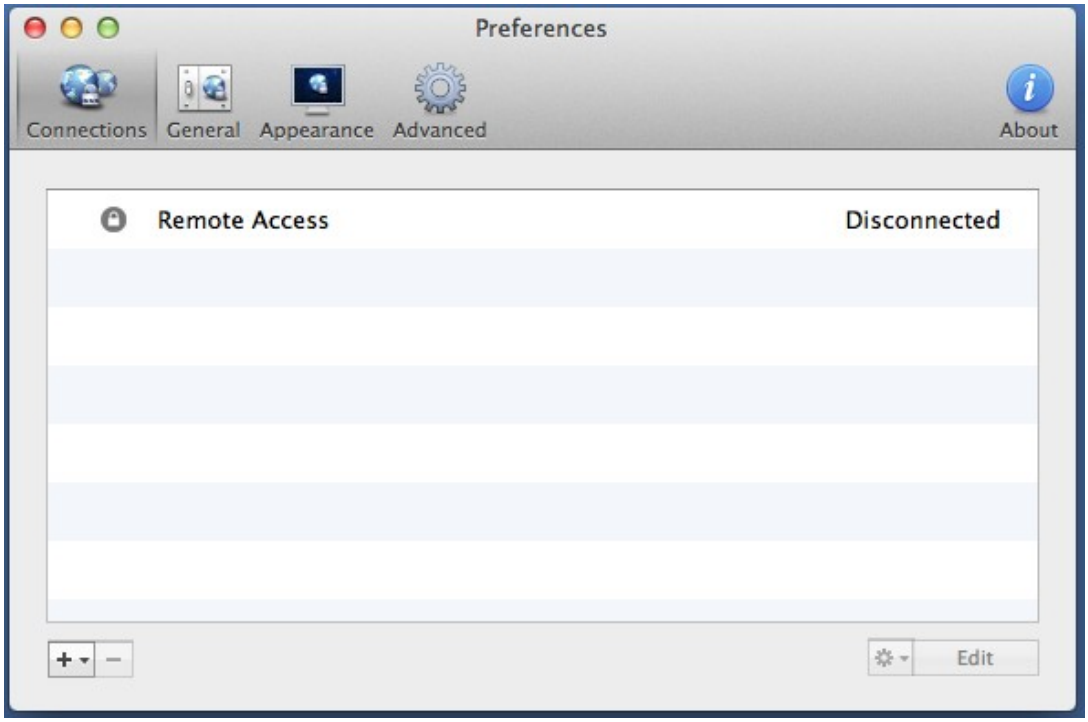


Fig. 4: Connessioni viste da viscosity

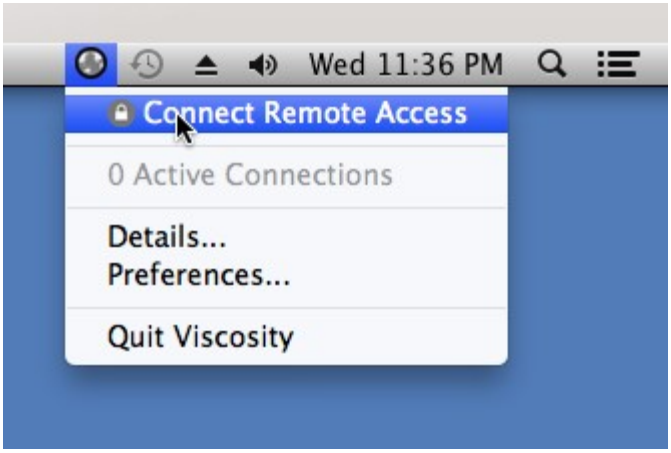


Fig. 5: Collegare viscosity

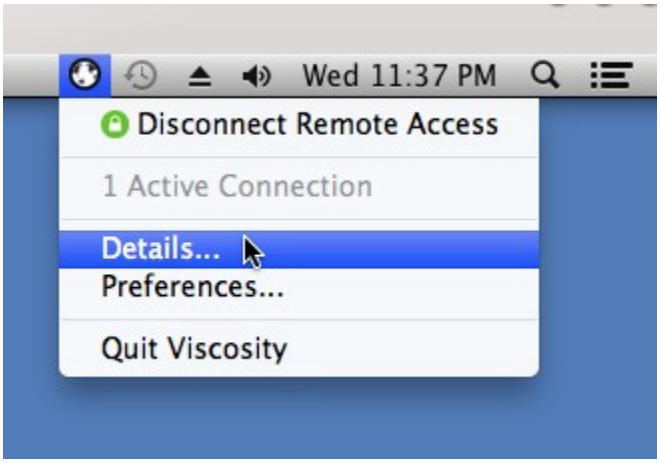


Fig. 6: Menu di viscosity

Nella prima schermata (figura *Dettagli di viscosity*), vengono visualizzati lo stato della connessione, l'ora della connessione, l'IP assegnato al client e l'IP del server. Un grafico della larghezza di banda viene visualizzato nella parte inferiore dello schermo, mostrando il throughput in entrata e in uscita dell'interfaccia OpenVPN.

Facendo clic sulle frecce Su/Giù al centro della schermata dei dettagli vengono visualizzate ulteriori statistiche sul traffico di rete. Questo mostra il traffico inviato all'interno del tunnel (TUN/TAP in entrata e in uscita), così come il traffico TCP o UDP totale inviato compreso il sovraccarico del tunnel e la crittografia. Per le connessioni che utilizzano principalmente pacchetti di piccole dimensioni, il sovraccarico è considerevole con tutte le soluzioni VPN. Le statistiche mostrate in figura *Dettagli di viscosity: statistiche del traffico* provengono solo dai pochi ping che attraversano la connessione. Anche il traffico inviato a far apparire la connessione viene conteggiato, quindi il sovraccarico iniziale è superiore a quello che sarà dopo essere stato collegato per qualche tempo. Inoltre, il tipico traffico VPN avrà le dimensioni dei pacchetti più grandi di pimg di 64 byte, rendendo il sovraccarico totale e la differenza tra questi due numeri notevolmente inferiore.

Cliccando sulla terza icona al centro della schermata **Dettagli si** visualizza il file di registro OpenVPN (figura *Dettagli di viscosity: registri*). Se c'è qualche problema di connessione, rivedere i registri qui per aiutare a determinare il problema. Vedere anche *Risoluzione dei problemi di OpenVPN*.

Client iOS e installazione

iOS è anche in grado di eseguire OpenVPN in modo nativo utilizzando il client di OpenVPN Connect per iOS disponibile in App Store. Questa applicazione non richiede il jailbreaking del dispositivo iOS. L'applicazione deve avere il file di configurazione e i certificati configurati al di fuori del dispositivo iOS e poi importati ad esso. Il pacchetto di esportazione del client di OpenVPN su Firew4LL può essere utilizzato per esportare una **configurazione in linea** di tipo **OpenVPN Connect**. Trasferire il risultante file .ovpn al dispositivo di destinazione quindi utilizzando iTunes per trasferire i file itramite app o e-mail al dispositivo.

Utilizzare altri metodi per ottenere i file sul dispositivo in remoto, come Dropbox, Google Drive, O Box funzionerà in modo simile all'utilizzo della e-mail inoltre è generalmente più sicuro in quanto i contenuti rimarranno privati e, eventualmente, crittografati a seconda del metodo e la memorizzazione.

Se si utilizza il metodo delle e-mail, utilizzare la seguente procedura:

- **Esportare il file di configurazione in linea del tipo di OpenVPN connect** per la VPN.
- **Inviare il file esportato in una e-mail a un account configurato sul** dispositivo iOS
- Installare l'App OpenVPN Connect sul dispositivo
- Aprire l'applicazione per le mail sul dispositivo

- Aprire il messaggio di posta elettronica contenente l'allegato

Fig. 7: Dettagli di viscosity

- Toccare l'allegato. Quando viene toccato una delle scelte sarà quello di aprirlo con l'applicazione OpenVPN Connect
- Toccare per selezionare l'App OpenVPN connect e verrà offerto di importare la configurazione
- Toccare il pulsante + e il profilo verrà importato

  L'utilizzo di iTunes per trasferire la configurazione sul dispositivo iOS è semplice e più sicuro dell'e-mail.

- Esportare il file di **configurazione in linea** del tipo di **OpenVPN connect** per la VPN.
- Collegare il dispositivo iOS al computer e aprire iTunes
- Trovare e installare l'App OpenVPN Connect
- Fare clic sull'icona del dispositivo all'interno di iTunes nella barra degli strumenti
- Selezionare le App sul lato sinistro della finestra
- Individuare la sezione Condivisione dei file nella parte inferiore di questa schermata (scorrere verso il basso)
- Fare clic sull'icona per OpenVPN in **Condivisione dei file** e un elenco di file verrà visualizzato a destra sotto la voce **Documenti di OpenVPN**
- Copiare il file sul dispositivo utilizzando uno dei seguenti metodi. Il file sarà immediatamente disponibile sul dispositivo iOS.
  - Utilizzare Finder per trascinare e rilasciare il file *.ovpn* in quest'area – OPPURE –
  - Fare clic su **Aggiungere** e individuare il file da importare
- Aprire l'applicazione OpenVPN Connect e verrà offerto di importare il profilo

- Toccare il pulsante + e il profilo verrà importato

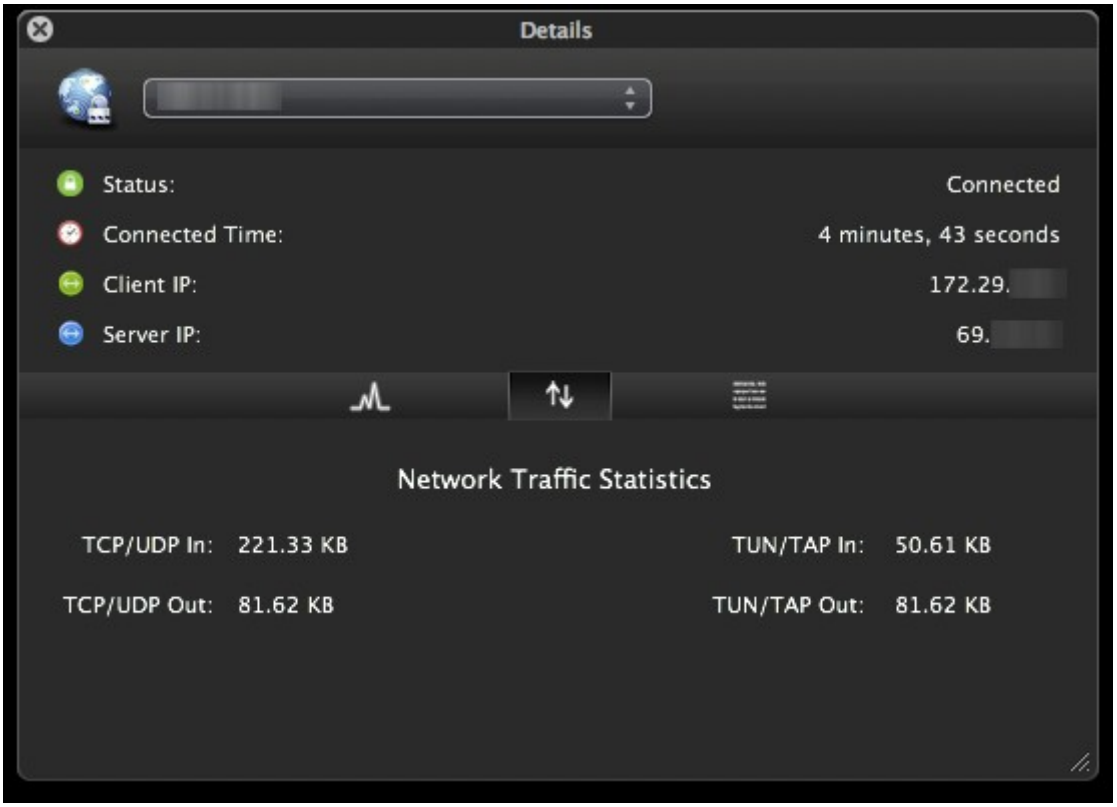


Fig. 8: Dettagli di viscosity: statistiche del traffico

Se il profilo è configurato per l'autenticazione dell'utente verrà richiesto per le credenziali, che possono facoltativamente essere salvate. Sotto il prompt delle credenziali c'è uno stato di connessione che cambierà tra disconnesso e connesso e indica anche quando si tenta una connessione. Facendo clic su di questo si aprirà il registro dei client di OpenVPN che è molto utile se si riscontrano problemi di connessione.

Per collegare la VPN, spostare il cursore nella parte inferiore del profilo da **Off** a **On** e l'applicazione tenterà di connettersi. Per scollegare manualmente, spostare il cursore su **Off**.

Quando si crea manualmente un file di configurazione per questo client, è necessario uno stile di configurazione in linea o file di CA, certificato del client, chiave del certificato del client e chiave TLS separati (se utilizzati). Non compare di accettare i file *.p12* contenenti il certificato/chiavi CA e client, quindi lo stile predefinito "archivio di configurazione » non funzionerà, anche se alcuni utenti hanno segnalato il funzionamento importando i file di configurazione estratti dal pacchetto di viscosity.

Client Android e installazioni

Per i dispositivi che eseguono Android 4.0 o una versione più recente, c'è un'app OpenVPN gratuita nel Play store di Google che funziona in modo eccellente senza bisogno di accesso dalla root. Si chiama OpenVPN per Android di Arne Schwabe.

> Il pacchetto di esportazione del client di OpenVPN su Firew4LL può esportare una **configurazione in linea** di tipo **Android** e il file .ovpn può essere trasferito al dispositivo di destinazione. Può essere copiato direttamente, via e-mail al dispositivo, ecc.

- Aprire l'app **OpenVPN per Android**
- Toccare Importare (icona della cartella file in alto a destra)

- Trovare il file .ovpn salvato sopra e toccarlo
- Toccare Importare (icona disco in alto a destra)

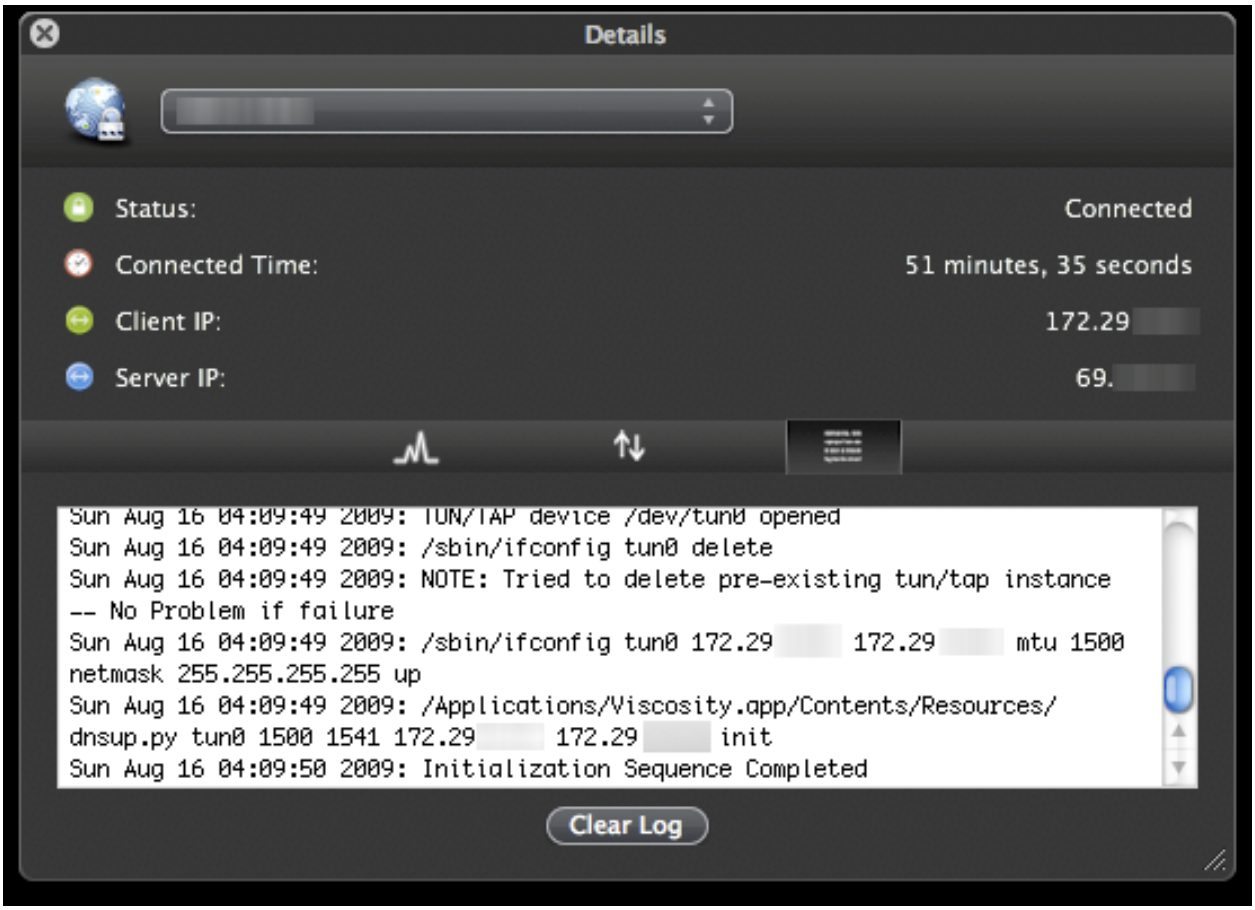


Fig. 9: Dettagli di viscosity: registri

La VPN importata viene ora mostrata nell'elenco. Modificare la voce per modificare il nome e altri dettagli. Toccare la VPN per connettersi. Se il profilo è configurato per l'autenticazione dell'utente, l'app richiederà credenziali durante la connessione.

Nota: Il client di OpenVPN Connect per Android funziona anche su Android 4.x e non richiede la root. Funziona in modo identico al client di iOS con lo stesso nome. Manca la possibilità di configurare completamente la VPN nella GUI, quindi non è raccomandato. Utilizzare l'esportazione della **Configurazione in linea** del tipo di **OpenVPN Connect** per l'utilizzo con quel client sia su Android che su iOS.

Client FreeBSD e Installazione

Se il client ha un'installazione di FreeBSD pronta, OpenVPN può essere trovato tra i suoi ports. Per installare OpenVPN, eseguire quanto segue dalla **root**:

```
# cd /usr/ports/security/openvpn && make install clean
```

In alternativa, può essere installato dai pacchetti:

```
# pkg install openvpn
```

Client Linux e Installazione

L'installazione di OpenVPN su Linux varierà a seconda della distribuzione preferita e del metodo di gestione delle installazioni software. OpenVPN è incluso nelle repository dei pacchetti della maggior parte delle principali distribuzioni Linux. Con tutte le varie possibilità tra le innumerevoli distribuzioni e le informazioni adeguate già disponibili in altre fonti online, questo libro non coprirà alcuna specificità. Basta cercare su Internet la distribuzione di scelta e "installare OpenVPN" per trovare informazioni.

Le distribuzioni basate su Ubuntu hanno una gestione OpenVPN integrata con la Gestione di rete, ma richiede l'installazione di un modulo aggiuntivo con il seguente comando:

```
apt install openvpn-server
```

Configurazione manuale del client

L'esecuzione di un'installazione del client manuale invece di utilizzare il pacchetto di esportazione del client di OpenVPN richiede ulteriori passaggi per installare il software e le impostazioni sui PC client. L'installazione del client su altri sistemi operativi viene lasciata al lettore.

Dopo aver installato OpenVPN, copiare i certificati nel client e creare il file di configurazione del client.

Copiare I certificati

Per ogni client sono necessari tre file dal firewall: il certificato CA, il certificato client e la chiave client. Un quarto file, la chiave TLS, è richiesto solo se il server è stato configurato per l'autenticazione TLS.

- Esportare il certificato CA da **Certificazione del sistema>Gestione** nella scheda **CA**, salvalo come ca.crt
- Esportare il certificato del client e la chiave come descritto in *utenti locali*, salvarli come nome utente.crt e nomeutente.chiave
- Copiare questi file nella directory di configurazione di OpenVPN sul client
- Copiare la chiave TLS dalla schermata di configurazione del server se l'autenticazione TLS viene utilizzata su questo server OpenVPN. Salvare questo in un nuovo file di testo chiamato tls.chiave e includerlo anche nella cartella di config.

Creare la configurazione

Dopo aver copiato i certificati nel client, è necessario creare il file di configurazione del client di OpenVPN. Questo può essere fatto con qualsiasi editor di file di testo normale come Blocco note su Windows. Quanto segue mostra le opzioni più utilizzate:

client dev tun proto udp remote vpn.example.com 1194 ping 10 resolv-retry infinite nobind persist-key persist-tun ca ca.crt cert username.crt key username.key verb 3 comp-lzo tls-auth tls.key 1 auth-user-pass

> **remote** Specifica l'host e la porta del server OpenVPN remoto. Qui è possibile specificare un indirizzo IP o FQDN. **proto** Specifica il protocollo utilizzato dalla connessione OpenVPN. Cambiare questa riga in proto tcp se TCP viene utilizzato sul server di OpenVPN **CA, cert, key** Deve essere modificato di conseguenza per ogni client per riflettere i nomi dei file salvati in precedenza. **tls-auth** Se l'autenticazione TLS non viene utilizzata, la riga TLS-auth può essere omessa. **auth-user-pass Se la VPN di accesso remoto non include l'autenticazione con nome utente e password, omettere questa riga.

Vedi anche:

Per un riferimento più completo alle direttive OpenVPN, fare riferimento al manuale OpenVPN per la versione del client installata

Distribuzione di configurazione e chiavi aii client

Il modo più semplice per distribuire le chiavi e la configurazione OpenVPN ai client è tramite il pacchetto di esportazione del client di OpenVPN. Se quel pacchetto non è una scelta valida, posizionare i file necessari in un archivio ZIP o in un archivio autoestraente che estrae automaticamente `C:\Program Files\OpenVPN\config`. Questo deve essere trasmesso in modo sicuro per l'utente finale, e non deve mai essere passato su reti non attendibili in chiaro.

Un client di OpenVPN deve essere installato sulla maggior parte dei dispositivi dell'utente finale, poiché la funzionalità client non è ancora integrata nella maggior parte dei sistemi operativi. Questa sezione fornisce una panoramica dell'installazione su diversi sistemi operativi comuni.

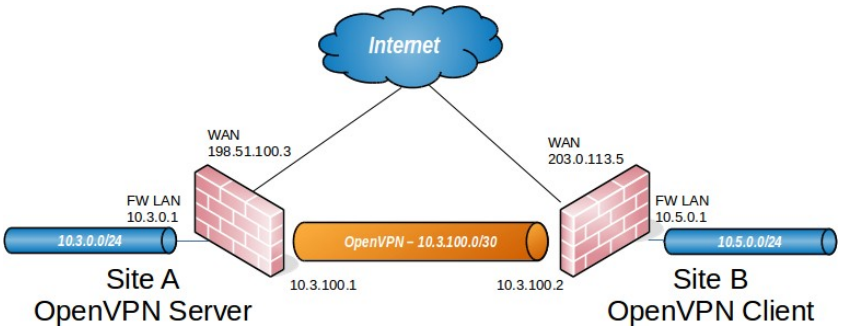


Fig. 10: Rete con esempio di sito-a-sito per OpenVPN

18.2.6 Esempio di sito-a-sito (Shared Key)

Questa sezione descrive il processo di configurazione di una connessione con sito-a-sito utilizzando un tunnel di OpenVPN in stile **Chiave condivisa**.

Quando si configura una connessione OpenVPN con sito-a-sito con chiave condivisa, un firewall sarà il server e l'altro sarà il client. Di solito la posizione principale sarà il lato server e gli uffici remoti fungeranno da client, anche se il contrario è funzionalmente equivalente. Come per una configurazione con accesso da remoto di OpenVPN ci sarà una sottorete dedicata in uso per l'interconnessione di OpenVPN tra le reti oltre alle sottoreti su entrambe le estremità. La configurazione di esempio qui descritta è raffigurata nella figura *Rete con esempio di sito-a-sito per OpenVPN*.

10.3.100.0 /30 viene utilizzato come **rete del tunnel**. Il tunnel di OpenVPN tra i due firewall ottiene un indirizzo IP su ciascuna estremità da quella sottorete, come illustrato nel diagramma. Le sezioni seguenti descrivono come configurare i lati server e client della connessione.

Configurazione lato server

- Passare a **VPN>OpenVPN**, scheda **Server**
- **Fare clic su** **Aggiungere per creare una nuova voce** server
- **Compilare i campi come segue, con tutto il resto lasciato sui valori**

  predefiniti:

Modalità del server Selezionare *Peer a Peer (chiave condivisa).*

Descrizione Inserire qui il testo per descrivere la connessione (ad esempio VPN del sito B per EsempioCo)

Chiave condivisa Selezionare **Generare automaticamente una chiave condivisa** o incollare una chiave condivisa preesistente per questa connessione.

Rete del tunnel Inserire la rete precedentemente scelta, 10.3.100.0/30

Rete remota Inserire la LAN sul lato del sito B, 10.5.0.0/24

- Fare clic su **Salvare**
- Fare clic su  per modificare il server che è stato creato un momento fa
- Trovare la casella della **Chiave condivisa**
- Selezionare tutto il testo all'interno della casella **Chiave condivisa**
- Copiare il testo negli appunti
- Salvare il contenuto in un file o incollarlo in un editor di testo come Blocco note

  Temporaneamente successivo, aggiungere una regola del firewall su WAN che consente l'accesso al server OpenVPN.
- Passare a **Firewall>Regole**, scheda **WAN**
- Fare clic su  **Aggiungere** per creare una nuova regola nella parte superiore dell'elenco
- Impostare il **Protocollo** su *UDP*
- Impostare l'indirizzo della sorgente in base al client. Se ha un indirizzo IP dinamico, lasciarlo impostato su *qualsiasi*, altrimenti impostare la regola per consentire solo dall'indirizzo IP della WAN del client:
  - Selezionare *Singolo host o Alias* in **Sorgente**
  - Inserire l'indirizzo WAN del client come **Indirizzo di sorgente** (ad esempio 203.0.113.5)
- Impostare la **destinazione** sull'"*indirizzo WAN*
- Impostare la **porta di destinazione** su questa istanza
- Immettere una **descrizione**, ad esempio OpenVPN dal sito B
- Fare clic su **Salvare** e la regola apparirà come la figura *Regola del firewall con l'esempio sito-a-sito di OpenVPN*.

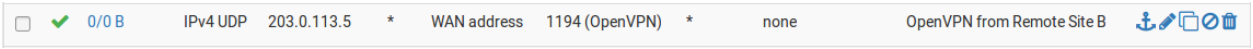


Fig. 11: Regola del firewall con l'esempio sito-a-sito di OpenVPN

- Fare clic su **Applicare le modifiche**

È necessario aggiungere una regola all'interfaccia **OpenVPN** per passare il traffico sulla VPN dalla LAN sul lato client alla LAN sul lato server. È possibile utilizzare una regola di stile «Consentire tutto» o un insieme di regole più severe. In questo esempio, consentire tutto il traffico è OK, quindi viene fatta la seguente regola:

- Passare a **Firewall>Regole**, scheda **OpenVPN**
- **Fare clic su**  **Aggiungere per creare una nuova regola** nella parte superiore dell'elenco
- Impostare il **Protocollo** su *qualsiasi*
- Immettere una **Descrizione** come Consentire tutto su OpenVPN
- Fare clic su **Salvare**

- Fare clic su **Applicare le modifiche**

La configurazione del server è terminata.

Configurazione lato client

- Passare a **VPN>OpenVPN**, scheda **Client** sul sistema del client
- **Fare clic su**  **Aggiungere per creare una nuova istanza** del client di OpenVPN
- **Compilare i campi come segue, con tutto il resto lasciato ai valori**

  predefiniti:

  Modalità del server *Selezionare Peer a Peer (chiave condivisa).*

  Host o indirizzo del server Immettere qui l'indirizzo IP pubblico o l'hostname del server OpenVPN (ad es. 198.51.100.3).

  Descrizione Inserire il testo per descrivere la connessione (ad esempio VPN del sito A di EsempioCo)

  Chiave condivisa Deselezionare **Generare automaticamente una chiave condivisa**, quindi incollare nella chiave condivisa per la connessione utilizzando la chiave copiata dall'istanza del server creata in precedenza.

  Rete del tunnel Deve corrispondere esattamente al lato server (ad esempio 10.3.100.0/30)

  Rete remota Inserire la rete LAN sul lato del sito A, 10.3.0.0/24

- Fare clic su **Salvare**

È inoltre necessario aggiungere una regola all'interfaccia OpenVPN per passare il traffico sulla VPN dalla LAN del lato server alla LAN del lato client. È possibile utilizzare una regola di stile «Consentire tutto» o un insieme di regole più severe. In questo esempio, consentire tutto il traffico è OK, quindi viene fatta la seguente regola:

- Passare a **Firewall>Regole**, scheda **OpenVPN**
- **Fare clic su**  **Aggiungere per creare una nuova regola** nella parte superiore dell'elenco
- Impostare il **Protocollo** su *qualsiasi*
- Immettere una **Descrizione** come Consentire tutto su OpenVPN
- Fare clic su **Salvare**
- Fare clic su **Applicare le modifiche**

La configurazione del client è completa. Non sono richieste regole del firewall sull'interfaccia WAN lato client perché il client avvia solo connessioni in uscita. Il server non avvia mai le connessioni per il client.

Nota: Con le configurazioni PKI di accesso remoto, in genere i percorsi e le altre opzioni di configurazione non sono definiti nella configurazione del client, ma vengono spinti dal server al client. Con le distribuzioni di chiavi condivise, i percorsi e altri parametri devono essere definiti su entrambe le estremità, se necessario (come descritto in precedenza e successivamente nelle *opzioni di configurazione personalizzate*), le opzioni non possono essere inviate dal server ai client quando si utilizzano chiavi condivise.

Provare la connessione

Il collegamento sarà immediatamente attivo al momento del salvataggio sul lato client. Provate a fare ping verso l'estremità remota per verificare la connettività. In caso di problemi, consultare la sezione Risoluzione dei problemi di OpenVPN.

18.2.7 Configurazione di esempio da sito a Sito (SSL/TLS)

Il processo di configurazione di una connessione con sito-a-sito utilizzando **SSL/TLS** è più complicato di quello con la **chiave condivisa**. Tuttavia, questo metodo è in genere molto più conveniente per la gestione di un gran numero di siti remoti che si collegano a un sito centrale in modo hub-and-spoke. Può essere utilizzato per un sito-a-sito tra due nodi, ma data la maggiore complessità della configurazione, la maggior parte delle persone preferisce utilizzare la chiave condivisa piuttosto che SSL/TLS per tale scenario.

Quando si configura una connessione OpenVPN con sito-a-sito utilizzando SSL/TLS, un firewall sarà il server e gli altri saranno i client. Di solito la posizione principale sarà il lato server e gli uffici remoti fungeranno da client, anche se una posizione ha un indirizzo IP statico e più larghezza di banda rispetto all'ufficio principale che potrebbe essere una posizione più desiderabile per il server. Oltre alle sottoreti su entrambe le estremità ci sarà una sottorete dedicata in uso per l'interconnessione di OpenVPN tra le reti. Questa configurazione di esempio è raffigurata nella figura *Rete con SSL/TLS con un esempio di sito-a-sito di OpenVPN*.

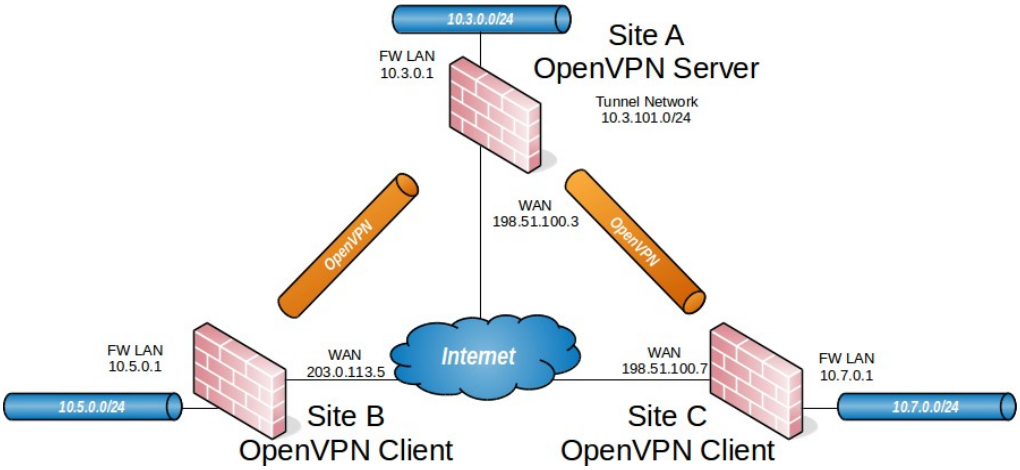


Fig. 12: Rete con SSL/TLS con un esempio di sito-a-sito di OpenVPN

10.3.101.0/24 viene utilizzato come rete del tunnel VPN con IPv4. Il modo in cui OpenVPN alloca gli indirizzi IP è lo stesso dei client di accesso remoto. Quando si utilizza uno stile di **topologia** di *sottorete*, ogni client otterrà un indirizzo IP in una sottorete comune. Quando si utilizza uno stile di **topologia** di *net30*, ogni client di connessione ottiene una sottorete /30 per interconnettersi con il server. Vedere *Topologia* per maggiori dettagli. Le sezioni seguenti descrivono come configurare i lati server e client della connessione. Qualsiasi sottorete può essere utilizzato per questo fino a quando non si sovrappone qualsiasi altra sottorete attualmente in uso sulla rete.

Affinché il server raggiunga le reti dei client dietro ogni connessione, sono necessari due elementi:

- Una *route* per dire al sistema operativo che OpenVPN conosce una rete remota
- Una *iroute* in un Override specifico del client che indica a OpenVPN come mappare la sottorete per un certificato specifico.

  Maggiori dettagli su questo argomento seguiranno nell'esempio.

Configurare il server con SSL/TLS

Prima che la VPN possa essere configurata, è necessaria una struttura del certificato per questa VPN. Creare una CA univoca per questa VPN e da tale CA creare un certificato server e quindi un certificato utente per ciascun sito remoto. Per i siti client, utilizzare un CN che li identifica in modo univoco in qualche modo, come il loro nome di dominio completo o un sito abbreviato o l'hostname. Per le specifiche di creazione di una CA e certificati, vedere *Gestione dei certificati*. Per questo esempio, la CA sarà chiamata S2SCA, il server CN sarà serverA, i client saranno clientB e clientC.

- Passare a **VPN>OpenVPN**, scheda **Server**
- Fare clic su  **Aggiungere** per creare un nuovo server
- Compilare i campi come descritto di seguito, con tutto il resto lasciato ai valori predefiniti. Queste opzioni sono discusse in dettaglio in precedenza in questo capitolo. Utilizzare i valori appropriati per questa rete o i valori predefiniti in caso di dubbi.

  Modalità del server Selezionare *Peer a Peer (SSL/TLS)* **Protocollo** Selezionare *UDP* **Modalità del dispositivo** Selezionare *tun* **Interfaccia** Selezionare *WAN* **Porta locale** Immettere meno che non ci sia un altro server OpenVPN attivo, nel qual caso utilizzare una porta diversa **Descrizione** Inserire qui il testo per descrivere la connessione **Autenticazione TLS** Seleziona questa casella per eseguire l'autenticazione TLS quanto quella SSL **Autorità di certificazione Peer** Selezionare la CA creata all'inizio di questo processo **Elenco delle revoche dei certificati dei peer** Se è stato creato un CRL, selezionalo qui **Certificato del server** Selezionare il certificato del server creato all'inizio di questo processo **Rete del tunnel IPv4** Inserire la rete del tunnel scelta, 10.3.101.0/24 **Rete locale IPv4** Inserire le reti LAN per tutti i siti, incluso il server: 10.3.0.0/24, 10.5.0.0/24, 10.7.0.0/24

Nota: Se ci sono più reti sul lato server che devono essere raggiunte dai client, come reti raggiungibili tramite percorsi statici, altre VPN e così via, aggiungerle come voci aggiuntive nella casella della rete locale con IPv4.

Rete remota IPv4 Inserire solo le reti LAN client: 10.5.0.0 / 24, 10.7.0.0 / 24

- Fare clic su Salvare
- Fare clic su  per modificare la nuova istanza del server
- Trovare la casella di **autenticazione TLS**
- Selezionare tutto il testo all'interno
- Copiare il testo negli appunti
- Salvare questo file o incollarlo in un editor di testo come Blocco note temporaneamente

  Successivamente, aggiungere una regola firewall su WAN che consente l'accesso al server di OpenVPN.
- Passare a **Firewall>Regole**, scheda **WAN**
- **Fare clic su**  **Aggiungere per creare una nuova regola** nella parte superiore dell'elenco
- Impostare il **protocollo** su *UDP*
- **Lasciare la sorgente impostata su *qualsiasi* poiché più siti** dovranno connettersi. In alternativa, è possibile creare un alias che contiene gli indirizzi IP di ciascun sito remoto se hanno indirizzi statici.
- Impostare la **destinazione** si *indirizzo WAN*
- Impostare la **porta di destinazione** su questa istanza

- Immettere una **descrizione**, ad esempio VPN per il multi-Sito di OpenVPN
- Fare clic su **Salvare**
- Fare click su **Applicare le modifiche**

È inoltre necessario aggiungere una regola all'interfaccia **OpenVPN** per passare il traffico sulla VPN dalla LAN del lato client alla LAN del lato server. È possibile utilizzare una regola di stile «Consentire tutto» o un insieme di regole più severe. In questo esempio, consentire tutto il traffico è OK, quindi viene fatta la seguente regola:

- Passare a **Firewall>Regole**, scheda **OpenVPN**
- Fare clic su  **Aggiungere** per creare una nuova regola nella parte superiore dell'elenco
- Impostare il **protocollo** su *qualsiasi*
- Inserie una **descrizione** come Consentire tutto su OpenVPN
- Fare click su **Salvare**
- Fare clic su **Applicare le modifiche**

  L'ultimo pezzo del puzzle è quello di **Aggiungere sostituzioni specifiche del client** per ogni sito client. Questi sono necessari per legare una sottorete del client a un particolare certificato per un sito in modo che possa essere instradato correttamente.
- Passare a **VPN>OpenVPN**, scheda **Sostituzioni specifiche del client**
- Fare clic su  per aggiungere una nuova sostituzione
- Compilare i campi in questa schermata come segue:

  Nome comune Immettere la CN del primo sito client. In questo esempio, è clientB.

  Rete remota IPv4 Questo campo imposta l'*iroute* richiesto, quindi inserisci la sottorete LAN del clientB, 10.5.0.0/24
- Fare clic su **Salvare**

  Aggiungere una sostituzione per il secondo sito, regolando il **nome comune** e la **rete remota IPv4** secondo necessità. Nell'esempio per il sito C, questi valori sarebbero rispettivamente clientC e 10.7.0.0/24.

  Il prossimo compito è esportare i certificati e le chiavi necessari per i client.
- Passare a **Sistema>Gestione dei certificati**
- **Fare clic sui collegamenti per esportare i seguenti elementi:**
  - Certificato CA
  - Certificato del sito del client (.crt) per ogni posizione del client.
  - Chiave del sito del client (.key) per ogni posizione del client.

Avvertimento: non esportare la chiave CA, il certificato del server o la chiave del server. Non sono necessari sui client e copiarli inutilmente indebolisce significativamente la sicurezza della VPN.

Ciò completa la configurazione del server, quindi, ora passare a configurare i client.

Configurazione del lato client con SSL/TLS

Sul client, importare il certificato CA insieme al certificato client e alla chiave per quel sito. Questi sono lo stesso certificato CA e lo stesso certificato del client presenti sul server ed esportati da lì. Questo può essere fatto in **Sistema>Gestione dei certificati**. Per le specifiche relative all'importazione della CA e dei certificati, vedere *Gestione dei certificati*.

Dopo aver importato i certificati, creare il client di OpenVPN:

- Passare a **VPN>OpenVPN**, scheda **Client**
- Fare clic su  **Aggiungere** per creare un nuovo client
- **Compilare i campi come segue, con tutto il resto lasciato ai valori**

  predefiniti

  Modalità del server Selezionare *Peer a Peer (SSL/TLS)*

  Protocollo Selezionare *UDP*

  Modalità del dispositivo Selezionare *tun*

  Interfaccia Selezionare *WAN*

  Host o indirizzo del server Immettere qui l'indirizzo IP pubblico o l'hostname del server OpenVPN (ad es. 51.100.3)

  Porta server Immettere 1194 o qualsiasi porta sia stata configurata sul server

  Descrizione Inserire qui il testo per descrivere la connessione

  Autenticazione TLS Selezionare **Abilitare l'autenticazione dei pacchetti TLS**, deselezionare **Genera re automaticamente una chiave di autenticazione TLS condivisa**, quindi incollare la chiave TLS per la connessione qui utilizzando la chiave copiata dall'istanza del server creata in precedenza

  Autorità di certificazione dei peer Selezionare la CA importata all'inizio di questo processo

  Certificato del client Selezionare il certificato del client importato all'inizio di questo processo
- Fare clic su Salvare

È inoltre necessario aggiungere una regola all'interfaccia OpenVPN per passare il traffico sulla VPN dalla LAN suk lato client alla LAN sul lato server. È possibile utilizzare una regola di stile «Consentire tutto» o un insieme di regole più severe. In questo esempio, consentire tutto il traffico è OK, quindi viene fatta la seguente regola:

- Passare a **Firewall>Regole**, scheda **OpenVPN**
- **Fare clic su**  **Aggiungere per creare una nuova regola** nella parte superiore dell'elenco
- Impostare il **protocollo** su *qualsiasi*
- Immettere una **descrizione** come Consentire tutto su OpenVPN
- Fare clic su Salvare
- Fare clic su Applicare le modifiche

La configurazione del client è completa. Non sono richieste regole del firewall sulla WAN del client perché il client avvia solo connessioni in uscita.

Nota: con le configurazioni PKI di accesso remoto, i percorsi e le

---

altre opzioni di configurazione non sono solitamente definiti nella configurazione del client, ma vengono spinti dal server al client. Se ci sono più reti da raggiungere sul lato server, configurarle sul server da spingere.

Testare la connessione

La configurazione è ora completa e la connessione sarà immediatamente attiva al momento del salvataggio sul lato client. Provare a eseguire il ping fino all'estremità remota per verificare la connettività. In caso di problemi, fare riferimento alla *Risoluzione dei problemi di OpenVPN*.

18.2.8 Controllo dello stato dei client e dei server OpenVPN

La pagina dello stato si OpenVPN in **Stato>OpenVPN** mostra lo stato di ciascun server e client OpenVPN. I controlli di avvio/arresto del servizio sono disponibili anche per ogni istanza server e client separata nella pagina di stato.

Per i server OpenVPN in modalità server SSL/TLS, lo stato fornisce un elenco di client remoti collegati insieme ai loro nomi utente o nomi comuni di certificati, come si vede in figura *Stato di OpenVPN per il server SSL/TLS con un client connesso*. I client possono anche essere disconnessi da questa schermata facendo clic su alla fine della riga del client. Per questi server viene visualizzato anche un pulsante **Mostrare la tabella di routing**. Facendo clic su questo pulsante verrà visualizzata una tabella di reti e indirizzi IP collegati tramite ciascun certificato del client.

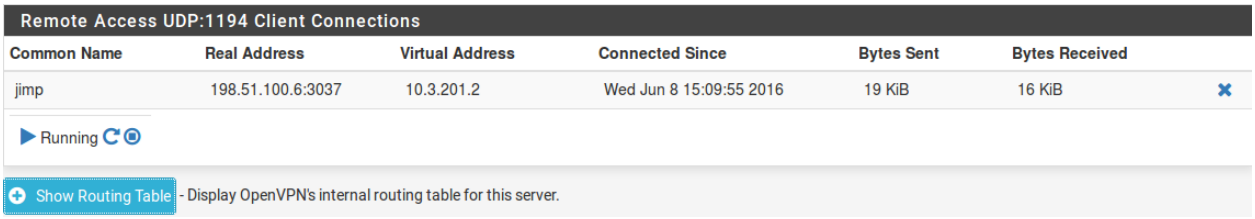


Fig. 13: Stato di OpenVPN per il server SSL/TLS con un client connesso

Per i server di OpenVPN in modalità chiave condivisa, lo stato indicherà se è in esecuzione e in attesa di connessioni o se il client remoto è connesso.

Per i client OpenVPN, lo stato indica se una connessione è in sospeso o attiva.

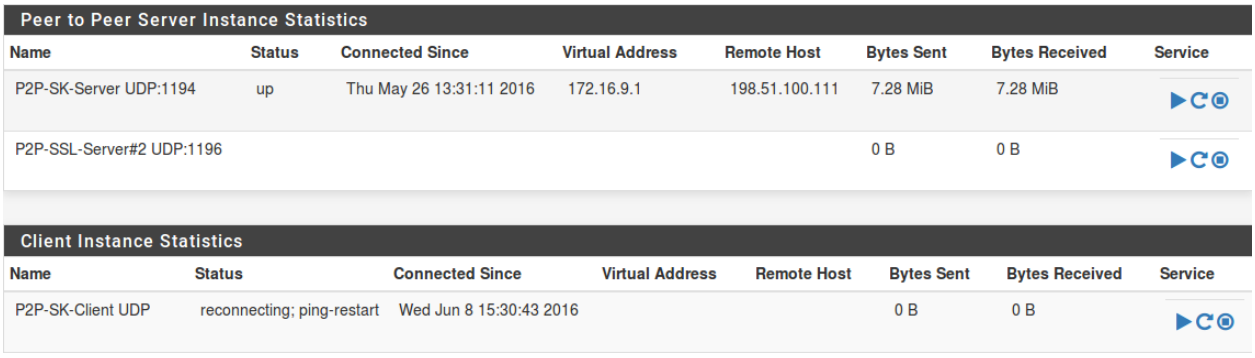


Fig. 14: Stato di OpenVPN che mostra un server attivo, uno in attesa di una connessione e un client che tenta di riconnettersi

18.2.9 Consentire il traffico al server di OpenVPN

Dopo aver impostato un server OpenVPN, è necessaria una regola firewall per consentire il traffico al server OpenVPN.

- Passare a **Firewall>Regole**, scheda **WAN**
- Fare clic su  per creare una nuova regola nella parte superiore della lista
- Impostare il **protocollo** su *UDP*
- Lasciare la **sorgente** impostata su *qualsiasi*
- Impostare la **destinazione** su l'*indirizzo WAN*
- Impostare la **porta di destinazione** su questa istanza
- Immettere una **descrizione**, ad esempio Consentire il traffico al server OpenVPN
- Fare clic su **Salvare**
- Fare clic su **Applicare le modifiche**

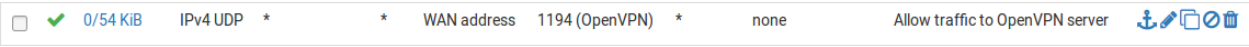


Fig. 15: Regola della WAN del server di OpenVPN

Questa regola è raffigurata nella figura *Regola della WAN del server di OpenVPN*.

Se gli indirizzi di sorgente del client sono noti e non cambiano, l'origine della regola potrebbe essere modificata per limitare il traffico solo da quei client. Questo è più sicuro che lasciare il server esposto a tutto l'Internet, ma è necessario per accogliere i client con indirizzi IP dinamici, i client in roaming, e così via. Il rischio di lasciare il servizio esposto con la maggior parte delle configurazioni OpenVPN è minimo, specialmente nei casi in cui viene utilizzata l'autenticazione TLS. Con l'autenticazione basata sui certificati c'è meno rischio di compromissione rispetto alle soluzioni basate su password che sono suscettibili alla forza bruta. Ciò presuppone una mancanza di buchi nella sicurezza nella OpenVPN stessa, che ad oggi ha una solida registrazione del tracciamento della sicurezza.

18.2.10 Consentire il traffico sul tunnel di OpenVPN

Per impostazione predefinita, tutto il traffico è bloccato dall'ingresso del tunnel OpenVPN. Per consentire al traffico dai nodi OpenVPN remoti di effettuare connessioni alle risorse sul lato locale, sono necessarie regole del firewall in **Firewall>Regole**, nella scheda **OpenVPN**.

Come per altri aspetti del firewall, queste regole corrisponderanno solo al traffico che entra nel sistema dal lato remoto, non al traffico che esce dal lato server, quindi creare le regole di conseguenza. Nei casi in cui Firew4LL viene utilizzato su entrambe le estremità e il traffico è necessario per raggiungere le reti locali su entrambi i lati, quindi le regole sono necessarie su entrambi i firewall.

Aggiungere una regola OpenVPN che passa tutto il traffico come segue:

- Passare a **Firewall>Regole**, scheda **OpenVPN**
- **Fare clic su**  **per creare una nuova regola nella parte** superiore della lista
- Impostare il **protocollo** su *qualsiasi*
- Immettere una **descrizione** come Consentire tutto su OpenVPN
- Fare clic su **Salvare**
- Fare clic su **Applicare le modifiche**

Per limitare il traffico solo a sorgenti e destinazioni specifiche, modificare le regole in base alle esigenze. Un set di regole rigoroso è più sicuro, ma più difficile da creare.

18.2.11 Client OpenVPN e accesso a Internet

Per i client di accesso remoto OpenVPN per raggiungere Internet tramite la connessione OpenVPN, è necessario un NAT in uscita per tradurre il traffico all'indirizzo IP della WAN del firewall. Le regole del NAT in uscita automatiche predefinite coprono questo aspetto, ma se il NAT in uscita manuale è in uso, sono necessarie regole manuali per eseguire il NAT in uscita sul traffico da sorgenti che includono la rete del tunnel OpenVPN o le reti remote.

NAT in uscita per maggiori dettagli sul NAT in uscita.

18.2.12 Assegnazione delle interfacce OpenVPN

Per eseguire un filtro NAT, la politica del routing o il tunnel specifico complesso, l'interfaccia OpenVPN deve essere assegnata come interfaccia OPT e configurata di conseguenza.

L'assegnazione dell'interfaccia OpenVPN consente diverse modifiche utili per il controllo avanzato del traffico VPN:

- Aggiungere una scheda firewall in **Firewall>Regole**
- Aggiungere *reply-to* alle regole sulla scheda interfaccia VPN per facilitare il routing di ritorno
- Aggiungere una voce di gateway per il lato più lontano della VPN per la politica di routing
- Consentire di selezionare l'interfaccia altrove nella GUI e nei pacchetti
- Consentire un controllo più preciso della porta forward e del NAT in uscita per la VPN

Assegnazione e configurazione dell'interfaccia

- Passare a **Interfacce>(assegnare)**
- Selezionare l'interfaccia ovpns o ovpnc appropriata nelle **porte di rete disponibili**, la descrizione della VPN viene stampata per riferimento.
- Fare clic su  **Aggiungere** per assegnare l'interfaccia come una nuova interfaccia OPT (ad esempio OPT1)

  La figura *Assegnare l'interfaccia OpenVPN* mostra ovpns1 assegnata come OPT1.

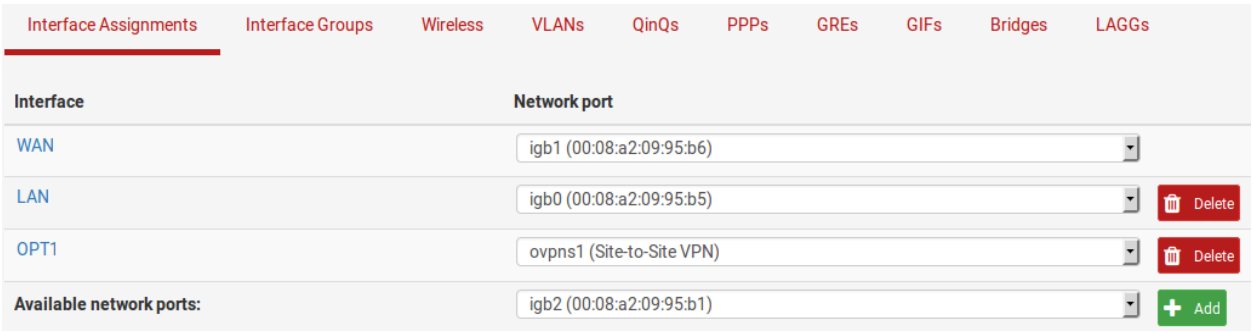


Fig. 16: Assegnare l'interfaccia OpenVPN

- Passare alla pagina di configurazione dell'interfaccia, **Interfacce>OPTx**
- Selezionare **Abilitare**

- Immettere una **descrizione** appropriata che diventerà il nome dell'interfaccia (ad esempio ServerVPN)
- Selezionare *nessuno* sia per il **tipo di configurazione IPv4** che per il **tipo di configurazione IPv6**

Nota: Questo non configura alcuna informazione sull'indirizzo IP dell'interfaccia, che è necessaria poiché la OpenVPN stessa deve configurare queste impostazioni.

- Fare click su **Salvare**
- Fare click su **Applicare le modifiche**

Ciò non modifica la funzionalità di OpenVPN, rende l'interfaccia disponibile per la regola firewall, NAT e gateway, tra gli altri usi.

Dopo aver assegnato l'interfaccia OpenVPN, modificare il server o il client OpenVPN e fare clic su **Salvare** una volta anche lì per reinizializzare la VPN. Ciò è necessario affinché la VPN possa recuperare dal processo di assegnazione.

Filtraggio con OpenVPN

Quando viene assegnata l'interfaccia OpenVPN, è presente una scheda in **Firewall>Regole** dedicata solo a questa singola VPN. Queste regole riguardano il traffico proveniente dal lato remoto della VPN e ottengono persino la parola chiave per la reply-to di pf che assicura che il traffico che entra in questa interfaccia VPN esca dalla stessa interfaccia. Questo può aiutare con alcuni scenari NAT e di configurazione più avanzati.

Nota: le regole aggiunte qui vengono elaborate dopo le regole della scheda OpenVPN, che vengono selezionate per prime. Per corrispondere alle regole di una scheda VPN assegnata, il traffico **non deve corrispondere** alle regole della scheda OpenVPN. Rimuovere le regole di stile "Consentire tutto" dalla scheda OpenVPN e creare invece regole più specifiche.

Vedi anche:

Per ulteriori informazioni sulle regole del firewall, fare riferimento a *Firewall*.

Politica di routing con OpenVPN

Quando l'interfaccia OpenVPN è assegnata e abilitata, viene aggiunta una voce gateway automatica in **Sistema>Routing**, nella scheda **Gateway**. Con questo, il traffico può essere diretto nella VPN utilizzando il campo **Gateway** sulla LAN o altre regole firewall di interfaccia interna.

Se utilizzato con una VPN per raggiungere siti Internet, potrebbe essere necessaria una maggiore configurazione. O il NAT in uscita deve essere eseguito sull'interfaccia VPN prima che se ne vada (per i servizi VPN come PIA, StrongVPN e simili) o il NAT deve essere fatto dall'altra parte prima che raggiunga la connessione internet effettiva.

Vedi anche:

Vedere *Politica di routing* per ulteriori informazioni sulla politica di routing.

Avvertimento: non utilizzare questo gateway automatico per i percorsi statici. Utilizzare il campo della Rete remota nella configurazione VPN. La definizione di un percorso statico utilizzando il gateway OpenVPN automatico non funzionerà correttamente.

NAT con OpenVPN

Quando viene assegnata L'interfaccia OpenVPN, le regole NAT possono essere applicate allo stesso modo di qualsiasi altra interfaccia. Ciò è utile quando si collegano due sottoreti in conflitto o per rendere SPECIFICHE le regole NAT a questa connessione VPN (NAT in uscita, inoltro della porta o NAT 1:1)

18.2.13 NAT con connessioni OpenVPN

Per molti scenari NAT avanzati che utilizzano OpenVPN, è necessario assegnare l'interfaccia come descritto in *Assegnazione di interfacce Open-VPN*

Un uso comune di NAT con OpenVPN è quello di mascherare le sottoreti LAN in conflitto tra due posizioni. Se due reti utilizzano la stessa sottorete o sottoreti sovrapposte, come il loro LAN o altra rete interna, non possono comunicare attraverso una VPN con sito-a-sito senza NAT.

Ad esempio, se 10.3.0.0/24 è la LAN su entrambi i lati di una VPN, gli host su una sottorete 10.3.0.0/24 non raggiungeranno mai l'altra estremità della VPN per comunicare con la sottorete 10.3.0.0/24 remota. I client tratteranno sempre quella rete come locale, tentando di raggiungere gli altri sistemi tramite ARP. Con il NAT, tuttavia, il lato remoto può essere fatto funzionare come se stesse usando una sottorete diversa.

Nota: l'utilizzo del NAT funzionerà per molti protocolli, ma alcuni che sono comunemente desiderabili tra le connessioni VPN, principalmente la condivisione di file SMB/CIFS tra gli host di Windows, non funzioneranno in combinazione con il NAT. Se viene utilizzato un protocollo che non è in grado di funzionare con il NAT, non è una soluzione praticabile.

Figura *Sito-a-sito con sottoreti in conflitto* mostra un esempio in cui entrambe le estremità utilizzano la stessa sottorete. Dopo aver assegnato l'interfaccia OpenVPN a un'interfaccia OPT su entrambi i lati, come descritto in *Assegnazione e configurazione dell'interfaccia*, è possibile applicare il NAT 1:1.

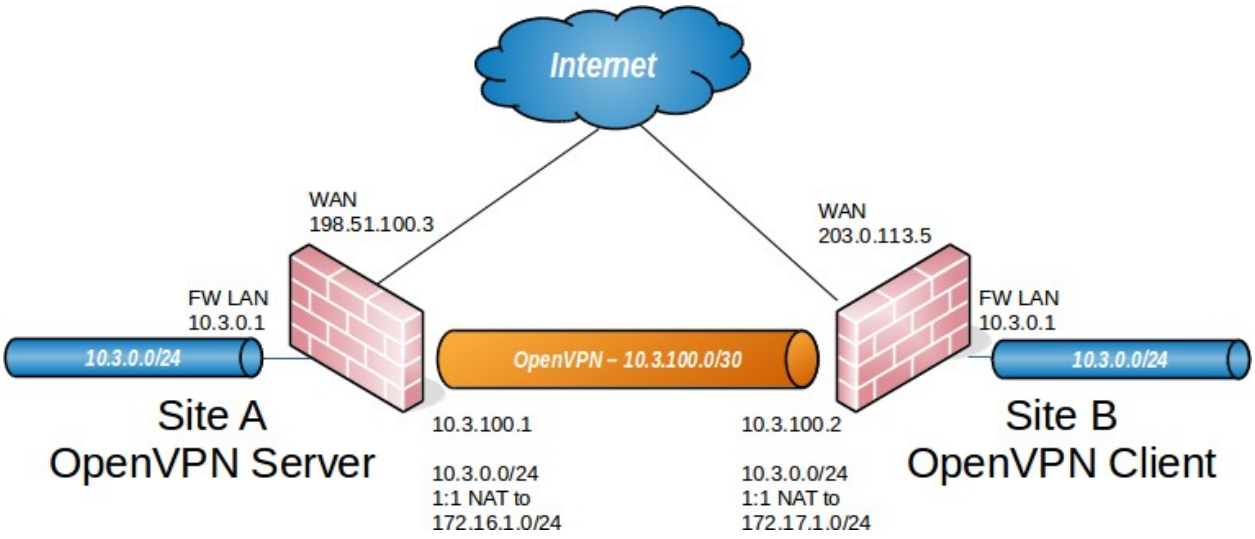


Fig. 17: Sito-a-sito con sottoreti in conflitto

Il traffico dal sito A sarà tradotto in 172.16.1.0/24, e il sito B sarà tradotto in 172.17.1.0/24. Una voce del NAT 1:1 viene aggiunta su ciascuna estremità per tradurre l'intero intervallo /24. Per raggiungere il sito A dal sito B, gli indirizzi IP 172.16.1.x verranno utilizzati. L'ultimo ottetto nell'IP 10.3.0.x sarà tradotto all'ultimo ottetto dell'IP 172.16.1.x tradotto. Raggiungere 10.3.0.10 sul sito A dal sito B, utilizzare 172.16.1.10. Per raggiungere 10.3.0.50 sul sito B dal sito A, utilizzare 172.17.1.50. La figura *Configurazione del NAT 1:1 del sito B* mostra la configurazione del NAT 1:1 per ciascun lato, dove l'interfaccia *tun* è assegnata come OPT1.

Nella configurazione OpenVPN su entrambi i lati, la **rete remota** deve essere specificata come sottorete IP tradotta, non come 10.3.0.0 / questo esempio, la **rete remota** nel sito A è 172.17.1.0/24 e 172.16.1.0/24 nel sito B.

Dopo aver applicato le modifiche della configurazione del NAT e configurato la rete remota di conseguenza su entrambi i lati, le reti saranno in grado di comunicare utilizzando le sottoreti tradotte.

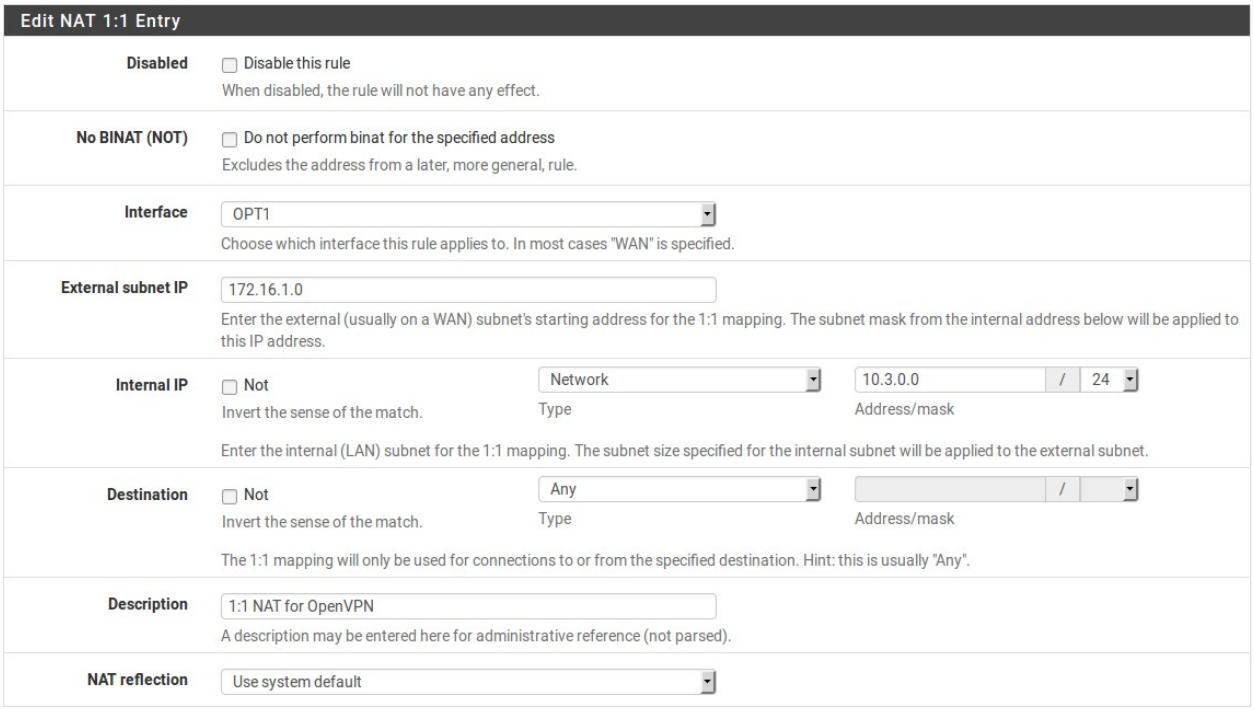


Fig. 18: Configurazione del NAT 1:1 del sito A

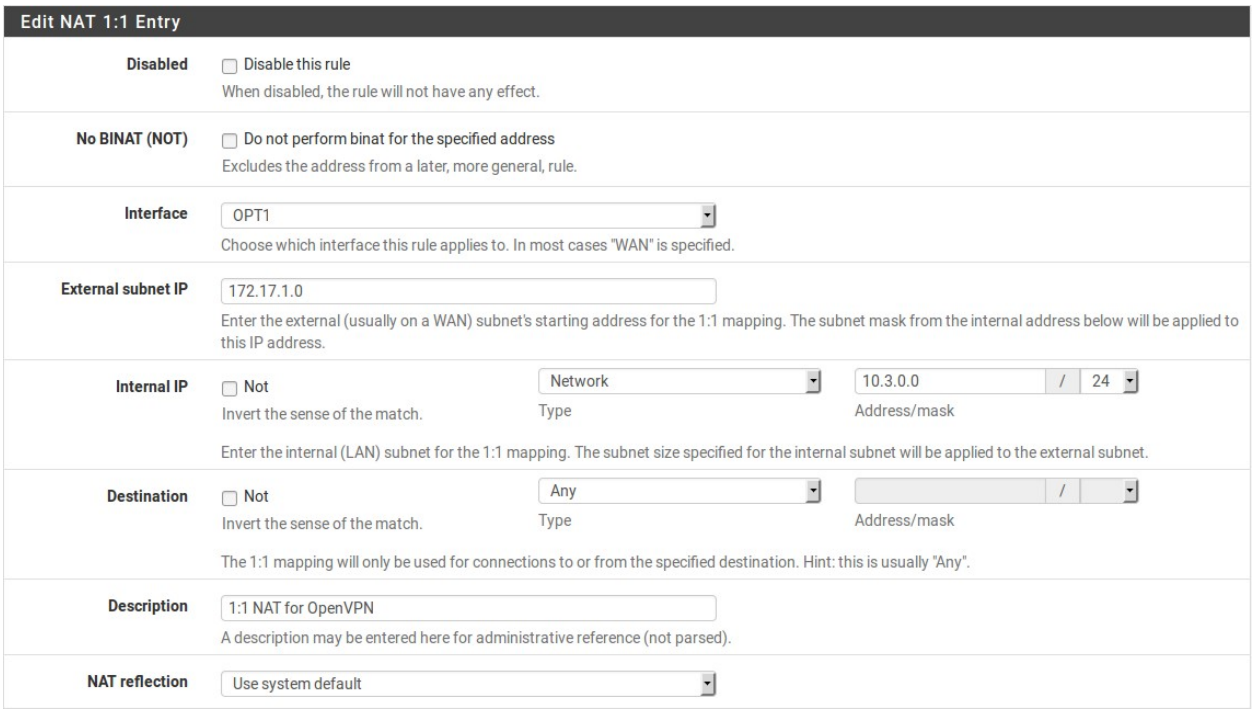


Fig. 19: Configurazione del NAT 1:1 del sito B

18.2.14 OpenVPN e Multi-WAN

OpenVPN può supportare la Multi-WAN, con alcuni avvertimenti in determinate circostanze. Questa sezione copre le connessioni Multi-WAN con le configurazioni di server e client di OpenVPN.

OpenVPN assegnata a un gruppo di gateway

Un gruppo di gateway (*Gruppi di gateway*) può essere selezionato come **interfaccia** per un'istanza di OpenVPN. Tale gruppo di gateway deve essere configurato solo per il failover, non per il bilanciamento del carico. I gruppi di failover hanno solo un gateway per livello. Durante la creazione del gruppo gateway, può anche essere scelto un VIP per l'uso con un gateway specifico. Se selezionato per un server VPN, verrà utilizzata per prima l'interfaccia o il VIP del gateway del livello 1 nel gruppo. Se quel gateway va down, si sposterà al livello 2, e così via. Se il gateway di livello 1 viene ripristinato, la VPN riprenderà immediatamente a funzionare su tale WAN. Quando viene utilizzato per un server VPN, ciò significa che il server è attivo solo su una WAN alla volta. Alcuni dei metodi descritti di seguito potrebbero rivelarsi migliori per le circostanze più comuni, ad esempio la necessità di utilizzare entrambe le WAN in concomitanza con la VPN. Se utilizzato con i client di OpenVPN, l'interfaccia in uscita verrà commutata in base ai livelli del gruppo di gateway.

Server OpenVPN e MultiWAN

I server OpenVPN possono essere utilizzati con qualsiasi connessione WAN, anche se i mezzi per farlo variano a seconda delle specifiche di una determinata configurazione.

Server OpenVPN che utilizza TCP

TCP non è il protocollo preferito per OpenVPN. Tuttavia, utilizzare TCP può rendere la scongiurazione di multi-WAN per OpenVPN più facile quando la VPN utilizza un'impostazione di interfaccia su *qualsiasi*. I server OpenVPN che utilizzano TCP funzioneranno correttamente su tutte le WAN in cui le regole del firewall consentono il traffico sul server OpenVPN. Per ogni interfaccia WAN è necessaria una regola del firewall. Questo metodo dovrebbe essere considerato come un'ultima risorsa e utilizzato solo se gli altri metodi non sono attuabili.

Nota: questo funziona a causa della natura orientata alla connessione di TCP. L'OpenVPN può rispondere all'altra estremità con la sorgente corretta conservata poiché fa parte di una connessione aperta.

Server OpenVPN che utilizza UDP

I server OpenVPN con UDP supportano anche la Multi-WAN, ma con alcune condizioni che non sono applicabili con TCP.

Queste limitazioni di OpenVPN sono dovute alla natura senza connessione di UDP. L'istanza OpenVPN risponde al client, ma il sistema operativo seleziona il percorso e l'indirizzo di origine in base a ciò che la tabella di routing ritiene sia il percorso migliore per raggiungere l'altro lato. Per le WAN non predefinite, questo non sarà il percorso corretto.

Metodo server multiplo

In alcuni casi, ogni WAN deve avere il proprio server OpenVPN. Gli stessi certificati possono essere usati per tutti i server. Solo due parti della configurazione OpenVPN devono cambiare:

Rete del tunnel Ogni server deve avere una **rete del tunnel** unica che non si sovrappone a qualsiasi altra rete tunnel o sottorete interna.

Interfaccia Ogni server OpenVPN deve specificare un'**interfaccia** WAN diversa.

Metodo del port forward

Un'opzione più semplice e flessibile è quella di associare il server OpenVPN all'interfaccia *LAN* o all'*host locale* e utilizzare una porta forward da ogni WAN per indirizzare la porta OpenVPN al servizio. Utilizzando questo metodo, la funzionalità reply-to in pf garantirà che il traffico di ritorno ritorni alla sorgente corretta tramite l'interfaccia prevista.

Questo metodo richiede un piccolo intervento manuale quando viene utilizzato con il pacchetto di esportazione del client. L'opzione di **risoluzione del hostname** deve essere impostata su uno dei metodi di inoltro automatico della porta, altrimenti le impostazioni di esportazione predefinite lo lascerebbero tentare di connettersi all'indirizzo sbagliato. Vedere *Pacchetto di esportazione del client di OpenVPN* per i dettagli

Failover automatico per i client

Più server remoti possono essere configurati sui client di OpenVPN. Se il primo server non può essere raggiunto, verrà utilizzato il secondo. Questo può essere utilizzato in combinazione con una distribuzione server OpenVPN con Multi-WAN per fornire il failover automatico per i client. Se i server OpenVPN sono in esecuzione sugli indirizzi IP 198.51.100.3 e 203.0.113.5, entrambi che utilizzano la porta 1194, le righe remote nel file di configurazione del client saranno le seguenti:

remote 198.51.100.3 1194 udp remote 203.0.113.5 1194 udp

Per i client configurati su Firew4LL, il primo remoto viene configurato dal ***Campo dell'host o dell'indirizzodel server nella GUI**. **Il secondo "remoto" è specificato** nel campo ****Avanzate**.

Questo metodo ha tre comportamenti degni di nota che alcuni possono trovare indesiderabili:

- Ci vorranno almeno 60 secondi per rilevare un guasto e passare al server successivo.
- Qualsiasi errore di connessione farà sì che si provi il secondo server, anche se non si tratta di un errore della WAN.
- **Non** opera il «fail-back». Una volta che un client si connette al secondo indirizzo IP del server rimarrà lì fino alla disconnessione.

Client OpenVPN e MultiWAN

Per utilizzare UN'interfaccia opt WAN, selezionarla come interfaccia. I client OpenVPN configurati sul firewall rispetteranno l'interfaccia scelta e un percorso statico viene aggiunto automaticamente dietro le quinte per garantire che il traffico prenda il percorso corretto.

Se l'interfaccia è invece impostata su qualsiasi, il client seguirà la tabella di routing del sistema quando effettua la connessione al server OpenVPN. In questo caso sarà necessario un percorso statico manuale per indirizzare il traffico verso l'endpoint remoto sulla WAN desiderata.

OpenVPN Site-to-Site con MultiWAN e OSPF

Basandosi sui concetti esposti in precedenza nel capitolo, è possibile configurare una VPN ridondante utilizzando un protocollo di routing dinamico come OSPF come si vede nell'esempio della figura *Esempio di configurazione di OpenVPN che coinvolge OSPF su WAN multiple*.

Innanzitutto, impostare le istanze della OpenVPN con sito-a-sito con **chiave condivisa** su ogni WAN per i siti remoti. **Non compilare** i campi **reti remote** su entrambi i lati, solo gli indirizzi di **rete del tunnel**.

- Impostare due server sul lato locale, ciascuno su una porta diversa. Utilizzare due reti tunnel distinte e non sovrapposte (ad esempio 172.31.55.0/30 e 172.31.56.0/30)
- Impostare due client sul firewall remoto, ciascuno associato a uno dei server di cui sopra, corrispondenti agli indirizzi IP e ai numeri di porta coinvolti.
- Assicurarsi che i client siano impostati per la loro specifica WAN, scegliere l'interfaccia dal menu a discesa, o un VIP del CARP che si trova su una delle WAN in uso.
- Assicurarsi che queste connessioni OpenVPN si colleghino tra client e server. L'indirizzo del tunnel su entrambi i lati risponderà a un ping quando funzionano correttamente. Se i tunnel non vengono stabiliti, vedere *Risoluzione dei problemi di OpenVPN* per suggerimenti sulla risoluzione dei problemi della connessione.
- Assicurarsi che le regole del firewall OpenVPN consentano tutto il traffico o almeno consentano il traffico OSPF da una sorgente delle reti del tunnel a una destinazione di qualsiasi. La destinazione sul traffico sarà un indirizzo multicast, che può essere utilizzato per filtrare in modo specifico se necessario, ma non c'è molto da guadagnare in termini di sicurezza se la sorgente è bloccata nelle regole in quanto il traffico non può lasciare quel segmento.

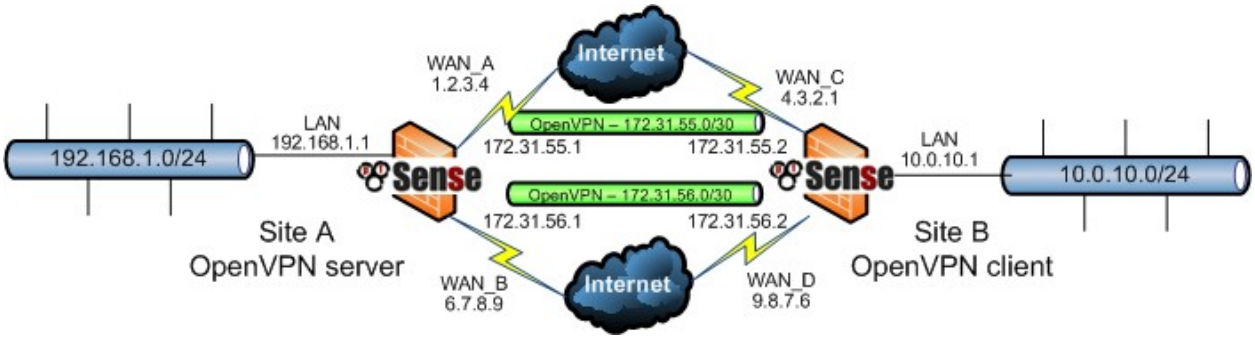


Fig. 20: Esempio di configurazione di OpenVPN che coinvolge OSPF su WAN multiple

Una volta collegate entrambe le istanze, configurare OSPF.

- Installare il pacchetto Quagga_OSPF da **Sistema>Pacchetti**, scheda **Pacchetti disponibili** su **entrambi i firewall**.
- Passare a **Servizi>quagga OSPFd**, scheda **Interfacce**
- Aggiungere ogni interfaccia di OpenVPN
  - Impostare il costo su 10 sul collegamento primario e 20 sul secondario, e così via
  - Aggiungere la LAN e le altre interfacce interne come interfacce **passive**
- Passare alla scheda **Impostazioni globali**
- Immettere una password principale. Non importa che cosa viene impostato, è utilizzato internamente per accedere al demone dello stato.
- Impostare l'ID del router su un valore simile a un indirizzo IP (ad esempio 10.3.0.1.) l'ID del router è univoco su ciascun dispositivo, motivo per cui impostarlo sull'indirizzo IP della LAN di un router è una buona pratica.
- Impostare l'ID dell'area che è anche un valore simile a un indirizzo IP. L'ID dell'area è in genere impostato su 0.0.0.0 o 0.0.0.1, ma è possibile utilizzare qualsiasi valore formattato correttamente. L'ID dell'area è lo stesso per tutti i router coinvolti in questa VPN
- Fare click su Salvare

Una volta che OSPF è stato configurato su tutti i router, tenteranno di formare una relazione vicina.

Dopo che OSPF è stato configurato su entrambe le estremità, la scheda **Stato** mostrerà un peering completo per ogni istanza su ciascuna wan se collegata correttamente e verranno elencati i percorsi ottenuti tramite OSPF. Una volta che ciò accade, provare a scollegare/ricollegare le WAN e ad aggiornare lo stato durante l'esecuzione di un traffico di test attraverso la VPN, ad esempio un ping ICMP.

18.2.15 OpenVPN e CARP

OpenVPN funziona bene con l'elevata disponibilità utilizzando il CARP. Per fornire una soluzione OpenVPN ad elevata disponibilità con CARP, configurare il server o il client OpenVPN per utilizzare il VIP del CARP con l'opzione interfaccia e configurare i client per connettersi al VIP del CARP.

Quando le impostazioni di sincronizzazione della configurazione XMLRPC sono abilitate, le istanze OpenVPN si sincronizzeranno automaticamente. Lo stato di connessione non viene mantenuto tra gli host, quindi i client devono riconnettersi dopo il failover, ma OpenVPN rileverà l'errore di connessione e si riconnetterà entro un minuto o giù di lì dal failover. L'elevata disponibilità e il CARP sono discussi ulteriormente in *Elevata disponibilità*.

Quando un VIP del CARP viene selezionato come **interfaccia** per un'istanza di OpenVPN, il firewall spegne automaticamente le istanze del client di OpenVPN in base alle esigenze quando un nodo CARP si trova in uno stato ddel BACKUP. Ciò impedisce a OpenVPN di effettuare connessioni in uscita non necessarie in modalità client. Quando le transizioni di stato del VIP del CARP al MASTER, le istanze OpenVPN vengono avviate automaticamente.

18.2.16 Connessioni OpenVPN con bridge

Le configurazioni di OpenVPN discusse a questo punto sono state tutte instradate, utilizzando le interfacce *tun*. Questo è il metodo preferibile, ma OpenVPN offre anche la possibilità di utilizzare interfacce *tap* e client di collegamento direttamente sulla LAN o un'altra rete interna. Questo può fare in modo che ai client remoti sembri di essere sulla LAN locale.

Impostazioni del server di OpenVPN

La maggior parte delle impostazioni per una VPN di accesso remoto a ponte sono le stesse esposte sopra per una VPN di accesso remoto tradizionale. Saranno annotate qui solo le differenze.

Modalità dispositivo Per creare una connessione a ponte, questo deve essere impostato su *tap*.

Rete del tunnel Rimuovere i valori dalle caselle della rete del tunnel con IPv4 e della rete del tunnel con IPv6 in modo che siano vuote. Il modo in cui funziona un OpenVPN con il bridge impostato per la *tap* non ha bisogno di una rete tunnel in quanto OpenVPN non utilizza la stessa assegnazione di indirizzi di cui ha bisogno in modalità *tun*.

DHCP del bridge Una volta selezionato, DHCP verrà passato all'interfaccia con il bridge configurata in seguito. Nello scenario più comune, questa è una LAN. L'utilizzo di questo metodo che collega i client ha bisogno di ricevere indirizzi IP dallo stesso pool DHCP utilizzato dai client LAN direttamente cablati.

Interfaccia con il bridge Questa impostazione non crea il bridge, indica solo a OpenVPN quale interfaccia verrà utilizzata per il bridge. Nella maggior parte dei casi, questa è una LAN. Questo controlla quale indirizzo IP esistente e quale maschera di sottorete vengono utilizzati da OpenVPN per il bridge. Impostare su *nessuno* farà sì che le impostazioni **DHCP del bridge del server** di seguito vengano ignorate.

Avvio/Fine di DHCP del bridge del server Quando si utilizza la modalità *tap* per il server multipunto, è possibile configurare un intervallo DHCP da utilizzare sull'interfaccia a cui è collegata questa istanza *tap*. Se queste impostazioni vengono lasciate vuote, DHCP verrà passato all'interfaccia bridge e l'impostazione dell'interfaccia di sopra verrà ignorata. Ciò consente di impostare un intervallo di indirizzi IP da utilizzare solo dai client OpenVPN in modo che possano essere contenuti all'interno di una porzione

della rete interna piuttosto che consumare indirizzi IP dal pool DHCP esistente. Immettere i valori dell'indirizzo IP per l'**Avvio di DHCP del bridge del server** e per la **Fine del DHCP del bridge del server** secondo le necessità.

Creare il bridge

Una volta creato il server con il *tap* di OpenVPN, l'interfaccia di OpenVPN deve essere assegnata e collegata all'interfaccia interna.

Assegnare un'interfaccia OpenVPN

Per includere l'interfaccia VPN in un bridge, questa deve essere assegnata. La procedura per l'assegnazione di un'interfaccia è descritta in precedenza in questo capitolo, in *Assegnazione di interfacce OpenVPN*.

Creare il bridge

Una volta assegnata l'interfaccia VPN, creare il bridge come segue:

- Passare a **Interfacce>(assegnare),** scheda **Bridge**
- Fare clic su  **Aggiungere** per creare un bridge
- **Usare Ctrl-Click sia sull'interfaccia VPN che sull'interfaccia in cui** verrà creato il bridge (ad esempio *LAN*)
- Fare click su **Salvare**

Maggiori informazioni sul bridging possono essere trovate in *Bridging*.

Connettersi con i client

I client che si connettono alla VPN devono anche essere impostati per utilizzare la modalità *tap*. Una volta impostato, connettersi con un client come quello esportato utilizzando il pacchetto di esportazione del client di OpenVPN. I client riceveranno un indirizzo IP all'interno della sottorete interna come se fossero sulla LAN. Si riceveranno anche traffico broadcast e quello multicast.

18.2.17 Opzioni di configurazione personalizzate

OpenVPN offre decine di opzioni di configurazione, molte al di là dei campi più comunemente utilizzati presentati nella GUI. Questo è il motivo per cui esiste la casella di **configurazione avanzata**. Ulteriori opzioni di configurazione possono essere configurate utilizzando questa area di input, separata da punto e virgola.

Questa sezione copre le opzioni personalizzate più utilizzate singolarmente. Ce ne sono molte altre, anche se raramente necessarie. La Pagina principale di OpenVPN le descrive tutte.

Avvertimento: prestare attenzione quando si aggiungono opzioni personalizzate, poiché non viene applicata alcuna convalida di input per garantire la validità delle opzioni utilizzate. Se un'opzione viene utilizzata in modo errato, il client o il server OpenVPN potrebbero non avviarsi. Visualizzare i registri OpenVPN in Stato>Registri di sistema nella scheda OpenVPN per garantire che le opzioni utilizzate siano valide. Qualsiasi opzione non valida comporterà un messaggio di registro, seguito dall'opzione che ha causato l'errore:: Options error: Unrecognized option or missing parameter(s)

Opzioni di routing

Per aggiungere percorsi aggiuntivi per un particolare client o server OpenVPN, utilizzare le caselle della **Rete locale** e della **Rete remota**, se necessario, utilizzando un elenco di reti separate da virgole.

L'opzione di configurazione personalizzata della route può anche essere utilizzata, ma non è più necessaria. Tuttavia, alcuni utenti preferiscono questo metodo. L'esempio seguente aggiunge un percorso per 10.50.0.0/24:

route 10.50.0.0 255.255.255.0; route 10.254.0.0 255.255.255.0;

Per aggiungere più percorsi, separarli con un punto e virgola:

route 10.50.0.0 255.255.255.0; route 10.254.0.0 255.255.255.0;

L'opzione di configurazione della route viene utilizzata per aggiungere percorsi localmente per le reti raggiungibili tramite la VPN. Per una configurazione del server OpenVPN tramite PKI, è possibile anche inviare percorsi aggiuntivi ai client. La GUI può configurarli utilizzando il campo della **Rete locale**. Per inviare manualmente i percorsi per 10.50.0.0/24 e 10.254.0.0/24 a tutti i client, utilizzare la seguente opzione di configurazione personalizzata:

push «route 10.50.0.0 255.255.255.0»; push «route 10.254.0.0 255.255.255.0»;

Reindirizzamento del gateway predefinito

OpenVPN consente inoltre di reindirizzare il gateway predefinito attraverso la VPN, quindi tutto il traffico non locale dal client viene inviato tramite la VPN. Questo è va molto bene per le reti locali non attendibili come hotspot wireless, in quanto fornisce una protezione contro numerosi attacchi che sono un rischio su reti non attendibili. Questo è configurabile ora nella GUI, selezionando la casella di **Reindirizzamento del gateway** nella configurazione dell'istanza OpenVPN. Per fare questo manualmente, aggiungere la seguente opzione personalizzata:

push «redirect-gateway def1»

Lo stesso valore può essere utilizzato come opzione personalizzata sul lato client inserendo redirect-gateway def1 senza specificare push . (Notare l'opzione è composta dalle lettere » def «seguite dalla cifra *uno*, non dalla lettera «L».)

18.2.18 Condivisione di una porta con OpenVPN e un server Web

Per essere più subdolo o attento con un server OpenVPN, sfruttare la capacità di condivisione delle porte in OpenVPN che permette di passare qualsiasi traffico non OpenVPN ad un altro indirizzo IP dietro il firewall. Il solito caso d'uso per questo sarebbe quello di eseguire il server OpenVPN sulla porta tcp/443 lasciando che OpenVPN consegni il traffico HTTPS a un server web al posto di una porta forward.

Spesso su reti bloccate, solo porte come 80 e 443 saranno consentite per motivi di sicurezza e l'esecuzione di istanze Open-VPN su queste porte consentite può aiutare gli utenti a uscire in situazioni in cui l'accesso potrebbe altrimenti essere limitato.

Per impostarlo, configurare un server OpenVPN in ascolto sulla porta TCP 443 e aggiungere una regola firewall per passare il traffico all'indirizzo IP della WAN o al VIP utilizzato per OpenVPN sulla porta 443. Per passare il traffico all'"IP interno non sono necessarie ulteriori regole della porta forward o del firewall.

Nelle opzioni personalizzate dell'istanza OpenVPN, aggiungere quanto segue:

port-share x.x.x.x 443

Dove x.x.x.x è l'indirizzo IP interno del server web a cui verrà inoltrato il traffico non VPN.

Ora, se un client OpenVPN è puntato sull'indirizzo pubblico, si connetterà e funzionerà correttamente, e se un browser Web è puntato sullo stesso indirizzo IP, sarà collegato al server web.

Nota: ciò richiede l'utilizzo di TCP e può comportare prestazioni VPN ridotte.

18.2.19 Controllo dei parametri del client tramite RADIUS

Quando si utilizza RADIUS come sorgente di autenticazione per una VPN, Firew4LL supporta la ricezione di alcuni parametri di configurazione del client dal server RADIUS come attributi di risposta. È possibile specificare i seguenti valori:

Cisco-AVPair inacl= Le regole del firewall in entrata per governare il traffico dal client al server. Dato in formato ACL in stile Cisco (ad esempio Permettere tcp da qualsiasi a qualsiasi) le maschere d sottorete sono specificate in stile wildcard.

Cisco-AVPair outacl= Le regole del firewall in uscita per governare il traffico dal server al client. Formattato come il parametro **inacl**.

Server del DNS di Cisco-AVPair= Server DNS da spingere al client. Possono essere specificati più server, valutati in base agli spazi.

Route di Cisco-avpair= Istruzioni di route aggiuntive da inviare al client. Specificate come x.x.x.x y.y.y.y dove il primo parametro è un indirizzo di rete e il secondo è una maschera di sottorete.

Indirizzo IP del frame= l'indirizzo IP da assegnare al client. Quando si utilizza una **topologia** di stile *sottorete*, il server RADIUS deve anche inviare una maschera del frame impostata in modo appropriato per la rete del tunnel della VPN. Quando si utilizza una **topologia** di stile *net30*, il client riceve questo indirizzo IP e il lato server è impostato come un indirizzo IP inferiore all'indirizzo fornito al client.

18.2.20 Risoluzione dei problemi OpenVPN

Se si riscontrano problemi durante il tentativo di utilizzare OpenVPN, consultare questa sezione per informazioni sulla risoluzione dei problemi più comuni.

Controllare lo stato di OpenVPN

Il primo posto dove guardare è **Stato>OpenVPN**. Lo stato della connessione per ogni VPN è mostrato lì. Se una VPN è collegata, è in attesa, si sta riconnettendo, ecc, sarebbe indicato su quella schermata. Per ulteriori informazioni, vedere *Controllo dello stato dei client e dei server OpenVPN*.

Controllare il registro del firewall

Se una connessione VPN non si stabilisce o si stabilisce ma non passa il traffico, controllare i registri del firewall in **Stato>Registri di sistema** nella scheda **Firewall**. Se il traffico per il tunnel stesso viene bloccato, ad esempio il traffico verso l'indirizzo IP della WAN sulla porta 1194, regolare di conseguenza le regole del firewall WAN. Se il traffico è bloccato sull'interfaccia OpenVPN, aggiungere regole alla scheda **OpenVPN** per consentire il traffico lì.

Alcuni host funzionano, ma non tutti

Se il traffico tra alcuni host sulla VPN funziona correttamente, ma alcuni host non lo fanno, la causa è di solito una di queste quattro cose.

Gateway predefinito mancante, errato o ignorato Se il dispositivo non ha un gateway predefinito o ne ha uno che punta a qualcosa di diverso da Firew4LL, non sa come tornare correttamente alla rete remota sulla VPN. Alcuni dispositivi, anche con un gateway predefinito specificato, non utilizzano quel gateway. Questo è stato visto su vari dispositivi incorporati, tra cui telecamere IP e alcune stampanti. Non c'è nulla che possa essere fatto al riguardo oltre a far riparare il software del dispositivo. Questo può essere verificato eseguendo una cattura dei pacchetti sull'interfaccia interna del firewall collegato alla rete contenente il dispositivo. La risoluzione dei problemi con tcpdump è coperta in *Utilizzo di tcpdump dalla riga di comando*. Se il traffico viene visto lasciare l'interfaccia interna sul firewall, ma nessuna risposta ritorna, il dispositivo non sta instradando correttamente il suo traffico di risposta o sta potenzialmente bloccandolo tramite firewall locale sul dispositivo

Maschera di sottorete non corretta Se la sottorete in uso su un'estremità è 10.0.0.0/24 e l'altra è 10.254.0.0/24, e un host ha una maschera di sottorete errata di 255.0.0.0 or /8, non sarà mai in grado di comunicare attraverso la VPN perché pensa che la sottorete VPN remota faccia parte della rete locale e quindi il routing non funzionerà correttamente.

Firewall dell'host Se c'è un firewall sull'host di destinazione, potrebbe non consentire le connessioni.

Regole del firewall su |firew4ll| Assicurarsi che le regole su entrambe le estremità consentano il traffico di rete desiderato.

Controllare i registri OpenVPN

Passare a **Stato>Registri di sistema** e fare clic sulla scheda **OpenVPN** per visualizzare i registri OpenVPN. Al momento della connessione, OpenVPN registrerà messaggi simili al seguente esempio:

openvpn[32194]: UDPv4 link remote: 1.2.3.4:1194 openvpn[32194]: Peer Connection Initiated with 192.168.110.2:1194 openvpn[32194]: Initialization Sequence Completed

---

Nota: il numero seguente openvpn sarà diverso, è l'ID del processo di OpenVPN che crea la connessione.

Se i messaggi *inizializzati dalla connessione remota del peer* e del *link da remoto* non vengono visualizzati quando si tenta la connessione, è probabile che la causa sia una configurazione del client errata, quindi il client non sta connettendosi al server corretto o le regole firewall errate bloccano la connessione del client.

Garantire che nessuna connessione IPsec sia sovrapposta

A causa del modo in cui IPSec si lega al kernel di FreeBSD, qualsiasi connessione IPsec abilitata che corrisponde alle sottoreti locali e remoti che esiste quando IPsec è abilitato (anche se non è attivo) farà sì che il traffico non venga mai instradato attraverso la connessione OpenVPN. Tutte le connessioni IPsec che specificano le stesse reti locali e remote devono essere disabilitate. Se un tunnel IPsec è stato recentemente disabilitato o rimosso, controllare che le sue voci SPD siano state rimosse guardando **Stato>IPsec** nella scheda **SPD**. Se sono presenti, rimuoverle da quella schermata.

Controllare la tabella di routing del sistema

Passare a **Diagnostica>Route** e rivedere i percorsi noti dal firewall. Per le VPN con sito-a-sito, saranno presenti percorsi per le reti remote all'interfaccia *tun* o *tap* appropriata. Se i percorsi sono mancanti o errati, la **rete locale**, la **rete remota** o le opzioni personalizzate non sono configurate correttamente. Se è in uso una configurazione con chiave condivisa e non PKI, assicurarsi che i comandi" push » non vengano utilizzati.

Provare da diversi punti di osservazione

Se la connessione sembra essere attiva per il registro, ma non funziona dalla LAN, provarla dal firewall stesso. Questi test possono essere facilmente eseguiti utilizzando la pagina **Diagnostica>Ping** sul firewall.

Prima di tutto testare l'utilizzo dell'interfaccia interna usata per le connessioni del traffico interno OpenVPN (in genere LAN) come sorgente del ping. Se ciò non funziona, riprovare a utilizzare l'indirizzo sorgente *predefinito* in modo che il firewall fornisca il ping dall'interfacci della OpenVPN stessa.

Se il ping *predefinito* funziona ma il ping di rete interno non lo fa, controllare le regole e i percorsi del firewall sul lato opposto.

1. **Tracciare il traffico con la cattura dei pacchetti**

L'utilizzo della cattura di pacchetti per determinare dove il traffico sta o non sta scorrendo è una delle tecniche di risoluzione dei problemi più utili. Iniziare con l'interfaccia interna (comunemente LAN) sul lato in cui viene avviato il traffico, passare all'interfaccia *tun* su quel firewall, quindi all'interfaccia *tun* sul firewall remoto e infine all'interfaccia interna sul firewall remoto. Determinare dove si vede il traffico e dove non si vede può aiutare notevolmente a restringere dove si trova il problema. La cattura dei pacchetti è coperta in dettaglio in *Cattura dei pacchetti*.

Le route non verranno inviate a un client

Quando si tenta di utilizzare l'impostazione di **rete locale** o un'istruzione push per inviare i percorsi a un client e il client non li riceve correttamente, potrebbero accadere un paio di cose:

- **Verificare che una configurazione del server SSL/TLS sia utilizzata** con una **rete del tunnel** più grande di a /30. La modalità server in OpenVPN ha effetto solo quando si utilizza una sottorete abbastanza grande da contenere più client, ad esempio a /24.
- **Se il client è in esecuzione su Windows 10 o simili, provare a** eseguire il client come amministratore. Alcune versioni del client OpenVPN richiedono la modalità amministratore per applicare i percorsi alla tabella di routing del PC del client.
- **Quando si utilizza una configurazione con chiave condivisa, spingere** i percorsi non funzionerà. Utilizzare le caselle di **rete remota** o le dichiarazione della route su ciascun lato (sia client che server) per indirizzare il traffico verso sottoreti sull'altra estremità del tunnel.

Perché non posso eseguire il ping di alcuni indirizzi dell'adattatore di OpenVPN?

In modalità server SSL/TLS che utilizza una **topologia** di stile *net30*, OpenVPN non risponderà al ping su determinati indirizzi virtuali utilizzati esclusivamente per il routing degli endpoint. Non fare affidamento sul ping degli indirizzi degli endpoint OpenVPN come mezzo per determinare se il tunnel sta passando correttamente il traffico. Invece, effettuare il ping di qualcosa nella sottorete remota, come l'indirizzo IP LAN del server.

Nota: Questo non è rilevante quando si utilizza una **topologia** di stile *sottorete*

Secondo la parte «*FAQ sulla OpenVPN*»_, nella sezione intitolata *Perché l'opzione "ifconfig-pool" di OpenVPN utilizza una sottorete /30 (4 indirizzi IP privati per client) quando viene utilizzata in modalità tun?:*

Poiché 192.168.1.5 è solo un indirizzo IP virtuale all'interno del server OpenVPN, utilizzato come endpoint per le route, OpenVPN non si preoccupa di rispondere ai ping su questo indirizzo, mentre 192.168.1.1 è un vero indirizzo IP nei server O/S, quindi risponderà ai ping.

Questo può sembrare un po" contro-intuitivo, poiché sul server di ifconfig in uscita è simile a:

tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500 inet6 fe80::202:b3ff:fe03:8028%tun0 prefixlen 64 scopeid 0xc inet 192.168.100.1 –> 192.168.100.2 netmask 0xffffffff Opened by PID 27841

Mentre il client mostra:

tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> metric 0 mtu 1500 inet6 fe80::202:b3ff:fe24:978c%tun0 prefixlen 64 scopeid 0xa inet 192.168.100.6 –> 192.168.100.5 netmask 0xffffffff Opened by PID 1949

In questo caso,.5 o.1. probabilmente non risponderanno al *ping*. L'indirizzo .5 non risponderà perché si tratta di un indirizzo virtuale, e .1 perché non c'è un percorso per raggiungerlo direttamente. Gli indirizzi .5 e .6 fanno parte di un /30 che va da .7, e tentare il ping di .1 andrebbe invece fuori il percorso predefinito.

Ci sono molti casi in cui il lato più lontano di un tunnel OpenVPN risponderà al ping, ma non al locale. Questo è anche contro-intuitivo, ma funziona soprattutto nei casi in cui è presente un link con sito-a-sito. Se il server mostra i suoi indirizzi tun come x.x.x.1 -> x.x.x.2 e il client mostra il contrario x.x.x.2 -> x.x.x.1, allora il lontano risponderà al ping da entrambe le estremità.

Impossibile instradare i client in un tunnel con sito-a-sito per SSL/TLS

Se viene utilizzato un tunnel con sito-a-sito SSL/TLS e tutti i percorsi appaiono corretti ma il traffico non può ancora fluire correttamente, controllare la dimensione della rete del tunnel. Se si tratta di una configurazione con sito-a-sito tra solo due posizioni, la rete del tunnel dovrebbe essere a /30 in modo che non richieda istruzioni iroute per raggiungere le reti client. Per ulteriori informazioni, consultare la nota sulla *Rete del tunnel con IPv4/IPv6*. Quando si collegano più siti a una singola istanza del server, controllare la configurazione in base a *Configurazione di esempio di sito-a-sito (SSL/TLS),* in particolare le sostituzioni e le iroute specifici del client.

La voce iroute di Override specifica del Client sembra non avere alcun effetto

Quando si imposta una configurazione PKI di OpenVPN con sito-a-sito, è necessario configurare un'istruzione iroute utilizzando i campi di **Rete remota** nella voce **Override specifica del client** impostata per il nome comune del certificato del client.

Innanzitutto, assicurarsi che il **Nome comune** corrisponda al certificato e che il percorso interno venga appreso/aggiunto come previsto. Potrebbe essere necessario aumentare la verbosità del registro in OpenVPN (cioè *verbosità 10* nelle opzioni personalizzate) per vedere se funziona.

Inoltre, per ogni rete utilizzata in un client specifico la voce **Rete remota con l'override specifico del client** (iroute), è necessaria anche una **Rete remota** (route) nel server. Le definizioni di **Rete remota** (route) nelle impostazioni del server consentono al sistema operativo del firewall di sapere che le reti verranno indirizzate a OpenVPN da qualsiasi altra parte. Le opzioni della **Rete remota** (iroute) sulla voce di **Override specifica del client** sono interne a OpenVPN in modo che sappiano quali reti vengono instradate per un certificato specifico.

Perché i client OpenVPN ottengono tutti lo stesso indirizzo IP?

Se lo stesso certificato viene utilizzato per tutti i client, che scoraggiamo fortemente, ai client viene assegnato lo stesso indirizzo IP quando si connettono. Per aggirare questo problema, controllare **Duplicare le connessioni** nella configurazione del server.

Importazione dei parametri DH OpenVPN

Quando si importa una configurazione OpenVPN esistente in Firew4LL, non è necessario importare i parametri DH. I parametri DH non sono specifici per una determinata configurazione nel modo in cui sono ottenuti i certificati o chiavi.

Per dirla semplicemente, i parametri DH sono alcuni bit extra di casualità che aiutano durante il processo di scambio delle chiavi. Non devono corrispondere su entrambi i lati del tunnel, e quelli nuovi possono essere fatti in qualsiasi momento. Non è necessario importare un set esistente di parametri DH.

Nota: per impostazione predefinita, Firew4LL utilizza una serie di parametri DH pre-generati. Un nuovo set può essere generato manualmente se lo si desidera, vedere *Lunghezza dei parametri DH* per i dettagli.

OpenVPN è una soluzione VPN con SSL di open source che può essere utilizzata per client di accesso remoto e con connettività sito-a-sito. OpenVPN supporta i client su una vasta gamma di sistemi operativi, tra cui tutti i BSD, Linux, Android, Mac OS X, iOS, Solaris, Windows 2000 e versioni successive, e anche alcuni telefoni VoIP.

Ogni connessione OpenVPN, sia di accesso remoto o sito-a-sito, è costituita da un server e un client. Nel caso di VPN sito-a-sito, un firewall funge da server e l'altro da client. Non importa quale firewall possieda questi ruoli. In genere, la posizione del firewall primario fornirà la connettività del server per tutte le posizioni remote, i cui firewall sono configurati come client. Questo è funzionalmente equivalente alla configurazione opposta alla posizione primaria impostata come client che si connette ai server in esecuzione sui firewall nelle posizioni remote. In pratica, i server vengono quasi sempre eseguiti in una posizione centrale.

Esistono diversi tipi di metodi di autenticazione che possono essere utilizzati con OpenVPN: chiave condivisa, X. 509 (noto anche come SSL/TLS o PKI), autenticazione utente tramite locale, LDAP e RADIUS o una combinazione di X.509 e autenticazione utente. Per la chiave condivisa, viene generata una singola chiave che verrà utilizzata su entrambi i lati. SSL/TLS prevede l'utilizzo di un set attendibile di certificati e chiavi. L'autenticazione dell'utente può essere configurata con o senza SSL/TLS, ma il suo utilizzo è preferibile dove possibile a causa della maggiore sicurezza offerta.

Le impostazioni per un'istanza OpenVPN sono trattate in questo capitolo, nonché l'esecuzione della procedura guidata del server di accesso remoto di OpenVPN, le configurazioni dei client ed esempi di più scenari di connessione sito-a-sito.

Nota: sebbene OpenVPN sia una VPN con SSL, non è una VPN con SSL "senza client" nel senso dato dai fornitori di firewall commerciali. Il client OpenVPN deve essere installato su tutti i dispositivi client. In realtà nessuna soluzione VPN è veramente «senza client», e questa terminologia non è altro che uno stratagemma di marketing. Per una discussione più approfondita sulle VPN con SSL, questo post di Matthew Grooms, uno sviluppatori di strumenti per IPsec e Firew4LL, negli archivi dell'elenco mail fornisce alcune informazioni eccellenti.

Per la discussione generale dei vari tipi di VPN disponibili in Firew4LL e dei loro pro e contro, vedere *Reti private virtuali.*

Vedi anche:

Per ulteriori informazioni, è possibile accedere all'archivio degli Hangouts per visualizzare l'Hangout di settembre 2014 sui concetti di OpenVPN avanzati e l'Hangout di settembre 2015 sulle VPN di accesso remoto

18.2.21 OpenVPN e certificati

L'utilizzo dei certificati è il mezzo preferito per eseguire le VPN di accesso remoto, poiché consente di revocare l'accesso per le singole macchine. Con le chiavi condivise, è necessario creare un server e una porta univoci per ciascun client o distribuire la stessa chiave a tutti i client. Il primo diventa un incubo di gestione, e il secondo è problematico nel caso di una chiave compromessa. Se una macchina client viene compromessa, rubata o persa o altrimenti deve essere revocata, la chiave condivisa deve essere nuovamente rilasciata a tutti i client. Con una distribuzione PKI, se un client è compromesso o l'accesso deve essere revocato per qualsiasi altro motivo, è sufficiente revocare il certificato del client. Nessun altro cliente è interessato.

La GUI di Firew4LL include un'interfaccia di gestione dei certificati completamente integrata con OpenVPN. Le autorità di certificazione (CA) e i certificati server sono gestiti in Gestione dei certificati nell'interfaccia web, situata in **Gestione dei certificati di sistema**. I certificati utente vengono gestiti anche nell'interfaccia web, come parte della gestione utente integrato presente in **Sistema>Gestione degli utenti**. I certificati possono essere generati per qualsiasi account utente creato localmente sul firewall ad eccezione dell'account dell'amministratore predefinito. Per ulteriori informazioni sulla creazione di un'autorità di certificazione, certificati e elenchi di revoca dei certificati, vedere *Gestione dei certificati*.

18.3 L2TP

18.3.1 Regole del firewall e L2TP

Per impostazione predefinita, quando il server L2TP è abilitato, le regole del firewall non verranno aggiunte automaticamente all'interfaccia scelta per consentire la porta UDP *1701*. Una regola del firewall deve essere aggiunta a qualsiasi interfaccia che il traffico L2TP inserirà, in genere WAN, WAN contenente il gateway predefinito, o IPsec.

18.3.2 L2TP e MultiWAN

L2TP utilizza la porta UDP 1701. Poiché L2TP si basa su UDP, il server potrebbe avere problemi con qualsiasi WAN che non sia il gateway predefinito. Il demone risponderà dal firewall utilizzando l'indirizzo più vicino al client, seguendo la tabella di routing, che è la WAN con il gateway predefinito per i client remoti.

18.3.3 Configurazione del server con L2TP

Per utilizzare L2TP, prima passare a **VPN>L2TP**. Selezionare **Abilitare il server L2TP**.

Interfaccia

L'impostazione dell"**interfaccia** controlla dove il demone L2TP legherà e ascolterà le connessioni. Questa è in genere l'interfaccia *WAN* che accetta le connessioni in entrata.

Indirizzamento dell'IP

Prima di iniziare, determinare quali indirizzi IP utilizzare per il server L2TP e i client e quanti client simultanei supportare.

Indirizzo del server Un indirizzo IP *non utilizzato* al di fuori dell"**intervallo di indirizzi remoti**, ad esempio 10.3.177.1 come mostrato nella figura *Indirizzamento dell'IP di L2TP*.

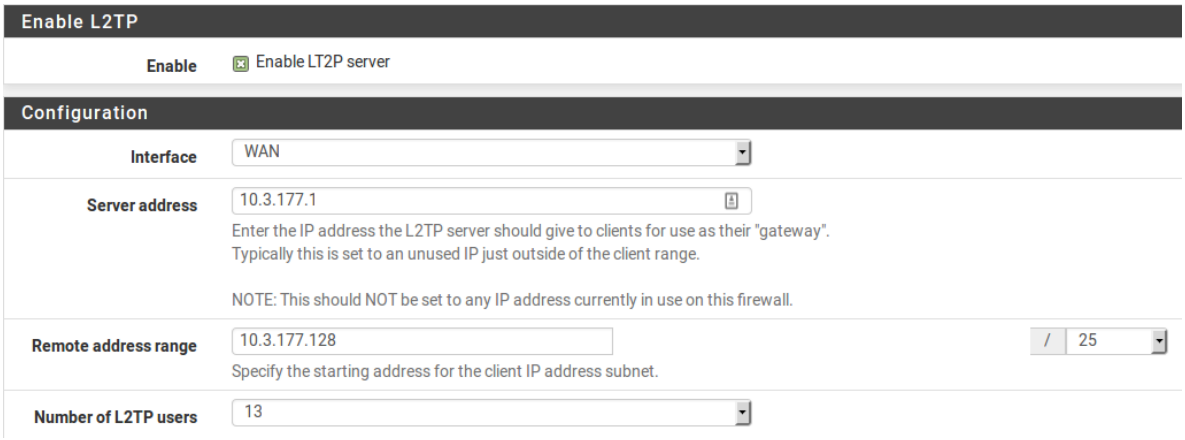


Fig. 1: Indirizzamento dell'IP di L2TP

Intervallo di indirizzi remoti Di solito una sottorete nuova e inutilizzata, come 10.3.177.128 / 25 (.128 fino a .255). Questi sono gli indirizzi da assegnare ai client quando si connettono.

Numero di utenti L2TP Controllare quanti utenti L2TP potranno connettersi contemporaneamente, in questo esempio *16* è stato selezionato.

I server DNS possono anche essere definiti per gli utenti finali quando necessario. Compilare i campi del server** DNS su L2TP **primario** e ** secondario con gli indirizzi IP del server DNS per la connessione dei client.

Autenticazione

Segreto Richiesto da alcune implementazioni L2TP, simile a una password di gruppo o chiave precondivisa. Il supporto per questo varia da client a client. Lasciare il campo vuoto a meno che non sia noto per essere richiesto. Se necessario, inserire e confermare il segreto.

Tipo di autenticazione Decide tra L'autenticazione *PAP*, *CHAP* o *MS-CHAPv2* per gli utenti. Il supporto per questo può variare da client a client e può anche dipendere dal server RADIUS. I tipi basati su *CHAP* sono più sicuri, ma *PAP* è più ampiamente compatibile.

Gli utenti possono essere autenticati dal database dell'utente locale o tramite un server RADIUS esterno. Questo può essere usato per autenticare gli utenti L2TP dalla Directory attiva di Microsoft (vedere *Autenticazione RADIUS con il server di Windows*) così come numerosi altri server in grado RADIUS.

Se si utilizza RADIUS, selezionare la casella **Usare un server RADIUS per l'autenticazione** e compilare il server RADIUS e il segreto condiviso. Un secondo server RADIUS può anche essere aggiunto nel caso in cui il primo fallisca. Per l'autenticazione che utilizza il database dell'utente locale, lasciare la casella deselezionata. Gli utenti devono essere aggiunti manualmente nella scheda **utenti** della schermata **VPN>L2TP** a meno che non si utilizzi RADIUS. Vedere *Aggiungere utenti* qui sotto per maggiori dettagli sul sistema di autenticazione integrato.

Salvare le modifiche per avviare il server L2TP

Dopo aver compilato gli elementi di cui sopra, fare clic su **Salvare**. Ciò salverà la configurazione e avvierà il server L2TP.

Configurare le regole del firewall per i client L2TP

Passare a **Firewall>Regole** e fare clic sulla scheda **VPN su L2TP**. Queste regole controllano il traffico dai client L2TP. Fino a quando non è stata aggiunta una regola firewall per consentire il traffico, tutto il traffico avviato dai client L2TP connessi verrà bloccato. Il traffico avviato dai client LAN a L2TP viene controllato utilizzando le regole del

firewall della LAN. Inizialmente una regola permettere tutto può essere desiderata qui per scopi di test come mostrato nella figura *Regola del firewall della VPN su L2TP* e, una volta verificata la funzionalità, limitare il set di regole come desiderato.

Nota: ricordare che una regola deve essere aggiunta all'interfaccia che riceve il traffico L2TP, in genere WAN o IPsec, per passare UDP al firewall con una porta di destinazione di 1701.

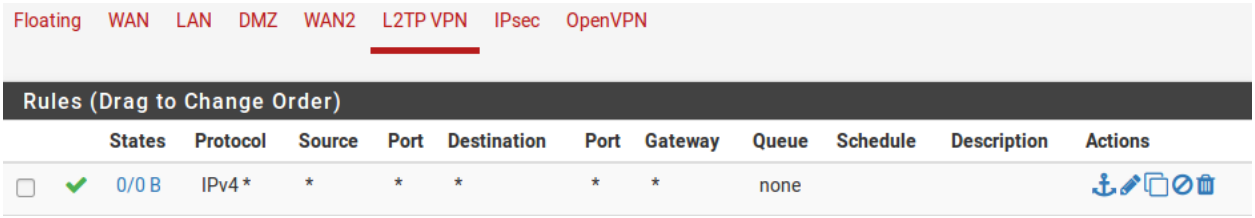


Fig. 2: Regola del firewall della VPN su L2TP

Aggiungere utenti

L'aggiunta di utenti al sistema per gli utenti di L2TP integrato è semplice. Per aggiungere utenti locali:

- Passare a **VPN>L2TP**, scheda **Utenti**. Verrà presentata la schermata utenti come mostrato nella figura *Scheda degli utenti di L2TP*.
- Fare clic su Aggiungere per mostrare il modulo utilizzato per aggiungere utenti.

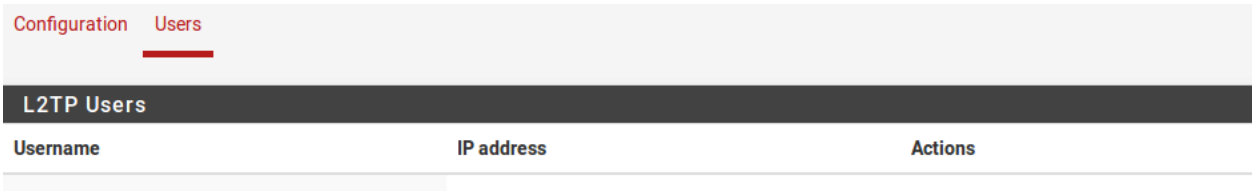


Fig. 3: Scheda degli utenti di L2TP

- Immettere il nome utente, la password e confermare la password per un utente, come in figura *Aggiungere un utente di L2TP*.
- Immettere un'**assegnazione IP** statici se lo si desidera.

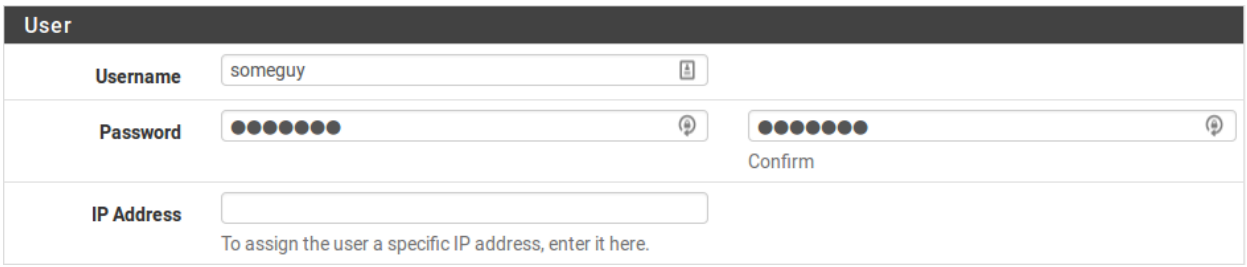


Fig. 4: Aggiungere un utente di L2TP

- **Fare clic su Salvare, quindi verrà restituito l'elenco degli** utenti.
- Ripetere il processo per ogni utente da aggiungere.

Per modificare un utente esistente, fare clic su . Gli utenti possono essere eliminati cliccando su .

18.3.4 L2TP con IPsec

Nelle versioni attuali di Firew4LL, L2TP / IPsec può essere configurato per i client mobili, anche se non è una configurazione che consigliamo.

Come avvertito all'inizio del capitolo, il client Windows, tra gli altri, e il demone IPSec di strongSwan non sono sempre compatibili, portando in molti casi al fallimento. Si consiglia vivamente di utilizzare un'altra soluzione come IKEv2 invece di L2TP/IPsec.

Vedi anche:

Esempio di configurazione del server IKEv2 contiene una procedura dettagliata per la configurazione di IKEv2.

Prima di configurare la porzione IPsec, impostare il server L2TP come descritto nella *Configurazione del server L2TP* e aggiungere utenti, regole del firewall, ecc..

Configurazione di IPsec

Queste impostazioni sono state testate e trovate adatte per funzionare con alcuni client, ma altre impostazioni simili potrebbero anche funzionare. Sentirsi liberi di provare altri algoritmi di crittografia, hash, ecc.

Scheda dei client mobili

- Passare alla scheda **VPN>IPsec**, nella scheda **Client mobili** su Firew4LL
- Controllare **Abilitare il supporto dei client mobili di IPsec**
- Impostare **Autenticazione utente** sul *Database locale* (non utilizzato, ma l'opzione deve avere qualcosa selezionato)
- Deselezionare **Fornire un indirizzo IP virtuale ai client**
- Deselezionare **Fornire un elenco di reti accessibili ai client**
- Fare click su **Salvare**

Phase 1

- Fare click sul pulsante **Creare la fase1** in alto se appare o modificare la fase 1 di IPsec per dispositivi mobileiesistente
  - Se non c'è nessuna fase 1 e il pulsante **Creare la fase1** non viene visualizzato, tornare alla scheda **Client mobili** e fare click lì.
- Impostare **Versione di scambio di chiavi** su *v1*
- Inserire una **Descrizione** appropriate
- Impostare **Metodo di autenticazione** su *PSK reciproco*
- Impostare **Modalità di negoziazione** per *Principale*
- Impostare **Mio identificatore** su *Mio indirizzo IP*
- Impostare **Algoritmo di crittografia** su *AES 256*
- Impostare **Algoritmo hash** su *SHA1*
- Impostare **Gruppo di chiavi DH** su *14 (2048 bit) *

Nota: iOS e altre piattaforme potrebbero invece funzionare con un **gruppo di chiavi DH** di *2*.

- Impostare **Durata di vita** su 28800
- Deselezionare Disabilitare Rekey
- Impostare **Attraversamento del NAT** su *Automatico*
- Controllare **Abilitare DPD**, impostare per *10* secondi e *5* tentativi
- Fare click su **Salvare**

Phase2 2

- Fare clic su **Mostrare voci di fase 2** per visualizzare l'elenco della fase 2 di IPsec per i dispositivi mobili
- Fare clic su  **Aggiungere P2** per aggiungere una nuova voce di fase 2 se non esiste o fare click su  per modificare una voce esistente
- Impostare **Modalità** su **Trasporto**
- Inserire una **Descrizione** appropriata
- Impostare **Protocollo** su *ESP*
- Impostare **Algoritmi di crittografia** su *AES 128*
- Impostare **Algoritmi hash** su *SOLO SHA1*
- Impostare **Gruppo di chiavi PFS** su *off*
- Impostare **Durata di vita** su 3600
- Fare click su **Salvare**

Pre-Shared Key

La chiave pre-condivisa per la connessione, comune a tutti i client, deve essere configurata in modo speciale.

- Passare a **VPN>IPsec**, scheda **Pre-Shared Key** su Firew4LL
- Fare clic su  **Aggiungere** per aggiungere un nuovo PSK
- Impostare **Identificatore** su tutti gli utenti

Nota: il nome tutti gli utenti è una parola chiave speciale utilizzata da Firew4LL per configurare un PSK wildcard, che è necessario a L2TP/IPsec per funzionare. Non utilizzare altri **Identificatori** per questo PSK!

- Impostare **Tipo di segreto** su *PSK*
- Inserire una **Chiave pre-condivisa**, come aaabbbbccc – idealmente una molto più lunga, più casuale, e sicura!
- Fare click su **Salvare**
- Fare click su **Applicare le modifiche**

Regole del firewall di IPsec

Le regole del firewall sono necessarie per passare il traffico dall'host del client su IPsec per stabilire il tunnel L2TP e all'interno di L2TP per passare il traffico VPN con il tunnel effettivo ai sistemi attraverso la VPN. L'aggiunta delle regole L2TP è stata coperta nella sezione precedente. Per aggiungere regole IPsec:

- Passare a **Firewall>Regole**, scheda **IPsec**
- Rivedere le regole attuali. Se esiste una regola di stile «Consentire tutto», non è necessario aggiungerne un'altra. Continuare con l'attività successiva.
- Fare clic su  **Aggiungere** per aggiungere una nuova regola alla parte superiore dell'elenco
- Impostare **Protocollo** su *Qualsiasi*
- Impostare la **Sorgente** e la **Destinazione** su *Qualsiasi*

Nota: questo non deve far passare tutto il traffico, ma deve almeno far passare L2TP (porta UDP 1701) all'indirizzo IP della WAN del firewall.

- Fare clic su **Salvare**
- Fare click su **Applicare le modifiche**

18.3.5 Configurazione DNS

Se i server DNS vengono forniti ai client e viene utilizzato il **risolutore del DNS** non associato, la sottorete scelta per i client di L2TP deve essere aggiunta all'elenco di accesso.

- Passare a **Servizi>Risolutore del DNS**, scheda **Elenchi di accesso**
- Fare clic su  **Aggiungere** per aggiungere un nuovo elenco di accesso
- Immettere un **Nome dell'elenco di accesso**, ad esempio come *Utenti VPN*
- Impostare **Azione** su *Consentire*
- Fare clic su  **Aggiungere rete** in **Reti** per aggiungere una nuova rete
- Immettere la sottorete del client di VPN nella casella della **Rete**, ad esempio 10.3.177.128
- Scegliere il **CIDR** corretto, ad esempio 25
- Fare click su **Salvare**
- Fare click su **Applicare le modifiche**

Configurazione client

Quando si configurano i client, ci sono alcuni punti da cercare:

- Assicurarsi che la configurazione del sistema operativo del client sia impostata per connettersi all'indirizzo esterno corretto per la VPN.
- Potrebbe essere necessario forzare il tipo di VPN a **L2TP/IPsec** sul client se ha una modalità automatica.
- Il tipo di autenticazione del client deve corrispondere a quello configurato sul server L2TP (ad es. *CHAP*)

18.3.6 Risoluzione dei problemi con L2TP

Questa sezione copre i passaggi di risoluzione dei problemi più comuni che gli utenti incontrano con L2TP.

Impossibile connettersi

Verificare che le regole del firewall siano state aggiunte all'interfaccia esterna in cui il traffico L2TP entra nel firewall. Assicurarsi inoltre che il client si connetta all'indirizzo IP dell'interfaccia scelto nelle impostazioni L2TP.

Connesso a L2TP ma non lascia passare il traffico

Assicurarsi che le regole del firewall siano state aggiunte all'interfaccia **VPN su L2TP** come descritto in *Configurare le regole del firewall per i client L2TP*.

Assicurarsi inoltre che la sottorete remota attraverso la VPN sia diversa dalla sottorete locale. Non è possibile raggiungere una rete 192.168.1.0/24 attraverso la VPN quando la sottorete locale in cui risiede il client è anche 192.168.1.0/24, il traffico destinato a quella sottorete non attraverserà mai la VPN perché è sulla rete locale. Questo è il motivo per cui è importante scegliere una sottorete LAN relativamente oscura quando si utilizza una VPN.

La connessione non riesce con un client di Windows

Se il livello IPsec sembra essere completato, ma nessun traffico L2TP passa, è probabile che sia nota un'incompatibilità tra Windows e il demone di strongSwan utilizzato su Firew4LL. Al momento non esiste una soluzione nota se non spostare il sistema Windows da dietro il NAT o utilizzare una VPN di stile diverso come IKEv2.

Traffico L2TP bloccato in uscita

In alcuni casi, ad esempio quando combinato con IPsec, il traffico L2TP può anche richiedere una gestione speciale tramite regole dinamiche. Viene visualizzato come traffico bloccato nella direzione *in uscita* nei log del firewall, che mostra un'interfaccia server di L2TP.

Se ciò accade, aggiungere una regola dinamica come segue:

- Passare a **Firewall>Regole**, scheda **dinamiche**
- Fare clic su  **Aggiungere** per aggiungere una nuova regola alla parte superiore dell'elenco
- Impostare **Azione** su *Passare*
- Selezionare **Rapido**
- Selezionare *VPN su L2TP* per l'**interfaccia**
- Impostare **Direzione** su *In uscita*
- Impostare **Protocollo** su *TCP*
- Impostare **Sorgente/Destinazione** in base alle esigenze o impostare su *Qualsiasi*
- Funzioni avanzate: - Impostare le **Flag di TCP** a *Qualsiasi flag* - Imposta il **Tipo di stato** in *Stato sloppy*

18.3.7 L2TP Log

Una registrazione per gli eventi di login e logout viene mantenuto su **Stato>Registri di sistema**, nella scheda **VPN**, sotto gli **Accessi a L2TP**.

Ogni login e logout viene registrato con un timestamp e un nome utente, e ogni login mostrerà anche l'indirizzo IP assegnato al client L2TP. Il registro completo può essere trovato nella scheda **L2TP grezzo**.

Firew4LL può fungere da server VPN su L2TP. L2TP è puramente un protocollo del tunnel che non offre alcuna crittografia propria, quindi è tipicamente combinato con qualche altra tecnica di crittografia, come Ipsec.

Avvertimento: supporta L2TP/IPsec, tuttavia, alcuni client non funzioneranno correttamente in molti comuni scenari. Lo scenario di problema più comune è un client di Windows dietro il NAT, in tal caso il client Windows e il demone IPSec di strongSwan non sono pienamente compatibili, il che porta al fallimento. In queste situazioni, si consiglia di utilizzare invece IKEv2.

Vedi anche:

Esempio di configurazione del server per IKEv2 contiene una procedura dettagliata per la configurazione di IKEv2, che è una soluzione molto più flessibile.

Vedi anche:

Per la discussione generale dei vari tipi di implementazioni VPN disponibili in Firew4LL e dei loro pro e contro, vedere *Reti private virtuali*.

18.3.8 Avviso di sicurezza L2TP

L2TP da solo non è crittografato, quindi non è destinato al traffico privato. Alcuni dispositivi, come Android, offrono un client solo su L2TP che è in grado di connettersi a Firew4LL, ma dovrebbe essere utilizzato solo per il traffico che è già crittografato, o se il traffico non è considerato privato. Ad esempio, effettuare il tunnel del traffico Internet in modo che sembra provenire da un'altra posizione.

18.4 Scegliere una soluzione VPN

Ogni soluzione VPN ha pro e contro. Questa sezione tratterà le considerazioni principali nella scelta di una soluzione VPN, fornendo le informazioni necessarie per scegliere quella migliore per un dato ambiente.

18.4.1 Interoperabilità

Per interoperare con un firewall o un router prodotto da un altro fornitore, Ipsec è di solito la scelta migliore in quanto è incluso con quasi tutti i dispositivi con capacità VPN. Impedisce inoltre di essere bloccato in qualsiasi particolare firewall o soluzione VPN. Per la connettività da sito a sito interoperabile, Ipsec è di solito l'unica scelta. OpenVPN è interoperabile con poche altre soluzioni firewall/VPN, ma non molte. L'interoperabilità in questo senso non è applicabile ad altri tipi di VPN poiché non sono destinati ad applicazioni sita-a-sito.

18.4.2 Considerazioni sull'autenticazione

Nelle versioni attuali di Firew4LL, tutti i tipi di VPN supportano l'autenticazione utente. Ipsec e OpenVPN possono anche funzionare con chiavi o certificati condivisi. OpenVPN è un po" più flessibile in questo senso perché può funzionare solo con certificati, solo con chiavi condivise, solo con l'autenticazione dell'utente, o una combinazione

di questi. Utilizzare OpenVPN con i certificati, autenticazione TLS, e l'autenticazione dell'utente è il metodo più sicuro. I certificati OpenVPN possono anche essere protetti da password, nel qual caso un certificato compromesso da solo non è adeguato per la connessione a una VPN se è impostato per utilizzare solo i certificati. La mancanza di autenticazione aggiuntiva può essere un rischio per la sicurezza in quanto un sistema perso, rubato o compromesso contenente una chiave o un certificato significa che chi ha accesso al dispositivo può connettersi a una VPN fino a quando tale perdita viene scoperta e il certificato revocato.

Anche se non ideale, una mancanza di username e password di autenticazione su una VPN non è un grande rischio come può sembrare. Un sistema compromesso può facilmente avere un logger di chiave installato per catturare le informazioni di nome utente e password e facilmente sconfiggere tale protezione. Nel caso di sistemi persi o rubati contenenti chiavi, se il disco rigido non è crittografato, le chiavi possono essere utilizzate per connettersi. Tuttavia l'aggiunta di autenticazione password non è di grande aiuto nemmeno lì, come di solito lo stesso nome utente e password verranno utilizzati per accedere al computer, e la maggior parte delle password sono crackabili in pochi minuti utilizzando l'hardware moderno quando un utente malintenzionato ha accesso a un disco non criptato. La sicurezza delle password è spesso compromessa dagli utenti con note sul loro laptop o nel loro case del portatile con la password annotata. Come con qualsiasi implementazione di sicurezza, più livelli vengono utilizzati, meglio è, ma è sempre una buona idea mantenere questi livelli in prospettiva.

18.4.3 Facilità di configurazione

Nessuna delle opzioni VPN disponibili è estremamente difficile da configurare, ma ci sono differenze tra le opzioni:

- Ipsec ha numerose opzioni di configurazione e può essere difficile per i principianti.
- OpenVPN richiede l'uso di certificati per l'accesso remoto nella maggior parte degli ambienti, che viene fornito con la propria curva di apprendimento e può essere un po" difficile da gestire. Firew4LL include una procedura guidata per gestire le configurazioni di accesso remoto delle OpenVPN più comuni e i pacchetti di esportazione client delle OpenVPN facilitano il processo di attivazione dei client.

IPsec e OpenVPN sono opzioni preferibili in molti scenari per altri motivi discussi in questo capitolo.

18.4.4 MultiWAN

Se gli utenti richiedono la possibilità di connettersi a più WAN, sia IPsec che OpenVPN sono in grado di gestire tali configurazioni.

18.4.5 Disponibilità client

Il software VPN Client è un programma che gestisce la connessione alla VPN e la gestione di qualsiasi altra attività correlata come l'autenticazione, la crittografia, il routing, ecc. Per le VPN di accesso remoto, la disponibilità di software del client VPN è una considerazione primaria. Tutte le opzioni sono compatibili con la multipiattaforma con molti sistemi operativi diversi, ma alcuni richiedono l'installazione di client di terze parti. IPsec in modalità EAP-Mschapv2, IPsec in modalità EAP-TLS e IPsec in modalità Xauth sono le uniche opzioni con supporto del client integrato in alcuni popolari sistemi operativi desktop e mobili. Altri sistemi operativi variano e possono includere più o meno modalità IPsec o possono anche includere OpenVPN, come nel caso di molte distribuzioni Linux. Se l'utilizzo di client integrati è un must, consultare la documentazione del sistema operativo per tutte le piattaforme client richieste per vedere se è disponibile un'opzione comune e quindi controllare Firew4LL per vedere se tale modalità è possibile.

In alcuni casi possono essere necessarie più VPN di accesso remoto per ospitare tutti i client. Per esempio, IPsec potrebbe essere usato per alcuni e OpenVPN per altri. Alcune organizzazioni preferiscono mantenere le cose coerenti, quindi c'è un compromesso da fare, ma per motivi di compatibilità può valere la pena offrire più opzioni.

IPsec

I client Ipsec sono disponibili per Windows, Mac OS X, BSD, Linux e altri. Anche se i client nativi possono supportare solo determinate modalità e configurazioni specifiche. I client IPsec generici non sono inclusi nel sistema operativo, ad eccezione di alcune distribuzioni Linux e BSD. Una buona opzione gratuita per Windows è il client *Shrew Soft*. Mac OS X include sia Ikev2 e Ipsec supporto di Cisco (xauth). Ci sono opzioni gratuite e commerciali disponibili con una GUI facile da usare per gli utenti.

OSX 10.11, insieme a Windows 7 e successivi includono il supporto per Ipsec in modalità specifiche utilizzando Ikev2: EAP-TLS e EAP-Mschapv2. Entrambe le opzioni sono supportate da Firew4LL e sono coperte da *IPsec*.

Il client Ipsec in stile Cisco incluso con i dispositivi OS X e iOS è completamente compatibile con Firew4LL Ipsec utilizzando xauth. La configurazione per il client iOS è coperta dalla *configurazione del client di IKEv2 per iOS 9*.

Molti telefoni Android includono anche un client compatibile con Ipsec, che è discusso in *configurazione del client per IKEv2 con strongSwan per Android*.

OpenVPN

Openvpn ha client disponibili per Windows, Mac OS X, tutti i BSD, Linux, Solaris e Windows Mobile, ma il client non viene pre-installato in nessuno di questi sistemi operativi.

Android 4.x e i dispositivi successivi possono utilizzare un client OpenVPN disponibile gratuitamente che funziona bene e non richiede il rooting del dispositivo. Tale client è coperto in *Android 4.x e versioni successive*. Versioni precedenti di Android possono anche essere in grado di utilizzare OpenVPN tramite un client alternativo. Ci sono altre opzioni disponibili se il dispositivo è collegato alla root, ma questo è al di là della portata di questo libro.

iOS ha anche un client nativo OpenVPN. Per maggiori informazioni, vedere *iOS*.

Compatibilità con I firewall

I protocolli VPN possono causare difficoltà per molti firewall e dispositivi NAT. Questo è principalmente rilevante per la connettività con accesso a distanza, dove gli utenti saranno dietro una miriade di firewall per lo più controllati da terze parti con diverse configurazioni e funzionalità.

IPsec

Ipsec utilizza sia la porta UDP 500 che il protocollo ESP per funzionare. Alcuni firewall non gestiscono bene il traffico ESP dove è coinvolto il NAT, perché il protocollo non ha numeri di porta come TCP e UDP che lo rendono facilmente rintracciabile dai dispositivi NAT. I client IPsec dietro il NAT possono richiedere il funzionamento dell'attraversamento del NAT, che incapsula il traffico ESP sulla porta UDP 4500.

OpenVPN

OpenVPN è il più facile da usare per il firewall per le opzioni VPN. Poiché utilizza TCP o UDP e non è influenzato da alcuna funzione NAT comune come la riscrittura delle porte sorgente, è raro trovare un firewall che non funzioni con OpenVPN. L'unica difficoltà possibile è se il protocollo e la porta in uso siano bloccati. Alcuni amministratori usano una porta comune come UDP 53 (di solito DNS), o TCP 80 (di solito HTTP) o TCP 443 (di solito HTTPS) o per eludere la maggior parte dei filtri in uscita.

18.4.6 Protezione crittografica

Una delle funzioni fondamentali di una VPN è garantire la riservatezza dei dati trasmessi.

IPsec che utilizza chiavi pre-condivise può essere rotto se viene utilizzata una chiave debole. Utilizzare una chiave forte, almeno 10 caratteri di lunghezza con un mix di lettere, numeri e simboli maiuscoli e minuscoli. L'uso dei certificati è preferibile, anche se un po" più complicato da implementare.

La crittografia OpenVPN è compromessa se vengono divulgate le chiavi PKI o condivise, anche se l'uso di fattori multipli come l'autenticazione TLS in cima a PKI può mitigare alcuni dei pericoli.

18.4.7 Riepilogo

La tabella *Peculiarità e caratteristiche per tipo di VPN* mostra una panoramica delle considerazioni fornite in questa sezione.

Tabella 1: Peculiarità e caratteristiche per tipo di VPN

+==============-+=======================+================-+==========+====
==========+================-+ | Tipo di VPN | Client inclusi in OS | Interoperabile | MultiWan | Crittografia | Facile da usare | | | | | | | |
+"""""""""""""=+"""""""""""""""""""""""+"""""""""""""""=+"""""""""+"""""""""""""""+"""""""""""""""=+
| IPsec | Varia per la modalità | Si | Si | Si | No (senza NAT-T)| +==============-
+=======================+================-+==========+===============+================-
+ | Open-VPN | No | No | Si | Si | Si | +==============-+=======================+================-
+==========+===============+================-+

18.5 Regole di firewall e VPN

Le VPN e le regole del firewall sono gestite in modo incoerente in Firew4LL. Questa sezione descrive come vengono gestite le regole del firewall per ciascuna delle singole opzioni VPN. Per le regole aggiunte automaticamente discusse qui, l'aggiunta di tali regole può essere disabilitata selezionando **Disabilitare tutte le regole VPN aggiunte automaticamente** in **Sistema>Avanzate** nella scheda **Firewall/NAT**.

18.5.1 IPsec

Il traffico IPsec che entra nell'interfaccia WAN specificata è automaticamente permesso come descritto in IPsec. Il traffico incapsulato all'interno di una connessione IPsec attiva è controllato tramite regole definite dall'utente nella scheda **IPsec** in **Firewall>Regole**.

18.5.2 OpenVPN

OpenVPN non aggiunge automaticamente le regole alle interfacce WAN. La procedura guidata VPN per l'accesso remoto di OpenVPN offre la possibilità di creare opzionalmente regole per far passare il traffico WAN e il traffico sull'interfaccia OpenVPN. Il traffico incapsulato all'interno di una connessione OpenVPN attiva è controllato tramite regole definite dall'utente nella scheda **OpenVPN** in **Firewall>Regole**. Le interfacce OpenVPN possono anche essere assegnate in modo simile ad altre interfacce su Firew4LL. In questi casi si applicano ancora le regole del firewall della scheda OpenVPN, ma c'è una scheda separata specifica per l'istanza VPN assegnata che controlla il traffico solo per quella VPN.

18.6 VPN e IPv6

Ci sono alcune considerazioni speciali per le VPN quando si utilizzano in combinazione con Ipv6. I due punti principali di preoccupazione sono:

- Se un certo tipo di VPN supporta o meno Ipv6
- Assicurarsi che le regole del firewall non permettano traffico non cifrato che dovrebbe essere in arrivo su una VPN.

18.6.1 Supporto delle VPN a IPv6

Il supporto per Ipv6 varia da tipo a tipo e nel supporto al client. Assicurarsi di controllare con il fornitore dell'altro dispositivo per accertarsi che un firewall o client non-Firew4LL supporti le VPN Ipv6.

IPsec

Firew4LL supporta l'Ipsec che utilizza Ikev1 su Ipv6 con una particolarità: se viene utilizzato un indirizzo peer Ipv6, il tunnel può trasportare solo reti Ipv6 in fase 2, e lo stesso per Ipv4. Il traffico non può essere misto tra famiglie di indirizzi. *Vedere Ipsec e Ipv6*.

Quando un tunnel Ipsec è impostato per Ikev2, può includere sia le definizioni Ipv4 che Ipv6 di fase 2 contemporaneamente.

OpenVPN

Openvpn supporta pienamente Ipv6 per i client sito-a-sito e dei dispositivi mobili e i tunnel possono trasportare sia il traffico Ipv4 che quello Ipv6 contemporaneamente. *Vedere OpenVPN e IPv6*.

18.6.2 VPN con IPv6 e regole del firewall

Come accennato brevemente in *Problemi con firewall e VPN*, occorre prestare particolare attenzione quando si instrada il traffico Ipv6 attraverso una VPN e si utilizzano sottoreti pubblicamente instradabili. Lo stesso consiglio vale anche per Ipv4, ma è molto meno comune avere client su entrambi i lati di una VPN con Ipv4 che utilizzano indirizzi pubblicamente instradabili.

Il problema principale è che, poiché è possibile instradare tutto da una LAN all'altra LAN attraverso Internet, allora il traffico si potrebbe far scorrere non cifrato tra le due reti se la VPN è down (o non è presente affatto!). Questo è tutt'altro che ideale perché, sebbene la connettività sia disponibile, se un traffico fosse intercettato tra le due reti e quel traffico usasse un protocollo non criptato come HTTP, allora potrebbe compromettere la rete.

Un modo per evitarlo è quello di non consentire il traffico dalla LAN con IPv6 da remoto sulle regole della WAN del lato opposto. Consentire solo il traffico dalla sottorete del lato remoto sulle regole del firewall per qualsiasi tipo di VPN viene utilizzato per proteggere il traffico. Una regola di blocco esplicita potrebbe anche essere aggiunta all'inizio delle regole WAN per garantire che questo traffico non possa entrare direttamente dalla WAN. Un metodo migliore è quello di utilizzare una regola dinamica per rifiutare il traffico in uscita sulla WAN destinato ad un host delle reti locali degli host/da remoto con VPN. In questo modo il traffico insicuro non lascia mai i locali. Con la regola impostata per il registro, la "perdita" sarebbe ovvio per qualcuno che monitora i registri in quanto sarebbe mostrato bloccato in uscita sulla WAN.

Un'altra conseguenza meno ovvia di avere la connettività a doppio stack tra le reti è che le differenze nel DNS possono causare instradamento involontario. Supponiamo che la connettività VPN con IPv4 esista tra due siti, ma non esista una VPN con IPv6, solo la connettività IPv6 standard in entrambe le sedi. Se un host locale è impostato per preferire

IPv6 e riceve una risposta DNS AAAA con l'indirizzo IP con IPv6 per una risorsa remota, tenterebbe di connettersi prima su IPv6 piuttosto che usare la VPN. In casi come questo, sarebbe necessario fare attenzione ad assicurarsi che il DNS non contenga record in conflitto o che le regole dinamiche iano aggiunte per evitare che questo traffico IPv6 fuoriusca dalla WAN. Un articolo più approfondito su questo tipo di perdita di traffico può essere trovato nella bozza IETF denominata draft-gont-Opsec-vpn-leakages-00.

Le VPN forniscono un mezzo per incanalare il traffico attraverso una connessione criptata, impedendo che venga visto o modificato durante il transito. Firew4LL offre tre opzioni per la VPN: IPsec, OpenVPN e L2TP. Questo capitolo fornisce una panoramica sull'utilizzo della VPN, i pro e i contro di ogni tipo di VPN in Firew4LL e illustra come decidere quale sia la soluzione migliore per un particolare ambiente. I capitoli successivi discutono in dettaglio ogni opzione per la VPN.

L2TP è un protocollo che usa puramente il tunnel e non offre alcuna crittografia propria. È tipicamente combinato con altri metodi di cifratura come IPsec in modalità di trasporto. A causa di questo, non si adatta con la maggior parte della discussione in questo capitolo. Vedere VPN con L2TP per maggiori informazioni su L2TP.

18.7 Avviso su PPTP

Il supporto del server PPTP è stato rimosso da Firew4LL. Nonostante l'attrattiva della sua convenienza, PPTP non deve essere utilizzato in nessun caso perché non è più sicuro. Questo non riguarda solo l'implementazione di PPTP che era in Firew4LL; qualsiasi sistema che gestisce con PPTP non è più sicuro. Il motivo per l'insicurezza è che PPTP si basa su MS-Chapv2 che è stato completamente compromesso. Il traffico intercettato può essere decriptato da una terza parte al 100% in poco tempo, quindi si può considerare qualsiasi traffico trasportato in PPTP non cifrato. Utilizzare un altro tipo di VPN come OpenVPN o Ipsec il più presto possibile. Ulteriori informazioni sul compromesso in materia di sicurezza con PPTP sono disponibili all'indirizzo https://isc.sans.edu/diary/End+of+Days+for+MS-CHAPv2/13807 e https://www.cloudcracker.com/blog/ 2012/07/29/cracking-ms-chap-v2/.

18.8 Scenari comuni

Ci sono quattro usi comuni delle funzionalità VPN di Firew4LL, ciascuna trattata in questa sezione.

18.8.1 Connettività sito-a-sito

La connettività sito-a-sito viene utilizzata principalmente per connettere le reti in più luoghi fisici in cui è richiesta una connessione dedicata e sempre attiva tra le sedi. Questo metodo viene spesso utilizzato per collegare filiali a un ufficio principale, collegare le reti di partner commerciali, o collegare una rete ad un'altra posizione, come un ambiente di data center.

Prima della proliferazione della tecnologia VPN, i circuiti WAN privati erano l'unica soluzione per collegare più sedi. Queste tecnologie includono circuiti dedicati punto-a-punto, tecnologie di commutazione dei pacchetti come frame relay e ATM, e più recentemente, MPLS (Commutazione dell'etichetta multiprotocollo, Multiprotocol Label Switching) e fibra e rame basato sui servizi Ethernet metropolitani. Sebbene questi tipi di connettività WAN privata forniscano connessioni affidabili e a bassa latenza, sono anche molto costosi con commissioni mensili ricorrenti. La tecnologia VPN è cresciuta in popolarità perché fornisce la stessa connettività sito-a-sito sicura utilizzando connessioni Internet che sono generalmente molto meno costose.

Limitazioni della connettività VPN

Le prestazioni sono una considerazione importante quando si pianifica una soluzione VPN. In alcune reti, solo un circuito WAN privato può soddisfare i requisiti di larghezza di banda o latenza. La latenza è di solito il fattore più grande. Un circuito punto-a-punto DS1 ha una latenza fine-a-fine di circa 3-5 ms, mentre la latenza al primo hop su

una rete ISP sarà generalmente almeno tale se non superiore. I servizi Ethernet metropolitani o i circuiti in fibra hanno una latenza fine-a-fine di circa 0-3 ms, solitamente inferiore alla latenza al primo hop di una rete ISP. Qualcosa varierà in base alla distanza geografica tra i siti. I numeri indicati sono tipici per i siti entro un paio di centinaia di miglia l'uno dall'altro. Le VPN di solito vedono una latenza di circa 30-60 ms a seconda delle connessioni Internet in uso e della distanza geografica tra le posizioni. La latenza può essere ridotta al minimo e le prestazioni della VPN massimizzate utilizzando lo stesso ISP per tutte le sedi della VPN, ma questo non è sempre possibile.

Alcuni protocolli funzionano molto male con la latenza inerente alle connessioni su Internet. La condivisione di file Microsoft (SMB) è un esempio comune. Al di sotto dei 10 ms di latenza, funziona bene. A 30 ms o più, è lento, e a più di 50 ms è dolorosamente lento, causando frequenti blocchi durante la navigazione delle cartelle, il salvataggio di file, ecc. Ottenere un elenco di directory semplice richiede numerose connessioni di andata e ritorno tra il client e il server, ciò aggrava significativamente l'aumento del ritardo della connessione. In Windows Vista e Server 2008, Microsoft ha introdotto SMB 2.0 che include nuove funzionalità per affrontare il problema descritto. SMB 2.0 consente l'invio di più azioni in una singola richiesta, così come la possibilità di inoltrare richieste, il che significa che il client può inviare richieste aggiuntive senza attendere la risposta da richieste precedenti. Se una rete utilizza esclusivamente Vista e Server 2008 o sistemi operativi più recenti questo non sarà un problema, ma data la rarità di tali ambienti, questo dovrà di solito essere preso in considerazione. SMB 3.0 migliora ulteriormente in questo settore con il supporto per più flussi.

Altri due esempi di protocolli sensibili alla latenza sono il protocollo per il desktop da remoto di Microsoft (Microsoft Remote Desktop Protocol, RDP) e Citrix ICA. C'è una chiara differenza di prestazioni e reattività con questi protocolli tra tempi di risposta sotto i 20 ms tipicamente presenti in una WAN privata, e gli oltre 50-60 ms tempi di risposta comuni alle connessioni VPN. Se gli utenti remoti lavorano su desktop pubblicati che utilizzano dispositivi dei client leggeri, ci sarà una notevole differenza di prestazioni tra una WAN privata e VPN. Se tale differenza di prestazioni è abbastanza significativa da giustificare la spesa di una WAN privata varierà da un ambiente all'altro.

Ci possono essere altre applicazioni di rete in un ambiente sensibile alla latenza, dove le prestazioni ridotte di una VPN sono inaccettabili. O tutte le posizioni possono essere all'interno di un'area geografica relativamente piccola utilizzando lo stesso ISP, dove le prestazioni di una VPN rivaleggiano con quelle di connessioni WAN private.

18.8.2 Accesso remoto

Le VPN con accesso da remoto consentono agli utenti di connettersi in modo sicuro a una rete da qualsiasi luogo in cui sia disponibile una connessione Internet. Questo è più frequentemente utilizzato per i lavoratori da dispositivi mobili (spesso indicato come "Combattenti di strada o Road Warriors") o perché il lavoro richiede frequenti viaggi e poco tempo in ufficio, o per dare ai dipendenti la possibilità di lavorare da casa. Può anche consentire agli appaltatori o ai fornitori l'accesso temporaneo a una rete. Con la proliferazione degli smartphone, gli utenti hanno la necessità di accedere in modo sicuro ai servizi interni dai loro telefoni utilizzando una VPN con accesso da remoto.

18.8.3 Protezione delle reti wireless

Una VPN può fornire un ulteriore livello di protezione per le reti wireless. Questa protezione è duplice: fornisce un ulteriore livello di crittografia per il traffico che attraversa la rete wireless e può essere implementata in modo tale da richiedere un'ulteriore autenticazione prima di consentire l'accesso alle risorse di rete. Questo è distribuito per lo più come VPN con accesso da remoto. Questo è coperto in *Protezione aggiuntiva per una rete wireless*.

18.8.4 Relay sicuro

Le VPN con accesso da remoto possono essere configurate in modo da passare tutto il traffico dal sistema client attraverso la VPN. Questo è conveniente da avere quando si utilizzano reti non attendibili, come hotspot wireless in quanto consente ad un client di spingere tutto il suo traffico Internet attraverso la VPN e verso Internet dal server VPN. Questo protegge l'utente da una serie di attacchi che sono possibili su reti non attendibili, anche se ha un impatto

sulle prestazioni in quanto aggiunge ulteriori salti e latenza a tutte le connessioni. Tale impatto è di solito minimo con connettività ad alta velocità quando il client e il server VPN sono relativamente vicini geograficamente.

CAPITOLO 19

Traffic Shaper

19.1 Cosa puo" fare lo stabilizzatore (shaper) del traffico per una rete

L'idea di base dello stabilizzatore (shaping) il traffico è alzare e abbassare le priorità dei pacchetti o tenerli sotto una certa velocità. Questo concetto sembra semplice, tuttavia, il numero di modi in cui questo concetto può essere applicato è vasto. Questi sono solo alcuni esempi comuni che si sono dimostrati popolari con gli utenti del software Firew4LL.

19.1.1 Mantenere la navigazione stabile

I collegamenti asimmetrici, in cui la velocità di download differisce dalla velocità di upload, sono comuni, specialmente con DSL. Alcuni collegamenti sono così squilibrati che la velocità massima di download è quasi irraggiungibile perché è difficile per un firewall inviare abbastanza pacchetti ACK (riconoscimento) da mantenere lo scorrimento del traffico. I pacchetti ACK vengono trasmessi al mittente dall'host ricevente per indicare che i dati sono stati ricevuti correttamente e per segnalare che è OK inviarne di più. Se il mittente non riceve gli ACK in modo tempestivo, i meccanismi di controllo della congestione in TCP entreranno in funzione e rallenteranno la connessione.

Questo tipo di situazione è comune: quando si carica un file su un collegamento con capacità di throughput asimmetrico, la navigazione e il download rallentano la scansione o le bancarelle. Ciò accade perché la parte di caricamento del circuito è piena per il caricamento del file e c'è poco spazio per inviare pacchetti ACK che consentono ai download di continuare a scorrere. Utilizzando lo shaper per dare la priorità ai pacchetti ACK, il firewall può abilitare velocità di download più veloci e stabili sui collegamenti asimmetrici.

Questo non è così importante sui link simmetrici in cui la velocità di upload e download sono le stesse, ma può ancora essere auspicabile se la larghezza di banda in uscita disponibile è fortemente utilizzata.

19.1.2 Mantenere le chiamate VoIP chiare

Se le chiamate Voice sull'IP utilizzano lo stesso circuito dei dati, i caricamenti e i download potrebbero degradare la qualità delle chiamate. Il software Firew4LL può dare la priorità al traffico delle chiamate sopra altri protocolli, e garantire che le chiamate passino attraverso chiaramente senza interruzioni, anche durante lo streaming dei video ad

alta definizione di Netflix. Invece di interrompere la chiamata, lo shaper riduce la velocità degli altri trasferimenti per lasciare spazio alle chiamate.

19.1.3 Ridurre il Lag (ritard) nei giochi

Lo shaper ha anche opzioni per dare la priorità al traffico associato ai giochi in rete. Anlogamente alla priorità delle chiamate VoIP, l'effetto è che, anche se gli utenti della rete stanno scaricando durante il gioco, il tempo di risposta del gioco dovrebbe essere ancora veloce come se il resto della connessione fosse inattivo.

19.1.4 Tenere sotto controllo le applicazioni P2P

Abbassando la priorità del traffico associato a porte Peer-to-Peer note, gli amministratori possono essere più tranquilli sapendo che anche se questi programmi sono in uso, non ostacoleranno altro traffico sulla rete. A causa della sua priorità più bassa, altri protocolli saranno favoriti sul traffico P2P, che sarà limitato quando altri servizi hanno bisogno della larghezza di banda.

19.1.5 Applicare i limiti di larghezza di banda

I limitatori possono applicare un limite di larghezza di banda a un gruppo di dispositivi, come a tutto il traffico su un'interfaccia, o il mascheramento sui limitatori può applicarli per un indirizzo IP o per una rete. In questo modo il firewall può garantire che nessuna persona possa consumare tutta la larghezza di banda disponibile.

19.2 Limitazioni hardware

L" ottimizzazione del traffico viene eseguito con l'aiuto di **ALTQ**. Sfortunatamente, solo un sottoinsieme di tutte le schede di rete supportate è in grado di utilizzare queste funzionalità perché i driver devono essere modificati per supportare lo shaping con ALTQ. Le seguenti schede di rete sono in grado di utilizzare lo ottimizzazione del traffico:

ae(4), age(4), alc(4), ale(4), an(4), aue(4), axe(4), bce(4), bfe(4), bge(4), bridge(4), cas(4), cpsw(4), cxl(4), dc(4), de(4), ed(4), em(4), ep(4), epair(4), et(4), fxp(4), gem(4), hme(4), hn(4), igb(4), ix(4), jme(4), l2tp(4), le(4), lem(4), msk(4), mxge(4), my(4), ndis(4), nfe(4), ng(4), nge(4), npe(4), nve(4), ovpnc(4), ovpns(4), ppp(4), pppoe(4), pptp(4), re(4), rl(4), sf(4), sge(4), sis(4), sk(4), ste(4), stge(4), ti(4), tun(4), txp(4), udav(4), ural(4), vge(4), vlan(4), vmx(4), vr(4), vte(4), vtnet(4), xl(4)

I limitatori utilizzano un sistema di back-end diverso, che opera attraverso le `dummynet` pipe in `ipfw` e non attraverso **ALTQ**. In quanto tali, tutte le schede di rete possono essere utilizzate con i limitatori, senza restrizioni. Se un firewall contiene una scheda che non supporta ALTQ, può utilizzare invece i limitatori.

19.3 Tipi di pianificatore ALTQ

Il software Firew4LL contiene diversi tipi di pianificatori ALTQ per coprire una vasta gamma di scenari di shaping. Le opzioni per ALTQ sono:

Accodamento prioritario (PRIQ) Gestisce la priorità delle connessioni

Accodamento basato su classi (CBQ) Supporta la condivisione della larghezza di banda tra code e limiti di larghezza di banda

Curva gerarchica del servizio equo (HFSC) Supporta le garanzie di larghezza di banda in tempo reale insieme a un albero gerarchico di code nidificate.

Ritardo controllato (CoDel) Tentativi di combattere l'aumento del buffer (bufferbloat).

Accodamento equo (FAIRQ) Tenta di distribuire abbastanza larghezza di banda tra tutte le connessioni.

PRIQ, CBQ e HFSC sono selezionabili nelle procedure guidate dello shaper e le procedure guidate mostreranno le opzioni appropriate e creeranno le code in base alla disciplina ALTQ scelta.

19.3.1 Avvertimenti sulle prestazioni

L'attivazione di dello ottimizzazione del traffico con ALTQ pone un onere aggiuntivo sull'hardware e ci sarà una potenziale perdita complessiva delle prestazioni della rete. Sui sistemi che hanno potenza da risparmiare, questo potrebbe non essere evidente. Su sistemi che operano vicino alle loro specifiche limita che il firewall possa vedere un degrado delle prestazioni. Considerare la perdita peggiore rispetto al lavoro senza lo shaper dipende dal carico di lavoro individuale.

19.3.2 Accodamento prioritario (PRIQ)

PRIQ è una delle discipline più semplici da configurare e comprendere. Le code sono tutte direttamente sotto la coda di root, non esiste una struttura per avere code sotto altre code con PRIQ in quanto esiste con HFSC e CBQ. Non importa la larghezza di banda sulle interfacce, solo la priorità delle code. I valori per la priorità vanno da 15, e maggiore è il numero di priorità, più è probabile che la coda ottenga l'elaborazione dei suoi pacchetti.

PRIQ può essere d'ostacolo per le code minori, diminuendo le loro risorse quando le code di priorità più alte richiedono larghezza di banda. In casi estremi, è possibile che una coda di priorità inferiore abbia pochi o nessun pacchetto gestito se le code di priorità più elevate consumano tutte le risorse disponibili.

19.3.3 Curva gerarchica del servizio equo (HFSC)

La disciplina HFSC dello ottimizzazione del traffico è molto potente. È utile per servizi come VoIP e per i video per fornire una quantità minima garantita di larghezza di banda.

Le code in HFSC sono disposte in una gerarchia o in un albero, con code di root per ogni interfaccia, code primarie sottostanti e code secondarie nidificate sotto le code primarie (ecc.). Ogni coda può avere una larghezza di banda impostata e le relative opzioni.

Opzioni di coda specifiche per HFSC

HFSC supporta alcune opzioni di coda che non sono supportate da altre discipline. È attraverso queste opzioni che raggiunge l'elaborazione in tempo reale garantita e la condivisione dei collegamenti.

La curva di servizio (sc) si trova dove i requisiti di larghezza di banda per questa coda sono sintonizzati.

m1 Limite della larghezza di banda in grado di scoppiare

d Tempo per scoppiare il limite della larghezza di banda, specificato in millisecondi. (ad esempio 1000 = 1 secondo)

m2 Limite della larghezza di banda normale

Ad esempio, una connessione richiede larghezza di banda **m1** entro il tempo **d**, ma un massimo normale di **m2**. Entro il tempo iniziale impostato da **d**, **m2** non è selezionato, solo **m1**. Dopo che **d** è scaduto, se il traffico è ancora sopra **m2**, sarà stabilizzato. Più comunemente, **m1** e **d** sono lasciati vuoti, in modo che solo **m2** sia selezionato.

Ciascuno di questi valori può essere impostato per i seguenti usi:

Limite superiore Massima larghezza di banda consentita per la coda. Farà una limitazione della larghezza di banda dura. Il parametro **m1** qui può anche essere utilizzato per limitare lo scoppio. Nel lasso di tempo **d** una connessione non otterrà più di larghezza di banda **m1**.

Tempo reale Garanzia di larghezza di banda minima per la coda. Questo è valido solo per le code secondarie. Il parametro **m1** sarà sempre soddisfatto nel lasso di tempo **d** e **m2** è il massimo che questa disciplina consentirà di utilizzare. Nota: il valore per **m2** non può superare il 30% della larghezza di banda disponibile per la coda primaria.

Condivisione del link La quota di larghezza di banda di una coda registrata prima. Condividerà la larghezza di banda tra le classi se le garanzie in **tempo reale** sono state soddisfatte. Il valore **m2** per la **condivisione del link** sovrascriverà l'impostazione della **larghezza di banda** per la coda. Queste due impostazioni sono le stesse, ma se entrambe sono impostate, viene utilizzata **m2** dalla **condivisione del link**.

Combinando questi fattori, una coda otterrà la larghezza di banda specificata dai fattori in **tempo reale**, più quelli dalla **condivisione del link**, fino al massimo del **limite superiore**. Si può avere un sacco di tentativi ed errori, e forse utilizzare un sacco di aritmetica, ma potrebbe valerne la pena per garantire che il traffico di rete sia regolato correttamente. Per ulteriori informazioni sui valori **m1**, **d** e **m2** per diversi scenari, visitare il forum sullo ottimizzazione del traffico di Firew4LL.

19.3.4 Accodamento basato su classi (CBQ)

L'accodamento basato su classi, o CBQ, è simile a HFSC in quanto può avere un albero di code nidificate sotto altre code. Supporta i limiti della larghezza di banda (non garantisce come HFSC), le priorità per le code e ha la capacità di consentire alle code di prendere in prestito la larghezza di banda dalla primaria. A causa della configurazione della coda più semplice, può essere una buona alternativa a HFSC soprattutto se il firewall non ha bisogno di garantire larghezze di banda minime.

Con CBQ, le priorità della coda vanno da 7 con numeri più alti che indicano priorità più alta. Le code di uguale priorità vengono elaborate in modo round-robin.

Nota: sebbene le code secondarie possano prendere in prestito dalla

---

coda primaria, la somma della larghezza di banda delle code secondarie non può superare la larghezza di banda della primaria. Pertanto, CBQ non è un'alternativa ai limitatori per i limiti di larghezza di banda individuali (ad esempio per indirizzo IP).

Opzioni di coda specifiche per CBQ

La disciplina CBQ supporta il concetto di *prestito*, il che significa che se la casella di selezione **Prendere in prestito da altre code quando disponibile** sulla coda è abilitata, la coda sarà in grado di prendere in prestito altra larghezza di banda disponibile dalla coda primarie. Ciò consentirà solo a una coda secondaria di ottenere fino alla larghezza di banda dellla coda primaria immediata, se disponibile, non da altre code primarie.

19.3.5 Gestione attiva delle code con CoDel

La disciplina della gestione attiva delle code con CoDel (AQM) è l'abbreviazione per il ritardo controllato ed è pronunciata "coddle". È stata progettata per combattere i problemi associati all'aumento del buffer nell'infrastruttura di rete. Il bufferbloat è descritto in dettaglio su http://www.bufferbloat.net/projects/bloat/wiki/Introduction. In parole povere, il traffico può accumularsi e andare in pezzi piuttosto che avere un flusso regolare a causa delle dimensioni dei buffer nelle apparecchiature di rete. Controllando il ritardo del traffico questo effetto può essere diminuito.

CoDel non ha selezioni o opzioni di configurazione specifiche. Quando viene attivato per una coda, tenterà automaticamente di gestire il traffico come descritto nella Wiki di CoDel su http://www.bufferbloat.net/projects/codel/wiki. Tenta di mantenere bassi i ritardi del traffico ma consente lo scoppio, controlla i ritardi ma non presta attenzione al ritardo di andata e ritorno, al carico o alla velocità del collegamento e può regolarsi automaticamente se la velocità del collegamento cambia.

L'obiettivo per CoDel è la rete di fascia media. Non funziona bene sulla larghezza di banda molto bassa (1Mbit/s o meno) e non gestisce con bene un gran numero di flussi simultanei o carichi di traffico del grado dei datacenter.

CoDel non è configurabile utilizzando la procedura guidata, ma non richiede una configurazione complessa:

- Passare a **Firewall>Traffic Shaper**, per scheda **Interfaccia**
- Selezionare un'interfaccia (ad es. **WAN**)
- Impostare il **tipo di pianificatore** su *CODEL*
- Impostare un valore appropriato per la **larghezza di banda**
- Fare clic su **Salvare**
- Ripetere se necessario per tutte le altre interfacce di tipo WAN attive

19.3.6 Accodamento equo (FAIRQ)

In FAIRQ, le code vengono monitorate dalla priorità più alta a quella più bassa, ma il pianificatore tenta di distribuire in modo equo la larghezza di banda tra tutte le connessioni.

Quando non c'è contesa per la larghezza di banda, FAIRQ invierà tutti i pacchetti in attesa. Quando c'è contesa per la larghezza di banda FAIRQ inizierà a cercare code che non superino i loro limiti, iniziando prima con code ad alta priorità e lavorando poi con le code più basse. Un pacchetto in una coda con completa priorità alta viene elaborato dopo un pacchetto da una coda di priorità inferiore che non è completa. Se tutte le code sono complete, FAIRQ invierà un pacchetto dalla coda di priorità più alta.

FAIRQ consente alle connessioni di superare la larghezza di banda della coda, ma manterrà un consumo medio pari alla larghezza di banda della coda definita.

FAIRQ non è attualmente supportato nella procedura guidata dello shaper del traffico e richiede una configurazione manuale.

19.4 Configurazione dello Traffic Shaper ALTQ con la procedura guidata

La prima volta si consiglia di configurare lo Traffic Shaper utilizzando la procedura guidata, che guida gli amministratori attraverso il processo di configurazione dello shaper.

Suggerimento: a causa della complessità delle code e delle regole dello shaper, iniziare da zero è piuttosto complicato. Se un firewall ha bisogno di regole personalizzate, passare attraverso la procedura guidata e approssimare i requisiti, quindi fare regole personalizzate in seguito.

Ogni fase della procedura guidata imposta code e regole univoche che controllano il traffico assegnato in tali code. Per configurare tutto manualmente, specificare la velocità WAN nella prima schermata, quindi fare clic su **Avanti** per

tutti i passaggi rimanenti. La procedura guidata richiede che le opzioni siano abilitate su almeno un passaggio, ma non importa quale passaggio.

Nota: completare la procedura guidata e fare clic su **Finire** alla fine sostituirà **tutte** le code dello shaper esistenti e le regole dinamiche create dalla procedura guidata, incluse quelle clonate dalle regole della procedura guidata, con le code e le regole della nuova configurazione della procedura guidata.

19.4.1 Scelta della procedura guidata

Per iniziare con la procedura guidata dello ottimizzazione del traffico, passare a **Firewall>ottimizzazione del traffico** e fare clic sulla scheda **Procedura guidata**. In questa pagina viene visualizzato un elenco di procedure guidate di Traffic Shaper disponibili, tra cui:

LAN/WAN multiple Utilizzata quando il firewall ha una o più WAN e una o più LAN. Questa è la procedura guidata più comune e copre la maggior parte degli scenari.

Collegamenti dedicati Utilizzatta quando specifici accoppiamenti LAN+WAN devono essere contabilizzati nella configurazione dello shaper.

19.4.2 Avvio della procedura guidata

Ogni nome della procedura guidata è seguito dal nome del file della procedura guidata, che è un collegamento. Fare clic sul collegamento per avviare la procedura guidata. Questo esempio utilizza la procedura guidata per LAN/WAN multiple, quindi fare clic su traffic_shaper_wizard_multi_all.XML.

Successivamente, la procedura guidata si avvia e il primo passo richiede il numero di connessioni di tipo WAN e LAN sul firewall, come nella figura *Inserire il conteggio dell'interfaccia*.

- **Immettere il numero di connessioni di tipo WAN sul firewall. Si** tratta di connessioni con un gateway configurato sull'interfaccia o interfacce di tipo WAN dinamica come DHCP o PPPOE
- **Immettere il numero di connessioni di tipo LAN. Si tratta di** interfacce di rete locali senza un gateway sull'interfaccia
- Fare clic su **Avanti** per procedere con il passo successivo

In questo esempio il firewall ha solo un'interfaccia WAN e una LAN.

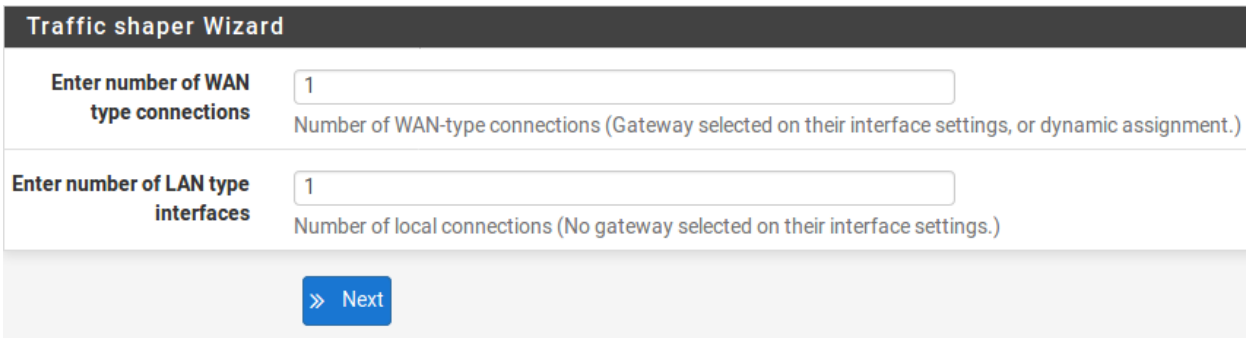


Fig. 1: Inserire il conteggio dell'interfaccia

19.4.3 Reti e velocità

Questo passaggio, mostrato nella figura *Configurazione dello shaper*, definisce le interfacce di rete che saranno all'interno e all'esterno dal punto di vista dello shaper, insieme alle velocità di **Download** e **Upload** per una determinata WAN. Quando il firewall ha più di un'interfaccia di un determinato tipo, la procedura guidata visualizza più sezioni della pagina per gestirle singolarmente.

Oltre alle interfacce e alle loro velocità, selezionare un **pianificatore** di ALTQ (*Tipi di pianificatore di ALTQ*) per le WAN e le LAN. Utilizzare lo stesso pianificatore su ogni interfaccia.

A seconda del tipo di connessione, la vera velocità di collegamento potrebbe non essere la velocità effettiva utilizzabile. Nel caso di PPPoE, il circuito non ha solo un overhead di PPPoE, ma anche un overhead dal collegamento di rete ATM sottostante utilizzato nella maggior parte delle distribuzioni PPPoE. Con alcuni calcoli, tra l'overhead di ATM, PPPoE, IP e TCP, il circuito potrebbe perdere fino al 13% della velocità di collegamento pubblicizzata. In caso di dubbio su cosa impostare la velocità, si consiglia di essere conservatori. Ridurre del 10-13% e lavorare di nuovo fino a valori più grandi. Se il firewall ha una linea di 3Mbit/s, impostarlo per circa 2,7 Mbit/s e quindi testare. La velocità sulla coda primaria risultante può essere modificata in seguito per regolare la larghezza di banda. Se ha un valore basso, la connessione verrà massimizzata esattamente alla velocità definita. Spingerlo più in alto fino a quando il firewall non vede più alcun guadagno nelle prestazioni.

La velocità di interfaccia può essere specificata in Kbit/s, Mbit/s, o Gbit/s, ma utilizzare le stesse unità in ogni pagina.

- Scegliere un"**interfaccia** e un **pianificatore** per ogni interfaccia di tipo LAN (ad esempio *LAN, PRIQ*)
- S cegliere un"**interfaccia** e un **pianificatore** per ogni interfaccia di tipo WAN (ad esempio *WAN, PRIQ*)
- Definire la velocità di **Upload** e le unità per ogni interfaccia di tipo WAN (ad esempio 1, *Mbit/s*)
- Definire la velocità di **Download** e le unità per ogni interfaccia di tipo WAN (ad esempio 10, Mbit/s)
- Fare clic su **Avanti** per procedere con il passo successivo

19.4.4 VOIP

La procedura guidata contiene diverse opzioni per la gestione del traffico delle chiamate VoIP, mostrato in figura *Voce su IP*. La priorità del traffico voce su IP imposta code e regole per dare priorità alle chiamate VoIP e al traffico correlato. Questo comportamento può essere messo a punto dalle altre impostazioni di questo passaggio della procedura guidata.

Attivare Una casella di selezione per abilitare le impostazioni VoIP in questo passaggio. Quando deselezionata, le opzioni sono disabilitate e queste code e regole non verranno aggiunte dalla procedura guidata.

Provider Ci sono alcuni fornitori ben noti tra cui server *Vonage*, *Voicepulse*, *PanasonicTDA*, e *Asterisk*. Se il provider VoIP per questo sito non è nell'elenco, scegliere *generico*. Questa scelta imposta regole in base alle porte e ai protocolli noti per essere utilizzati da questi provider, piuttosto che corrispondere per indirizzo.

Nota: questa scelta corrisponde in base alle porte SIP e RTP, tra gli altri, quindi può corrispondere al traffico da altre fonti, anche se utilizzano le stesse porte del servizio selezionato.

Server SIP Upstream L'IP del PBX o del trunk di SIP upstream o un alias contenente gli indirizzi IP o le reti per i trunk SIP. Quando impostato, questo sovrascrive il campo **Provider** e corrisponderà invece al traffico in base a questi indirizzi.

Nota: questa scelta corrisponde a tutto il traffico UDP da e verso gli indirizzi specificati. Nella maggior parte dei casi questo è OK, ma se ci sono altri servizi basati su UDP non VoIP sullo stesso indirizzo remoto, potrebbe corrispondere anche a quel traffico. Tali casi sono rari, tuttavia, quindi questa opzione tende ad essere più affidabile rispetto alla corrispondenza per porta.

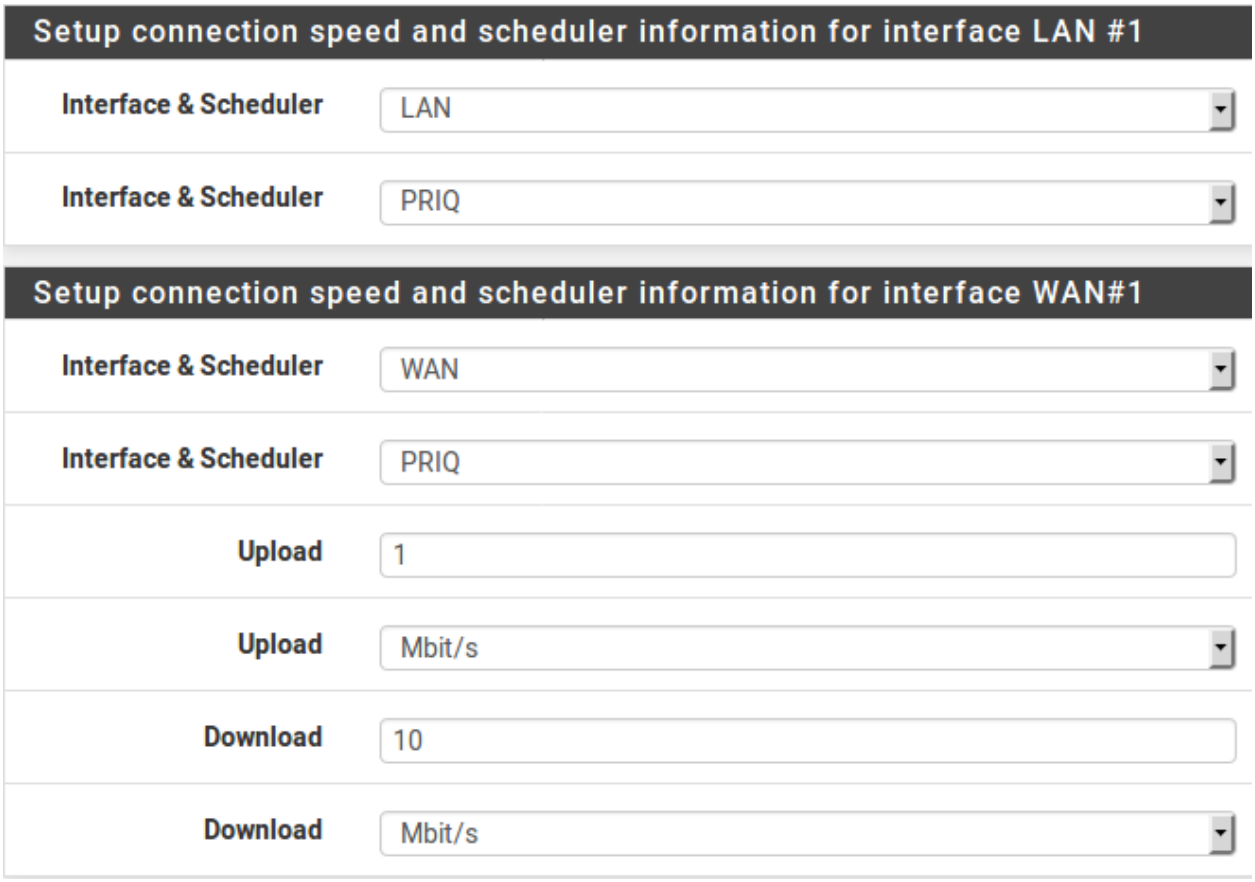


Fig. 2: Configurazione dello shaper

Upload per la connessione WAN La quantità di larghezza di banda di upload da garantire per i dispositivi VoIP. Ciò varierà in base al numero di dispositivi VoIP presenti sulla rete e alla larghezza di banda richiesta da ciascuna sessione. Questa impostazione viene utilizzata da HFSC e CBQ e deve essere lasciata vuota per PRIQ.

Nota: la prenotazione della larghezza di banda per un servizio come VoIP non può superare il 30% della larghezza di banda disponibile sul link. Ad esempio, su un collegamento di 10Mbit/s, lo shaper non può riservare più di 3Mbit/s.

Download per connessione LAN La quantità di larghezza di banda di download da garantire per i dispositivi VoIP. Questa impostazione viene utilizzata da HFSC e CBQ e deve essere lasciata vuota per PRIQ.

Nota: la migliore pratica è quella di utilizzare il trunk SIP **remoto** o l'indirizzo PBX perché altrimenti lo shaper potrebbe non essere in grado di abbinare correttamente il traffico. Ad esempio, utilizzando gli indirizzi IP dei telefoni, lo shaper può corrispondere solo al traffico in una direzione o per niente. Ciò è dovuto al modo in cui lo shaper

corrisponde al traffico con le regole dinamiche in una direzione in uscita. NAT si applica prima che il traffico venga abbinato quando si esce da una WAN, quindi le regole dello shaper non possono corrispondere alle connessioni in uscita in base agli indirizzi IP privati locali.

Per utilizzare queste opzioni:

- Controllare **Priorità del traffico voce su IP**
- Scegliere **uno** dei seguenti:
  - Scegliere un **Provider** dalla lista **o**
  - Immettere un **indirizzo del server SIP di upstream** o alias contenente un trunk SIP **remoto** o PBX
- Lasciare vuoto **Upload** e **Download** se si utilizza PRIQ, altrimenti immettere un valore di **Upload** o **Download** appropriato per ogni connessione
- Fare clic su **Avanti** per procedere con il passo successivo

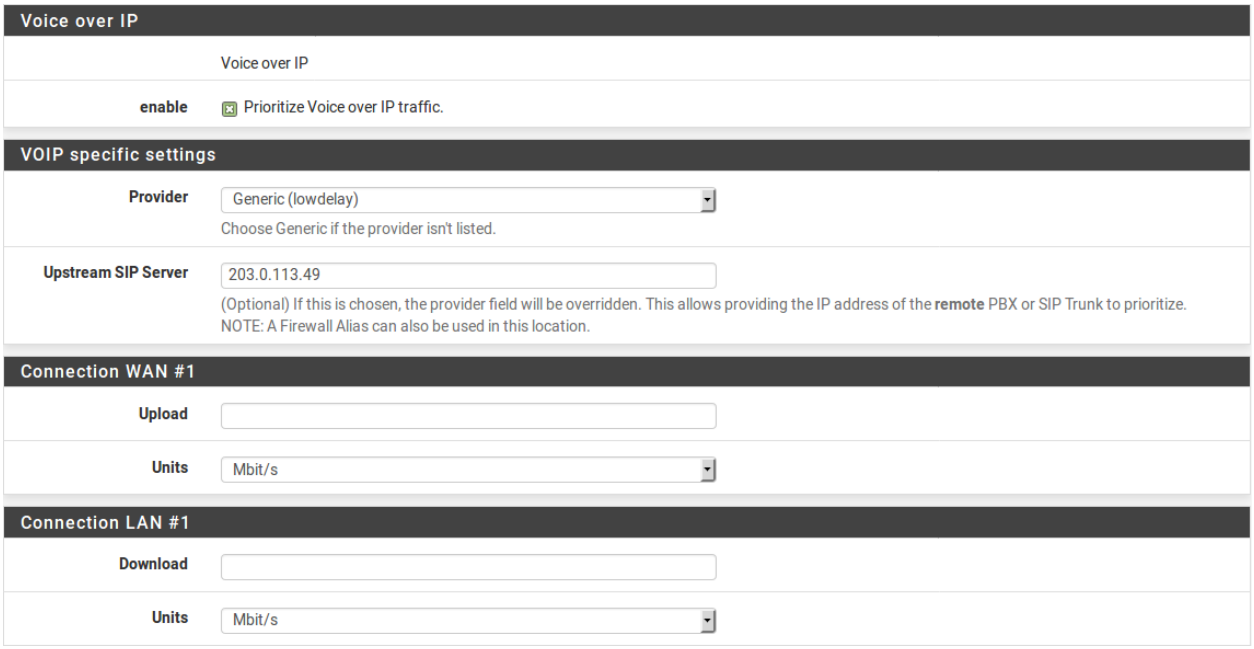


Fig. 3: Voce su IP

19.4.5 Casella di penalità

La casella di penalità, raffigurata nella figura *Casella di penalità*, è un luogo per relegare gli utenti dal comportamento anomalo o dispositivi che altrimenti consumano quantità indesiderate di larghezza di banda. A questi dispositivi viene assegnato un limite di larghezza di banda rigido che non può superare.

Abilitare Una casella di selezione per abilitare le impostazioni della casella di penalità in questo passaggio. Quando deselezionate, le opzioni sono disabilitate e queste code e regole non verranno aggiunte dalla procedura guidata.

Indirizzo L'indirizzo IP per penalizzare, o un alias contenente più indirizzi da penalizzare.

Larghezza di banda La quantità di larghezza di banda che l'**indirizzo** può consumare, al massimo.

Per utilizzare queste opzioni:

- Selezionare **IP o Alias da penalizzare**

- Immettere un indirizzo IP o un Alias nella casella **Indirizzo**
- Inserire il limite di **larghezza di banda**
- Scegliere le unità corrette per il limite di **larghezza di banda**
- Fare clic su **Avanti** per procedere con il passo successivo

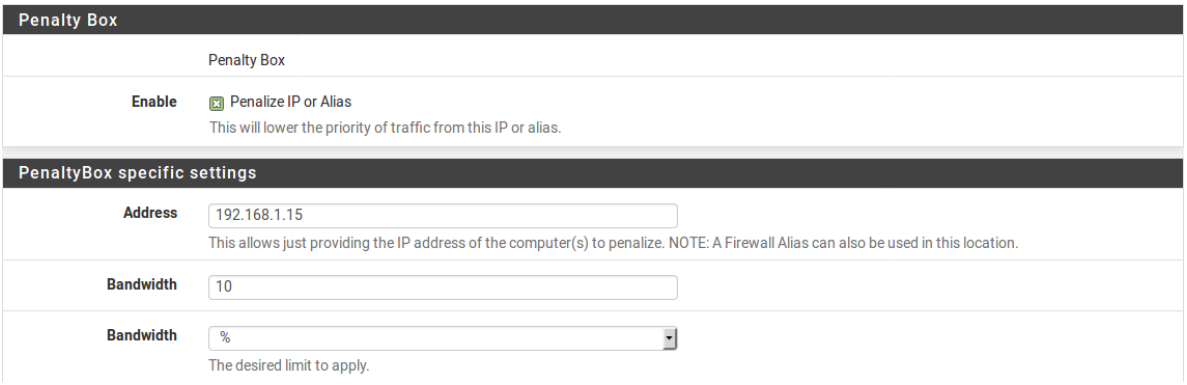


Fig. 4: Casella di penalità

19.4.6 Reti peer-to-peer (P2P)

Il passo successivo, mostrato in figura *Reti Peer-to-Peer*, imposta i controlli per molti protocolli di rete Peer-to-Peer (P2P). In base alla progettazione, i protocolli P2P utilizzeranno tutta la larghezza di banda disponibile a meno che non vengano messi in atto limiti. Se il traffico P2P sarà presente su una rete, la migliore pratica è garantire che non degraderà altro traffico.

Nota:

I protocolli P2P tentano deliberatamente di evitare il rilevamento. Bittorrent è particolarmente colpevole di questo comportamento. Spesso utilizza porte non standard o casuali o porte associate ad altri protocolli. Identificare tutto il traffico P2P può essere difficile o impossibile.

Abilitare Una casella di selezione per abilitare le impostazioni del traffico P2P in questo passaggio. Quando deselezionata, le opzioni sono disabilitate e queste code e regole non verranno aggiunte dalla procedura guidata.

Peer-to-Peer cattura tutto Fa sì che qualsiasi traffico non riconosciuto venga assunto come traffico P2P e tale traffico avrà la sua priorità abbassata di conseguenza.

> **Larghezza di banda** La quantità di larghezza di banda che il traffico non classificato può consumare, al massimo, quando P2P cattura tutto è attivo.

> **Avvertimento:** questa opzione acquisisce effettivamente la coda dello shaping del traffico predefinita e ne riduce la priorità. Quando questa opzione è attiva, è fondamentale che tutto il traffico legittimo sia abbinato a regole che impostano una priorità superiore alla priorità della coda P2P cattura tutto.
>
> Il passaggio Alzare/Abbassare le altre applicazioni della procedura guidata può essere d'aiuto qui, ma alla fine l'implementazione di questa attività richiede spesso regole manuali aggiuntive.

Abilitare/Disabilitare protocolli P2P specifici Queste opzioni identificano vari protocolli P2P noti. Il firewall assegnerà porte e protocolli associati a ciascuna opzione abilitata come traffico P2P.

Per utilizzare le opzioni in questo passaggio:

- Selezionare la **priorità più bassa del traffico Peer-to-Peer**
- Opzionalmente abilitare le funzionalità di **P2P cattura tutto**
  - Inserire il limite di **larghezza di banda** per **P2P Cattura tutto**, se abilitato
  - Scegliere le unità corrette per il limite di **larghezza di banda**
- Selezionare i protocolli per il firewall da classificare come traffico P2P
- Fare clic su Avanti per procedere con il passo successivo
-

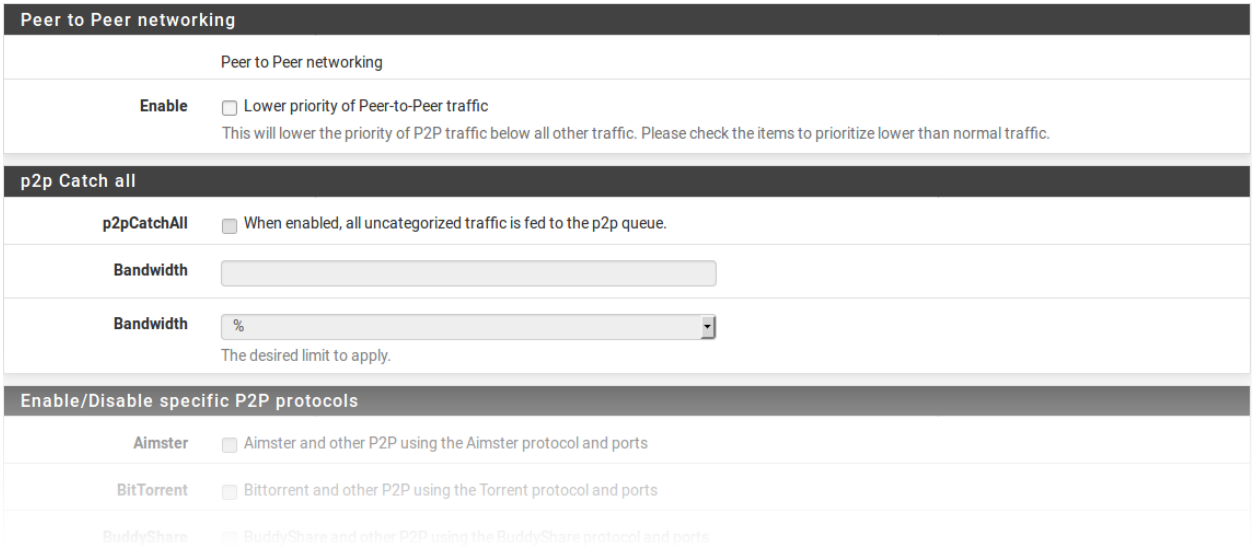


Fig. 5: Reti Peer-to-Peer

19.4.7 Giochi in Rete

I giochi Online in genere si basano sulla bassa latenza per esperienze di giocatori accettabili. Se un utente della rete tenta di scaricare file di grandi dimensioni o patch di gioco durante il gioco, il traffico può facilmente soffocare i pacchetti associati al gioco stesso e causare ritardo o disconnessioni. Se il firewall dà priorità al traffico di gioco, si può garantire che il traffico sarà consegnato prima e più velocemente.

> **Abilitare** Una casella di selezione per abilitare le impostazioni del traffico di gioco in questo passaggio. Quando deselezionata, le opzioni sono disabilitate e queste code e regole non verranno aggiunte dalla procedura guidata.
>
> **Abilitare/disabilitare console e servizi di gioco specifici** Queste opzioni corrispondono al traffico per intere console di gioco o servizi online che utilizzano porte e protocolli comuni a tutti, o almeno alla maggioranza, dei loro giochi.
>
> **Abilitare/disabilitare giochi specifici** Queste opzioni corrispondono al traffico per giochi specifici che si discostano dalle categorie generali nella sezione precedente.

Suggerimento: per dare la priorità a un gioco che non è elencato, selezionare qualsiasi altro gioco dall'elenco in modo che la procedura guidata crei le code e le regole da utilizzare come base di riferimento. Dopo aver completato la procedura guidata, modificare le regole risultanti per abbinare il gioco non elencato.

Per utilizzare le opzioni in questo passaggio:

- Controllare **Dare priorità al traffico di gioco di rete**
- Selezionare qualsiasi console di gioco sulla rete dall'elenco in **Abilitare/disabilitare console e servizi di gioco specifici**
- Selezionare tutti i giochi sulla rete dalla lista in **Abilitare/disabilitare giochi specifici**
- Fare clic su **Avanti** per procedere con il passo successivo

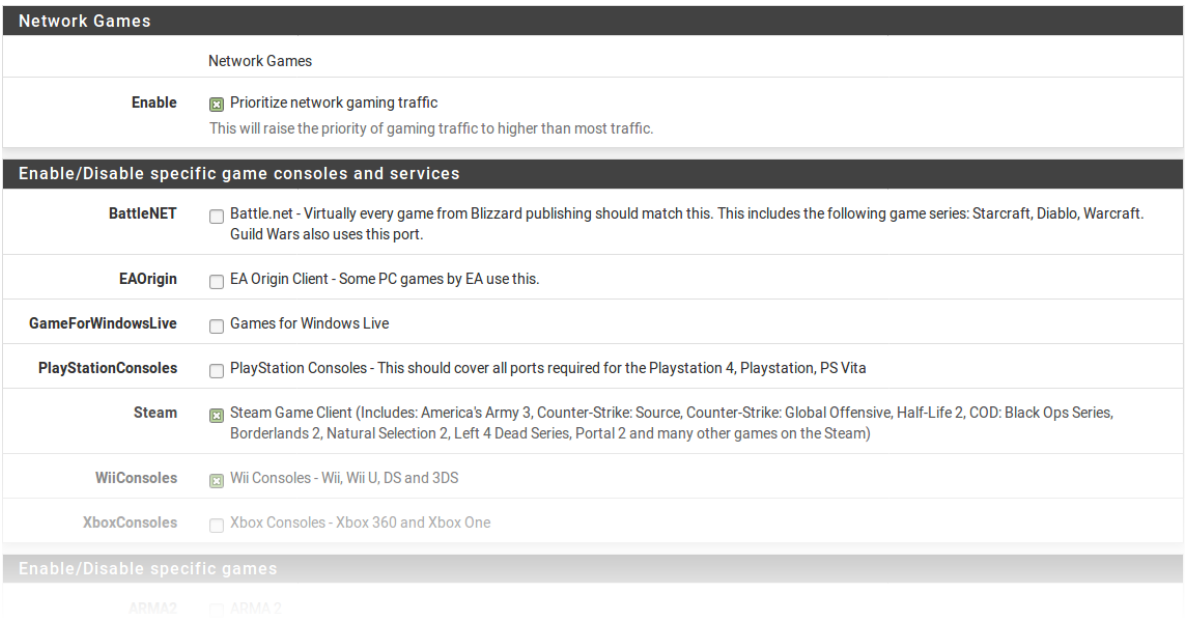


Fig. 6: Giochi Di Rete

19.4.8 Priorità o secondarietà di altre applicazioni

L'ultima schermata di configurazione della procedura guidata dello shaper, vista in figura *Alzare o abbassare le altre applicazioni,* elenca una serie di altre applicazioni e protocolli comunemente disponibili.

Le esigenze di una particolare rete dettano come il firewall dovrebbe gestire ogni protocollo. Ad esempio, in una gestione dell'ambiente aziendale potrebbe voler ridurre la priorità del traffico non interattivo come l'e-mail in cui una riduzione della velocità non viene solitamente notata dagli utenti e potrebbe anche voler aumentare la priorità dei servizi interattivi come RDP in cui le scarse prestazioni sono un impedimento per i dipendenti. In una casa, lo streaming multimediale può essere più importante e altri servizi possono avere la loro priorità abbassata dallo shaper.

Suggerimento: Come per altri passaggi di questa procedura guidata dello shaper, se un protocollo non è elencato, selezionare un protocollo simile e quindi regolare le regole dopo aver completato la procedura guidata.

Attivare Una casella di selezione per abilitare le impostazioni di questo passaggio. Quando deselezionata, le opzioni sono disabilitate e queste code e regole non verranno aggiunte dalla procedura guidata.

Categorie di protocollo Ogni sezione contiene protocolli ben noti, raggruppati per la loro funzione generale.

Ci sono più di 40 protocolli tra cui scegliere, e a ciascuno può essere data una *priorità più alta*, *priorità più bassa*, o lasciato alla *priorità predefinita*.

Suggerimento: Se l'opzione **P2P cattura tutto** è attivo, si consiglia vivamente di utilizzare questo passaggio per garantire che questi altri protocolli siano riconosciuti e trattati normalmente, piuttosto che penalizzati dalla regola P2P cattura tutto predefinita.

Per utilizzare le opzioni in questo passaggio:

- Selezionare **altri protocolli di rete**
- Individuare protocolli specifici nell'elenco per modificare la priorità.
- Per ogni protocollo, scegliere una tra *priorità più alta*, *priorità più bassa*, o lasciare *priorità predefinita*.
- Fare clic su **Avanti** per procedere con il passo successivo

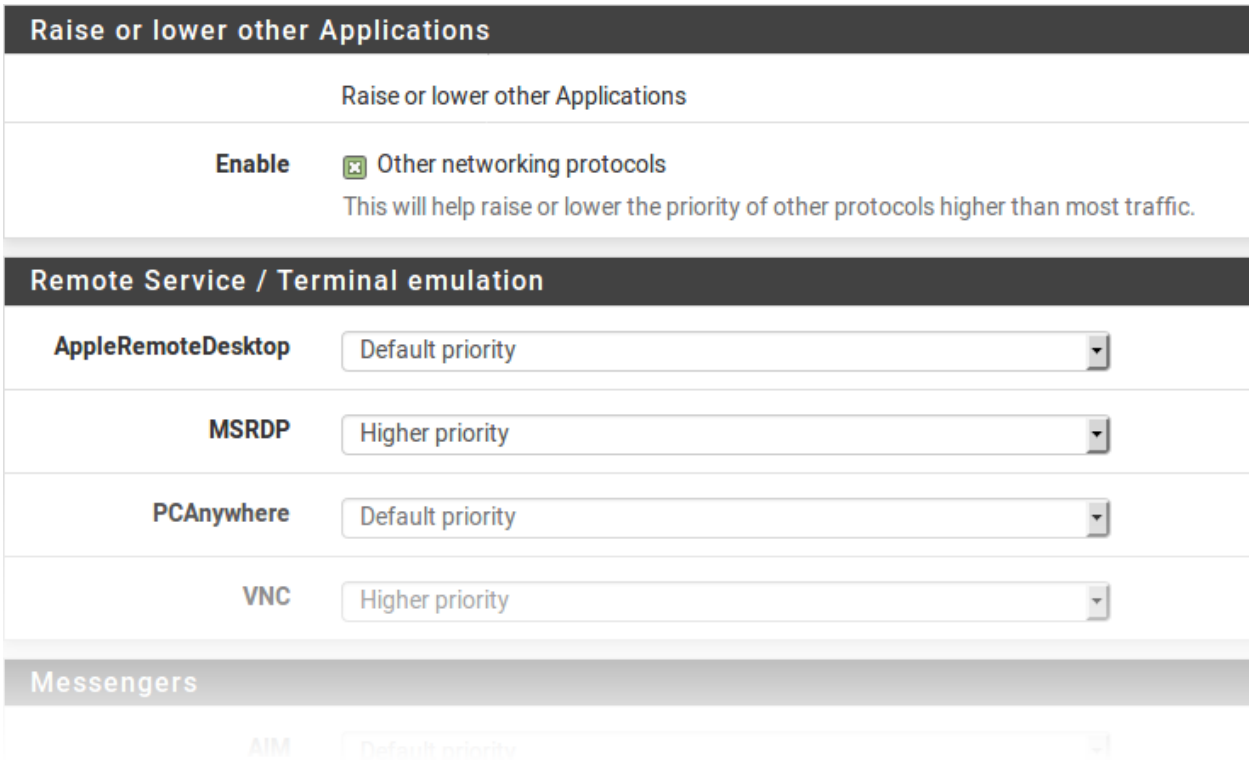


Fig. 7: Alzare o abbassare le altre applicazioni

19.4.9 Completamento della procedura guidata

Fare clic su **Finire** per completare la procedura guidata. Il firewall creerà quindi tutte le regole e le code per le opzioni abilitate, quindi ricaricherà il set di regole per attivare le nuove impostazioni dello Traffic Shaper.

A causa del firewall che funziona in modo stateful, il firewall può applicare solo le modifiche nello ottimizzazione del traffico alle nuove connessioni. Affinché le nuove impostazioni dello shaping del traffico siano completamente attive su tutte le connessioni, cancellare gli stati.

Per reimpostare il contenuto della tabella di stato:

- Passare a **Diagnostica>Stati**
- Fare clic sulla scheda **Ripristinare gli stati**

- Controllare **Reimpostare la tabella dello stato del firewall**
- Fare clic su **Ripristinare**

19.4.10 Procedura guidata dello shaper e IPv6

La procedura guidata dello shaper crea regole solo per il traffico IPv4. Le regole possono essere regolate manualmente o clonate e impostate per IPv6.

19.5 Monitoraggio delle code

Monitorare lo shaper utilizzando **Stato>Code** per garantire che lo ottimizzazione del traffico funzioni come previsto. Come si può vedere in figura *Code WAN di base*, questa schermata mostra ogni coda elencata per nome, il suo utilizzo corrente e altre statistiche correlate.

Status Queues

Queue	Statistics: PPS	PPS	Bandwidth	Borrows	Suspends	Drops	Length
Interface WAN							
qACK		4.8	2.49 Kbps	0	0	0	0/50
qDefault		60.2	71.73 Kbps	0	0	0	0/50
qGames		0.0	0 bps	0	0	0	0/50
qOthersHigh		3.1	5.36 Kbps	0	0	0	0/50
qOthersLow		0.0	0 bps	0	0	0	0/50

Fig. 8: Code WAN di base

Coda Il nome della coda dello Traffic Shaper.

Statistiche Una barra grafica che mostra come «completa» è questa coda.

PPS La velocità dei dati in coda in pacchetti al secondo (PPS)

Larghezza di banda La velocità dei dati in coda in bit al secondo (ad esempio Mbps, Kbps, bps).

Prestiti Prendere in prestito accade quando una coda vicina non è completa e la capacità è presa in prestito da lì. Il contatore si sospensione indica quando si verifica un'azione di ritardo. Il contatore di sospensione viene utilizzato solo con il pianificatore CBQ e dovrebbe essere zero quando sono in uso altri pianificatori.

Cali I cali si verificano quando il traffico in una coda viene eliminato a favore del traffico con priorità più elevata. I cali sono normali e questo non significa che una connessione completa venga interrotta, solo un pacchetto. Di solito, un lato della connessione vedrà che un pacchetto è stato perso e quindi bisogna inviarlo nuovamente, spesso rallentando il processo per evitare cadute future.

Lunghezza Il numero di pacchetti nella coda in attesa di essere trasmessi, oltre la dimensione totale della coda.

19.6 Personalizzazione avanzata

Le regole e le code generate dalla procedura guidata dello shaper potrebbero non essere adatte per una rete. I dispositivi di rete possono utilizzare servizi che devono essere stabilizzati che non sono elencati nella procedura guidata, giochi che utilizzano porte diverse o altri protocolli che devono essere limitati.

Dopo che le regole di base sono state create dalla procedura guidata, è relativamente facile modificare o copiare tali regole per apportare modifiche ad altri protocolli.

19.6.1 Modificare le code dello shaper

Le code sono dove la larghezza di banda e le priorità sono allocate dallo shaper. Ogni coda ha impostazioni specifiche per il pianificatore che è stato scelto nella procedura guidata (*tipi di pianificatore ALTQ*). Le code possono anche essere assegnate ad altri attributi che controllano il loro comportamento. Le code possono essere gestite in **Firewall>Traffic Shaper**. Fare clic su un nome di coda nell'elenco o nell'albero mostrato nelle schede **Tramite interfaccia** o **Tramite coda**, come mostrato nella figura *Elenco delle code dello Traffic Shaper*

> **Avvertimento:** La creazione o la modifica di code è solo per utenti avanzati. È un compito complesso con risultati potenti, ma senza una conoscenza approfondita delle impostazioni coinvolte la migliore pratica è quella di attenersi alle code generate dalla procedura guidata piuttosto che cercare di creare nuove code.

Per modificare una coda, fare clic sul suo nome nell'elenco/albero.

Per eliminare una coda, fare clic una volta per modificare la coda, quindi fare clic su Eliminare questa coda. Non eliminare una coda se è ancora riferimento per una regola firewall.

Per aggiungere una nuova coda, fare clic sull'interfaccia o sulla coda primaria in cui verrà posizionata la nuova coda, quindi fare clic su Aggiungere una nuova coda.

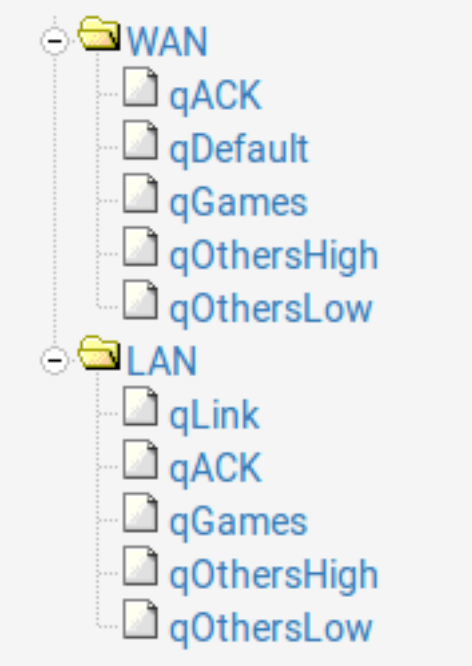


Fig. 9: Elenco delle code dello Traffic Shaper

Quando si modifica una coda, ciascuna delle opzioni deve essere attentamente considerata. Per ulteriori informazioni su queste impostazioni rispetto a quanto indicato qui, visitare la pagina delle FAQ di PF riguardo le Code e la priorità dei pacchetti o leggere il libro *Filtro dei pacchetti di PF con OpenBSD* .

Nome Il nome della coda deve essere compreso tra 1-15 caratteri e non può contenere spazi. La convenzione più comune è quella di iniziare il nome di una coda con la lettera "q" in modo che possa essere più facilmente identificata nel set di regole.

Priorità La priorità della coda. Può essere qualsiasi numero da 0-7 per CBQ e 0-15 per PRIQ. Sebbene HFSC possa supportare le priorità, il codice corrente non li onora durante l'esecuzione dello shaping. Le code con numeri più alti sono preferite dallo shaper quando c'è un sovraccarico, quindi posizionare le code di conseguenza. Ad esempio, il traffico VoIP ha la priorità più alta, quindi sarebbe impostato su un 7 su CBQ o 15 su PRIQ. Il traffico di rete Peer-to-Peer, che può essere ritardato a favore di altri protocolli, sarebbe impostato su 1.

Larghezza di banda (code di root) La quantità di larghezza di banda disponibile su questa interfaccia nella direzione in uscita. Ad esempio, le code di root dell'interfaccia di tipo WAN elencano la velocità di caricamento. Le interfacce di tipo LAN elencano la somma totale di tutta la larghezza di banda di download dell'interfaccia WAN.

Limite della coda Il numero di pacchetti che possono essere tenuti in una coda in attesa di essere trasmessi dallo shaper. La dimensione predefinita è **50**.

Opzioni del pianificatore Ci sono cinque diverse opzioni di pianificazione che possono essere impostate per una determinata coda:

Coda predefinita Seleziona questa coda come predefinita, quella che gestirà tutti i pacchetti non corrispondenti su un'interfaccia. Ogni interfaccia deve avere una sola coda predefinita.

Rilevamento precoce casuale (ROSSO) Un metodo per evitare la congestione su un link. Quando impostato, lo shaper tenterà attivamente di assicurarsi che la coda non si riempia. Se la larghezza di banda è superiore al massimo indicato per la coda, si verificheranno delle cadute. Inoltre, possono verificarsi cadute se la dimensione media della coda si avvicina al massimo. I pacchetti eliminati vengono scelti a caso, quindi è più probabile che le connessioni che utilizzano più larghezza di banda vedano le cadute. L'effetto è che la larghezza di banda è limitata in modo equo, incoraggiando l'equilibrio. RED dovrebbe essere utilizzato solo con le connessioni TCP poiché TCP è in grado di gestire i pacchetti persi e gli host possono inviare nuovamente i pacchetti TCP quando necessario.

Rilevamento precoce casuale in uscita e in entrata (RIO) Abilita il rosso con in/out, il che si traduce in una media delle code mantenuta e controllata rispetto ai pacchetti in entrata e in uscita.

Notifica esplicita della dongestione (ECN) Insieme al ROSSO, consente l'invio di messaggi di controllo che accelerano le connessioni se entrambe le estremità supportano ECN. Invece di far cadere i pacchetti come farà normalmente il rosso, imposterà un flag nel pacchetto che indica la congestione della rete. Se l'altro lato vede e rispetta il contrassegno, la velocità del trasferimento in corso sarà ridotta.

Coda attiva su Codel Un flag per contrassegnare questa coda come coda attiva per la disciplina dello shaper del Codel.

Descrizione Testo opzionale che descrive lo scopo della coda.

Larghezza di banda (Curva di servizio /Pianificatore) L'impostazione della larghezza di banda dovrebbe essere una frazione della larghezza di banda disponibile nella coda primaria, ma deve anche essere impostata con una consapevolezza delle altre code vicine. Quando si utilizzano le percentuali, il totale di tutte le code sotto una determinata primaria non può superare il 100%. Quando si utilizzano i limiti assoluti, i totali non possono superare la larghezza di banda disponibile nella coda primaria.

Opzioni specifiche del pianificatore Il prossimo passo sono le opzioni specifiche del pianificatore. Cambiano a seconda che una coda utilizzi HFSC, CBQ o PRIQ. Sono tutti descritti nei *tipi di pianificatore ALTQ*.

Fare clic su **Salvare** per salvare le impostazioni della coda e tornare all'elenco delle code, quindi fare clic su **Applicare le modifiche** per ricaricare le code e attivare le modifiche.

19.6.2 Modificare le regole dello shaper

Le regole dello ottimizzazione del traffico controllano il modo in cui il traffico viene assegnato in code. Se una nuova connessione corrisponde a una regola dello Traffic Shaper, il firewall assegnerà i pacchetti per tale connessione nella coda specificata da tale regola.

La corrispondenza dei pacchetti viene gestita dalle regole del firewall, in particolare nella scheda **Dinamiche**. Per modificare le regole dello shaper:

- Passare a **Firewall>Regole**
- Fare clic sulla scheda **Dinamiche**
- **Trovare la regola da modificare nell'elenco, come mostrato nella** figura *Elenco delle regole dello Traffic Shaper*
- **Fare clic su**  **per modificare una regola esistente o su**  per creare una copia di una regola
- Effettuare le regolazioni necessarie per abbinare diverse connessioni
- **Salvare e Applicare le modifiche come al solito durante si modificano** le regole del firewall

Le code possono essere applicate utilizzando le regole di *passaggio* sulle schede dell'interfaccia, ma la procedura guidata crea solo regole sulla scheda **Dinamiche** utilizzando l'azione *corrispondenza* che non influisce sul fatto che una connessione sia passata o bloccata; fa solo code al traffico. Poiché queste regole funzionano allo stesso modo di qualsiasi altra regola, qualsiasi criterio utilizzato per abbinare le connessioni può essere utilizzato per fare la coda.

Vedi anche:

Per ulteriori informazioni sulle regole dinamiche, vedere *Regole dinamiche* e *Configurazione delle regole del firewall* per informazioni sulle regole del firewall in generale.

Floating WAN LAN WANV6 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 /420 B	IPv4 UDP	*	*	*	27000 - 27030	*	qGames		m_Game Steam-game-udp outbound	
	0 /420 B	IPv4 TCP	*	*	*	27000 - 27030	*	qACK/qGames		m_Game Steam-game-tcp outbound	
	0 /420 B	IPv4 UDP	*	*	*	27015 - 27030	*	qGames		m_Game Steam-hltv outbound	
	0 /420 B	IPv4 UDP	*	*	*	4380	*	qGames		m_Game Steam-1 outbound	
	0 /420 B	IPv4 UDP	*	*	*	1200	*	qGames		m_Game Steam-2 outbound	
	0 /420 B	IPv4 UDP	*	*	*	3478 - 3480	*	qGames		m_Game Steam-voice outbound	
	0 /420 B	IPv4 TCP	*	*	*	6667	*	qACK/qGames		m_Game Wii-Consoles-TCP-1 outbound	

Fig. 10: Elenco delle regole dello Traffic Shaper

Suggerimenti per la corrispondenza delle regole dello shaper

Le connessioni possono essere difficili da abbinare correttamente a causa di diversi fattori, tra cui:

- **Il NAT si applica prima che le regole del firewall in uscita possano** corrispondere alle connessioni, quindi per le connessioni che hanno il NAT in uscita si applica quando lasciano un'interfaccia di tipo WAN, la sorgente dell'indirizzo IP privato è nascosta dal NAT e non può essere abbinata a una regola.
- **Alcuni protocolli come Bittorrent utilizzeranno porte casuali o le** stesse porte di altri servizi.
- **I protocolli multipli che utilizzano la stessa porta non possono** essere distinti dal firewall.
- **Un protocollo può utilizzare una gamma di porte così ampia che non** può essere distinto da altro traffico.

Mentre molti di questi elementi non possono essere risolti direttamente dal firewall, ci sono modi per aggirare queste limitazioni in alcuni casi.

Per abbinare da una sorgente di indirizzo privato in uscita nelle regole dinamiche della WAN, prima contrassegnare il traffico mentre passa su un'interfaccia locale. Ad esempio, abbinare in entrata sulla LAN e usare il campo **Tag** avanzato per impostare un valore, quindi usare il campo **Taggato** sulla regola dinamica del lato WAN per abbinare la stessa connessione che esce dal firewall. In alternativa, accodare il traffico mentre entra nella LAN con una regola di passaggio anziché quando esce da una WAN.

Abbinare per indirizzo invece che porta/protocollo dove possibile per risolvere protocolli ambigui. In questi casi, la sorgente locale o la destinazione remota possono essere un singolo indirizzo o un piccolo insieme di indirizzi. Ad esempio, la corrispondenza del traffico VoIP è molto più semplice se il firewall può corrispondere al trunk SIP remoto o al PBX piuttosto che tentare di abbinare una vasta gamma di porte per RTP (ad esempio 10000 - 20000).

Se BitTorrent è consentito su una rete ma deve essere modellato, dedicare un dispositivo locale specifico a cui è consentito utilizzare bittorrent e quindi stabilizzare tutte le connessioni da/per quel dispositivo come il traffico Peer-to-Peer.

19.6.3 Rimozione delle impostazioni dello Traffic Shaper

Per rimuovere tutte le code e le regole dello Traffic Shaper create dalla procedura guidata:

- Passare a **Firewall>Traffic Shaper**
- Fare clic sulla scheda **Per interfaccia**
- Fare clic su  **Rimuovere lo shaper**
- Fare clic su **OK** sul prompt di conferma

19.7 Limitatori

I limitatori sono un metodo alternativo di ottimizzazione del traffico. I limitatori utilizzano dummynet(4) per stabilire i limiti di larghezza di banda ed eseguire altre attività di assegnazione delle priorità e non si basano su ALTQ. I limitatori sono attualmente l'unico modo per ottenere l'indirizzo per IP o la limitazione della velocità di banda per rete utilizzando il software di Firew4LL. I limitatori sono utilizzati anche internamente dal captive portal per i limiti di larghezza di banda per utente.

I limitatori sono gestiti in **Firewall>Traffic Shaper** nella scheda **Limitatori**.

Come HFSC e CBQ, i limitatori possono essere annidati con code all'interno di altre code. O limitatori a livello di root (chiamati anche pipe), possono avere limiti di larghezza di banda e ritardi, mentre limitatori secondari (chiamati anche code), possono avere priorità (chiamate anche pesi). I limiti di larghezza di banda possono essere opzionalmente mascherati dall'indirizzo IP di sorgente o di destinazione, in modo che i limiti possano essere applicati per indirizzo IP o rete anziché come gruppo generale.

I limitatori sono quasi sempre utilizzati in coppia: uno per il traffico in entrata e uno per il traffico in uscita.

Secondo la sua pagina principale, il sistema dummynet(4) è stato originariamente progettato come mezzo per testare il controllo della congestione TCP ed è cresciuto da lì. A causa di questo scopo, una caratteristica unica dei limitatori è che possono essere utilizzati per indurre la perdita di pacchetti artificiali e ritardo nel traffico di rete. questo viene utilizzato principalmente nella risoluzione dei problemi e test (o per essere dannoso e giocare uno scherzo a qualcuno), e non si trovano spesso in produzione.

19.7.1 Usi per limitatori

L'uso principale per i limitatori è quello di applicare limiti di larghezza di banda per gli utenti o protocolli specifici, ad esempio "Massimo di 1Mbit/s per SMTP", o "Solo il PC di Joe può utilizzare 5Mbit/s". I limitatori possono applicare un indirizzo per IP o un limite per rete, ad esempio «Tutti gli utenti in 192.168.50.0/24 possono utilizzare un massimo di 3Mbit/s ciascuno» o"La rete ospite e la rete pubblica possono utilizzare 1Mbit/s per ogni segmento».

I limitatori sono l'unico tipo di pianificatori disponibile nel software Firew4LL che è in grado di superare la sottoscrizione (oversubscription) in questo modo. Lo shaper ALTQ richiede che tutte le code secondarie riassumano fino a non più della velocità della coda primaria, ma i limitatori mascherati consentono un limite impostato a tutti gli indirizzi IP che possono essere incanalati attraverso il limitatore dalle regole del firewall.

Concettualmente, considerare un limitatore come un secchio di larghezza di banda. Tutto il traffico che scorre attraverso un limitatore smascherato trae larghezza di banda dallo stesso secchio. Mascherare un limitatore imposta efficacemente più secchi della stessa dimensione, uno per gruppo mascherato. Se si tratta di un singolo host o di un'intera rete dipende dal valore della maschera.

I limitatori possono anche consentire la larghezza di banda riservata limitando tutto tranne un protocollo specifico che può quindi consumare tutta la larghezza di banda rimanente. In questo tipo di configurazione su un collegamento 10Mbit/s il firewall passerebbe il traffico da, ad esempio, un server SIP senza limitatore. Quindi il firewall userebbe una regola di passaggio per tutto l'altro traffico con un limite di 8Mbit/s. ciò consentirebbe al server SIP di utilizzare tutta la larghezza di banda desiderata, ma avrebbe sempre un minimo di 2Mbit/s per se stesso.

19.7.2 Come funzionano i limitatori

I limitatori, come ALTQ, mantengono il traffico a un certo punto facendo cadere o ritardando i pacchetti per ottenere una velocità di linea specifica. Di solito approfittando di meccanismi integrati da protocolli che rilevano la perdita e si allontanano a una velocità sostenibile.

Nelle situazioni in cui i pacchetti sono accodati sotto la stessa pipa principale, il firewall considera i loro pesi quando ordina i pacchetti prima che li invii. A differenza delle priorità in CBQ e PRIQ, il peso di una coda in un limitatore non lo affamerà mai per la larghezza di banda.

19.7.3 Limitatori e IPv6

I limitatori funzionano con IPv6, anche se richiede regole IPv4 e IPv6 separate da applicare correttamente i limitatori.

19.7.4 Limitazioni

Le pipe dei limitatori non hanno l'idea di prendere in prestito larghezza di banda da altri tubi. Un limite è sempre un limite superiore duro.

I limitatori usano IPFW, quindi ci sarà un sovraccarico aggiuntivo (anche se piccolo) dal modulo del kernel IPFW e dall'elaborazione dei pacchetti extra coinvolti.

I limitatori non possono garantire in modo efficace un importo minimo di larghezza di banda per una pipa o una coda, solo un massimo.

Le code secondarie non possono avere valori di larghezza di banda, quindi una pipa non può essere suddivisa in pipe più piccole per le code. Le code secondarie possono utilizzare solo i pesi per dare la priorità ai pacchetti all'interno di una pipa.

Il sovraccarico del ritardi e dell'accodamento dei pacchetti può causare un aumento dell'utilizzo di mbuf. Per ulteriori informazioni sull'aumento della quantità di mbuf disponibili, vedere *Ottimizzazione dell'hardware e risoluzione dei problemi*.

Limitatori e Multi-WAN

Quando si utilizzano limitatori con Multi-WAN, i limiti per i gateway non predefiniti devono essere applicati utilizzando le regole *in uscita* e configurato con il gateway appropriato.

19.7.5 Creazione di limitatori

I limitatori sono gestiti in Firewall>Traffic Shaper nella scheda Limitatori. Per creare un nuovo limitatore di livello root (pipa), fare clic su  Nuovo limitatore. Per creare un limitatore secondario (coda), fare clic su un limitatore esistente in base al quale può essere creato e fare clic su  Aggiungere una nuova coda.

Suggerimento: In quasi tutti i casi, i limitatori esistono in coppie dello stesso livello (ad esempio due pipe o due code): uno per il traffico in entrata e uno per il traffico in uscita. Quando si creano nuovi limitatori o code, crearne uno per ogni direzione.

Abilitare Selezionare la casella per abilitare questo limitatore. Se il limitatore è disabilitato, non sarà disponibile per l'uso dalle regole del firewall.

Nome Questo definisce il nome del limitatore, come apparirà per la selezione sulle regole del firewall. Il nome deve essere alfanumerico e può anche includere - e _.

Suggerimento: Quando si sceglie un nome, evitare di utilizzare In e Out poiché lo stesso limitatore, se utilizzato su WAN e LAN, sarebbe utilizzato nella direzione *In* su un'interfaccia e in direzione *Out* su un altro. La migliore pratica è quella di utilizzare verso Down o Download e Up o Upload.

Larghezza di banda (Pipe) Questa sezione definisce un valore di larghezza di banda per il pipe, o più larghezze di banda se le pianificazioni sono coinvolte. Questa opzione non viene visualizzata quando si modifica un limitatore fsecondario (coda).

> **Larghezza di banda** La parte numerica della larghezza di banda per il pipe, ad esempio 3 o 500.
>
> **Tipo di BW** L'unità per il campo della **larghezza di banda**, come *Mbit/s*, *Kbit/s* o *Bit/s*.

Pianificazione Se il firewall ha definito delle pianificazioni (*regole basate sul tempo*), il firewall le offre in questo elenco. Quando le pianificazioni sono in uso sul firewall, il limitatore può avere un valore di larghezza di banda per ogni potenziale pianificazione. Definirle facendo clic su  **Aggiungere pianificazione** per aggiungere un'altra definizione di larghezza di banda.

Se un limitatore contiene più specifiche di larghezza di banda, devono utilizzare ciascuna una pianificazione diversa. Ad esempio, se il firewall ha una pianificazione "Giornata di lavoro", deve anche avere una pianificazione "Ore non lavorative" che contiene tutto il tempo non incluso in "Giornata di lavoro" per la seconda specifica della larghezza di banda.

Maschera Questo elenco a discesa controlla come il limitatore maschererà gli indirizzi nelil pipe o nella coda.

Nessuno Se impostato su *nessuno*, il limitatore non esegue alcun mascheramento. La larghezza di banda delil pipe verrà applicata a tutto il traffico nel suo complesso.

Indirizzo di sorgente/destinazione Quando un limitatore è impostato per *indirizzo di sorgente* o *indirizzo di destinazione*, il limite di larghezza di banda delil pipe verrà applicato su base all'indirizzo IP o su base sottorete, a seconda dei bit di mascheramento, utilizzando la direzione scelta nel mascheramento.

In generale, un limitatore dovrebbe mascherare l'"**indirizzo di sorgente** sui limitatori di **Upload** (In) per le interfacce di tipo LAN e l'"**indirizzo di destinazione** sui limitatori di **Download** (Out) sulle interfacce di tipo LAN. Analogo allo scambio della direzionalità dei limitatori quando si applica a LAN e WAN, anche il mascheramento viene scambiato, quindi lo stesso limitatore mascherato impostato per **In** sulla LAN dovrebbe essere usato per **Out** sulla WAN.

Maschera di bit Ci sono caselle separate per controllare il mascheramento degli indirizzi per IPv4 e IPv6. Per IPv4 un valore di *32* per i bit della maschera IPv4 imposta un limite di indirizzo per IPv4, che è l'uso più comune. Per un limite per l'indirizzo IPv6, utilizzare *128* come valore di bit della maschera IPv6.

Per creare maschere per sottorete o simili, immettere i bit della sottorete nel campo appropriato per i bit della maschera IPv4 o IPv6, ad esempio *24* per limitare IPv4 in gruppi di sottoreti /24.

Descrizione Un breve testo opzionale per spiegare lo scopo di questo limitatore.

Opzioni avanzate Opzioni aggiuntive che variano quando si modifica una pipa o una coda.

Ritardo (pipe) L'opzione di **ritardo** si trova solo suli pipe dei limitatori. Introduce un ritardo artificiale (latenza), specificato in millisecondi, nella trasmissione di qualsiasi pacchetto nelil pipe del limitatore. Questo viene in genere lasciato vuoto in modo che i pacchetti vengano trasmessi il più velocemente possibile dal firewall. Questo può essere utilizzato per simulare connessioni ad alta latenza come uplink satellitari per test di laboratorio.

Peso (Code) L'opzione **peso** si trova solo sui limitatori secondari (code). Questo valore può variare da 100. Valori più alti danno maggiore precedenza ai pacchetti in una determinata coda. A differenza delle priorità PRIQ e CBQ, una coda scarsamente ponderata non rischia di essere affamata di larghezza di banda dal firewall.

Tasso di perdita di pacchetti Un altro metodo per degradare artificialmente il traffico. Il **tasso di perdita di pacchetti** può essere configurato per eliminare una certa frazione di pacchetti che entrano nel limitatore. Il valore è espresso come rappresentazione decimale di una percentuale, quindi 0,01 è 1% o un pacchetto su cento è caduto. Questo campo viene in genere lasciato vuoto in modo che ogni pacchetto venga consegnato dal firewall.

Dimensione della coda Imposta la dimensione della coda, specificata negli slot della coda, utilizzato per gestire il ritardo di accodamento. Lasciato vuoto, il valore predefinito è 50 slot, che è il valore consigliato. I collegamenti a bassa velocità potrebbero aver bisogno di una dimensione della coda inferiore per funzionare in modo efficiente. Collegamenti ad alta velocità possono avere bisogno di più slot.

Suggerimento: nei casi in cui ci sono diversi limitatori o limitatori con valori di grandi **dimensioni della coda**, potrebbe essere necessario impostare un **sistema sintonizzabile** per aumentare il valore della rete.inet.ip.dummynet.pipe_slot_limit sopra il numero totale di lotti di coda configurati tra tutte i pipe e le code.

Dimensione del (bucket) La dimensione del secchio, specificata anche negli slot, imposta la dimensione della tabella hash utilizzata per l'archiviazione delle code. Il valore predefinito è 64. Deve essere un valore numerico compreso tra 16 e 65536, incluso. Questo valore viene in genere lasciato vuoto.

Per ulteriori informazioni su questi valori, consultare la pagina principale di ipfw(8), nella sezione intitolata «Configurazione dello Traffic Shaper(Dum-mynet)".

19.7.6 Assegnazione e utilizzo di limitatori

I limitatori vengono assegnati utilizzando le regole del firewall tramite i selettori di **pipe In/Out** in **Opzioni avanzate**. Qualsiasi potenziale criterio di corrispondenza supportato da una regola del firewall può assegnare il traffico a un limitatore.

La cosa più importante da ricordare quando si assegna un limitatore a una regola è che i campi **In** e **Out** sono designati

dal punto di vista del firewall stesso.

Ad esempio, in una configurazione firewall con una singola LAN e una singola WAN, il traffico in entrata su un'interfaccia LAN sta andando verso Internet, cioè i dati *sono caricati*. Il traffico in uscita sull'interfaccia LAN sta andando verso il PC client, cioè dati *sono scaricati*. Sull'interfaccia WAN la direzionalità è invertita; il traffico in entrata proviene da Internet al client (download) e il traffico in uscita va dal client a Internet (upload).

Nella maggior parte dei casi, una regola del firewall avrà sia un limitatore **In** che un limitatore **Out**, ma solo il limitatore **In** è richiesto dal firewall per limitare il traffico in un'unica direzione.

I limitatori possono essere applicati alle normali regole di interfaccia o alle regole dinamiche. Durante il floating nella direzione *out*, le selezioni In/Out vengono capovolte concettualmente.

19.7.7 Controllo dell'utilizzo limitatore

Informazioni sui limitatori attivi possono essere trovate in **Diagnostica>Informazioni sul limitatore**. Qui, ogni limitatore e coda secondaria è mostrata in formato testo.

La larghezza di banda e i parametri impostati per ciascun limitatore vengono visualizzati dalla pagina, insieme al livello di traffico corrente che si sposta all'interno del limitatore. Nel caso di limitatori mascherati, il firewall visualizza la larghezza di banda di ciascun indirizzo IP o gruppo mascherato.

19.8 Ottimizzazione del traffico e VPN

Le seguenti discussioni riguardano principalmente lo shaping ALTQ. I limitatori funzioneranno bene con le VPN come farebbero con qualsiasi altra interfaccia e regole. Solo lo shaper ALTQ richiede una considerazione speciale.

Lo ottimizzazione del traffico con VPN è un argomento difficile perché il traffico VPN è considerato separato dal, ma anche una parte del, traffico WAN attraverso il quale scorre. Se la WAN è 10 Mbit/s, allora la VPN può anche utilizzare 10Mbit/s, ma non ci sono in realtà 20Mbit/s di larghezza di banda da considerare, solo 10Mbit/s. Così, i metodi di stabilizzazione che si concentrano più sulla priorità rispetto alla larghezza di banda sono più affidabili, come PRIQ o in alcuni casi, CBQ.

Se tutto il traffico all'interno della VPN deve essere prioritario per il firewall, è sufficiente considerare solo il traffico VPN stesso direttamente sulla WAN, piuttosto che tentare di mettere in coda il traffico sulla VPN separatamente. In questi casi, utilizzare una regola mobile sulla WAN per abbinare il traffico VPN stesso. Il tipo esatto di traffico varia a seconda del tipo di VPN. Il traffico IPsec e PPTP sulla WAN possono essere entrambi prioritari dalla procedura guidata dello shaper e queste regole possono essere utilizzate come esempio per abbinare altri protocolli.

19.8.1 OpenVPN

Con OpenVPN, sul sistema operativo esistono più interfacce, una per VPN. Questo può rendere la stabilizzazione più facile in alcuni casi. Le caratteristiche di OpenVPN possono anche rendere più facile modellare il traffico su WAN e ignorare il tunnel stesso.

Stabilizzazione interna al tunnel

Se sul tunnel vengono trasportate più classi di traffico, è necessario effettuare la prioritizzazione del traffico all'interno del tunnel. Affinché la procedura guidata consideri il traffico in questo modo, la VPN deve essere assegnata come propria interfaccia nella GUI. Per fare ciò, assegnarlo come descritto nell'*Assegnazione e nella configurazione dell'interfaccia*, quindi utilizzare la procedura guidata dello shaper come se si trattasse di un'interfaccia WAN separata e classificare il traffico come al solito.

Stabilizzazione esterna al tunnel (superarare TOS, passtos)

Se la preoccupazione principale è stabilizzare il traffico VoIP su una VPN, un'altra scelta da considerare è l'opzione passtos in OpenVPN, chiamata **Tipo di servizio** nelle opzioni client o server OpenVPN. Questa opzione copia il bit TOS dal pacchetto interno al pacchetto esterno della VPN. Pertanto, se il traffico VoIP ha la parte TOS (DSCP) del set di intestazione del pacchetto, anche i pacchetti OpenVPN avranno lo stesso valore.

Questa opzione è più utile per segnalare i router intermedi sulle esigenze QoS, tuttavia. Sebbene l'opzione DSCP sulle regole del firewall possa corrispondere in base ai bit TOS, come descritto nel *Punto di codice di Diffserv*, tale corrispondenza dovrebbe verificarsi nel pacchetto che crea uno stato del firewall e non sui pacchetti specifici che attraversano tale stato.

Nota: Poiché questa opzione indica ad OpenVPN di copiare i dati dal pacchetto interno al pacchetto esterno, espone alcune informazioni sul tipo di traffico che attraversa la VPN. Indipendentemente dal fatto che la divulgazione delle informazioni, anche se minore, vale il rischio per i guadagni offerti dalla corretta priorità dei pacchetti dipende dalle esigenze dell'ambiente di rete.

19.8.2 IPsec

IPsec è presentato al sistema operativo su una singola interfaccia, non importa quanti tunnel sono configurati e non importa quali WAN sono utilizzate dai tunnel. Ciò rende difficile stabilizzare il traffico IPsec, specialmente quando si cerca di modellare il traffico all'interno di un particolare tunnel IPsec.

Anche l'interfaccia IPsec non si può utilizzare da sola come interfaccia con la procedura guidata. Le regole dinamiche possono corrispondere al traffico della coda sull'interfaccia IPsec, ma nella maggior parte dei casi solo il traffico in entrata verrà accodato come previsto. I risultati effettivi possono variare.

19.9 Risoluzione dei problemi di shaper

ottimizzazione del traffico/QoS è un argomento difficile e può rivelarsi complesso da ottenere la prima volta. Questa sezione copre diverse insidie comuni.

19.9.1 Traffico Bittorrent non utilizza la coda P2P

Bittorrent è noto per non utilizzare porte standard. I client possono dichiarare quale porta altri client utilizzano per raggiungerli, il che significa il caos per gli amministratori di rete che cercano di tracciare il traffico in base alla sola porta. I client possono anche scegliere di crittografare il loro traffico. Le regole regolari dello shaper non hanno alcun modo per esaminare i pacchetti per dire di quale programma sembra essere il traffico, quindi è costretto a fare affidamento sulle porte. Questo è il motivo per cui potrebbe essere una buona idea utilizzare la regola P2P cattura tutto e/o creare regole per ogni tipo di traffico desiderabile e trattare la coda predefinita con priorità bassa.

19.9.2 Stabilizzazione del traffico UPnP

Fuori dalla scatola, il traffico consentito dal demone UPnP finirà nella coda predefinita. Ciò accade perché le regole generate dinamicamente dal demone UPnP non hanno alcuna conoscenza delle code a meno che UPnP non sia configurato per inviare il traffico in una coda specifica.

A seconda di ciò che i dispositivi client che utilizzano UPnP su una rete, questo può essere traffico a bassa priorità come Bittorrent, o traffico ad alta priorità come console di gioco o programmi di chat vocale come Skype.

Per configurare UPnP per utilizzare una coda ALTQ specifica:

- Impostare lo shaping ALTQ e decidere quale coda utilizzare per UPnP e NAT-PMP
- Passare a **Servizi>UPnP e NAT-PMP**
- Immettere il nome della coda ALTQ scelto nel campo **shaping del traffico**
- Fare click su **Salvare**

Questo trucco funziona solo con lo shaper ALTQ. In questo momento, il firewall non è in grado di assegnare il traffico UPnP a un limitatore.

19.9.3 Calcoli della larghezza di banda della coda ACK

Questo è un argomento complesso e la maggior parte degli utenti lo sorvola e indovina un valore sufficientemente alto. Per spiegazioni più dettagliate con formule matematiche, controllare la sezione shaping del traffico dei forum Firew4LL. C'è un post sticky in quella scheda che descrive il processo in grande dettaglio, e c'è anche un foglio di calcolo scaricabile che può essere utilizzato per facilitare il processo.

19.9.4 Perché <x> non è correttamente stabilizzato?

La ragione è quasi sempre una di queste scelte:

- Il traffico corrispondeva a una regola diversa da quella prevista
- Il traffico non corrisponde a nessuna regola

Come per altre domande in questa sezione, questo tende ad accadere a causa delle regole inserite internamente o da altri pacchetti che non hanno conoscenza delle code. Poiché nessuna coda è specificata per una regola, finisce nella coda predefinita o della root e non viene stabilizzata.

Lavorare sulla limitazione potrebbe richiedere di modificare le regole per abbinare meglio il traffico o disabilitare le regole interne che corrispondono al traffico in modi inaspettati. Un'altra tattica è identificare tutto il traffico e quindi utilizzare diverse opzioni di stabilizzazione sulla coda predefinita.

In rari casi, come bittorrent, potrebbe essere impossibile identificare con precisione tutto il traffico di un determinato tipo. Una soluzione alternativa è isolare il traffico su un dispositivo specifico sulla rete e quindi corrispondere in base all'indirizzo del dispositivo client.

19.9.5 La velocità di connessione della WAN cambia

Per aggiornare la velocità di una WAN in caso di modifica, cambiare le code appropriate in **Firewall>Traffic Shaper** per riflettere la nuova velocità.

Le code che devono essere aggiornate sono:

- La coda di root per ogni interfaccia WAN per la velocità di upload
- La coda di root per ogni interfaccia LAN per la velocità di download

- La coda qInternet per ogni interfaccia LAN per la velocità di download

Se questo firewall ha più Wan, la coda della root della LAN e la coda di qInternet deve utilizzare la velocità di download totale di tutte le WAN.

In alternativa, se la procedura guidata ha creato tutte le code e le regole e queste non sono state modificate, completare nuovamente la procedura guidata e aggiornare la velocità utilizzando la procedura guidata.

Lo shaping, del traffico o il servizio di qualità (Quality of Service, QoS) della rete, è un mezzo per dare priorità al traffico di rete. Senza lo ottimizzazione del traffico, i pacchetti vengono elaborati su una base first in/first out (primo ad entrare/primo ad uscire) dal firewall. QoS offre un mezzo per dare priorità a diversi tipi di traffico, assicurando che i servizi ad alta priorità ricevano la larghezza di banda di cui hanno bisogno prima di servizi con priorità minore.

Per semplicità, il sistema di ottimizzazione del traffico nel software di Firew4LL può anche essere indicato come lo "shaper" , e l'atto di shaping del traffico può essere chiamato "shaping".

19.10 Tipi di ottimizzazione del traffico

Ci sono due tipi di QoS disponibili nel software Firew4LL: ALTQ e limitatori.

Il framework di ALTQ viene gestito tramite pf ed è strettamente legato ai driver della scheda di rete. ALTQ può gestire diversi tipi di pianificatore e layout di coda. La procedura guidata dello shaper del traffico configura ALTQ e offre agli amministratori del firewall la possibilità di configurare rapidamente QoS per scenari comuni e consente regole personalizzate per attività più complesse. Tuttavia ALTQ è inefficiente, quindi il throughput massimo potenziale di un firewall viene abbassato in modo significativo quando è attivo.

Il software Firew4LL supporta anche un concetto di shaper separato chiamato Limitatori. I limitatori applicano limiti di larghezza di banda rigidi per un gruppo o per indirizzo IP o rete. All'interno di questi limiti di larghezza di banda, i limitatori possono anche gestire le priorità del traffico.

19.11 Nozioni di base sulla stabilizzazione del traffico

Per gli amministratori che non hanno familiarità con lo shaping del traffico, è come un buttafuori in un club esclusivo. I VIP (pacchetti molto importanti) entrano sempre prima e senza aspettare. I pacchetti regolari devono aspettare il loro turno in linea, e i pacchetti "indesiderabili" possono essere tenuti fuori fino a dopo che la vera festa sia finita. Per tutto il tempo, il club è tenuto a capacità e mai sovraccaricato. Se più Vip arrivano più tardi, potrebbero essere necessari pacchetti regolari per evitare che il posto diventi troppo affollato. I concetti di shaping ALTQ possono essere contro-intuitivi in un primo momento perché il traffico deve essere in coda in un luogo dove il sistema operativo può controllare il flusso di pacchetti. Il traffico in entrata da Internet che va a un host sulla LAN (download) è stabilizzato lasciando l'interfaccia LAN dal firewall. Allo stesso modo, il traffico che va dalla LAN a Internet (caricamento) viene stabilizzato quando si lascia la WAN.

Per ALTQ, ci sono code di ottimizzazione del traffico e regole di shaping del traffico. Le code allocano larghezza di banda e priorità. Le regole di ottimizzazione del traffico controllano il modo in cui il traffico viene assegnato in quelle code. Le regole per lo shaper funzionano come le regole del firewall e consentono le stesse caratteristiche di corrispondenza. Se un pacchetto corrisponde a una regola di shaper, verrà assegnato nelle code specificate da tale regola. Nel software Firew4LL, le regole shaper vengono gestite principalmente nella scheda **Floating** utilizzando l'azione *Corrispondenza* che assegna il traffico in code, ma le regole su qualsiasi interfaccia possono assegnare il traffico in code utilizzando l'azione *Passare*.

Le regole del limitatore sono gestite in modo diverso. I limitatori si applicano alle regole di passaggio regolari e applicano i loro limiti al traffico mentre entra e lascia un'interfaccia. I limitatori esistono quasi sempre in coppia: uno per il traffico di direzione «download» e uno per il traffico di direzione » upload.

CAPITOLO 20

Bilanciamento del carico di rete

20.1 Configurazione

20.1.1 Pool

Per configurare i pool:

- Passare a **Servizi>Bilanciamento del carico**
- Fare clic sulla scheda **Pool**
- Fare clic su  **Aggiungere** per aggiungere un nuovo pool
- Configurare le opzioni del pool come spiegato di seguito:

  Nome Un nome per il pool. Il nome è il modo per fare riferimento al pool durante la configurazione del virtual server che utilizzerà questo pool. Questo nome deve rispettare gli stessi limiti di un alias o di un nome di interfaccia. Solo lettere e numeri, l'unico separatore consentito è il trattino basso. .. Nota:: questo nome non può essere lo stesso di un alias esistente.

  Modalità Selezionare *bilanciamento del carico* per bilanciare il carico tra tutti i server del pool o *Failover manuale* per utilizzare sempre i server nell'elenco abilitato e poterli spostare manualmente tra lo stato abilitato e disabilitato.

  Descrizione Una descrizione più lunga opzionale per il pool.

  Porta Questa è la porta su cui i server sono in ascolto internamente. Questa può essere diversa dalla porta esterna, che viene definita in seguito nella configurazione del virtual server. Un alias può anche essere utilizzato per definire più porte, tuttavia, se viene utilizzato un alias, bisogna utilizzare lo stesso alias della porta qui e nella configurazione del virtual server.

  Riprovare Questo definisce il numero di volte in cui un server verrà contattato dal monitor prima di essere dichiarato inattivo.

  Monitorare Questo definisce il tipo di monitoraggio da utilizzare, che è il modo in cui il bilanciamento del carico determina se i server sono attivi e utilizzabili. Selezionando *TCP*, il bilanciatore

si connette alla porta precedentemente definita in **Porta** e, se non è in grado di connettersi a tale porta, il server viene considerato inattivo. Scegliendo *ICMP* farà in modo che si monitorino i server definiti con l'invio di un ping ICMP, e li segnerà down se non rispondono. Ci sono molti altri tipi di monitoraggio e possono essere personalizzati. Essi sono trattati in modo più dettagliato più avanti nel capitolo.

Indirizzo IP del server E' dove sono elencati gli indirizzi IP interni dei server nel pool. Inseriscili uno alla volta, facendo clic su **Aggiungere al pool** in seguito.

Membri del pool corrente Questo campo mostra l'elenco dei server in questo pool. Un server può essere rimosso dal pool facendo clic sul suo indirizzo IP e quindi facendo clic su **Rimuovere**. Ci sono due liste in questa sezione, **Pool disabilitati** e **Abilitato (predefinito)**. I server nell'elenco **Abilitato (predefinito)** sono attivi e utilizzati, i server nell'elenco dei **Pool disabilitati** non vengono mai utilizzati. L'elenco del **Pool disabilitati** viene utilizzato principalmente con la modalità di *Failover manuale*. I server possono essere spostati tra gli elenchi selezionandoli e facendo clic su  o 
.

- Fare click su **Salvare**

Se è necessario un failover automatico, creare un secondo pool da utilizzare come Pool di fall-back, contenente il set di backup degli indirizzi IP del server.

20.1.2 Virtual Server

Configurare un virtual server per gestire le connessioni client:

- Passare a **Servizi>Bilanciamento del carico**
- Fare clic sulla scheda **Server virtuali**
- Fare clic su  Aggiungere per aggiungere un nuovo Server virtuale
- Configurare le opzioni del virtual server come spiegato di seguito:

  Nome Nome del virtual server. Questo è per riferimento, ma deve anche rispettare gli stessi limiti di un alias o nome dell'interfaccia. Solo lettere e numeri, l'unico separatore consentito è un trattino basso. Non ci sono spazi o barre.

  Descrizione Una descrizione più lunga opzionale per il server virtuale. Il suo solo a scopo è di essere un riferimento e non ha limiti di formattazione.

  Indirizzo IP Dove gli indirizzi IP vengono inseriti per l'utilizzo da parte del virtual server. È di solito l'indirizzo IP della WAN o un indirizzo IP virtuale della WAN. Deve essere un indirizzo IP statico. Un VIP del CARP può essere utilizzata anche per una configurazione ad elevata disponibilità. Per ulteriori informazioni sull'elevata disponibilità e il VIP del CARP, fare riferimento a *Elevata disponibilità*. È possibile utilizzare un VIP Alias IP o un proxy dell'ARP del VIP (solo modalità TCP). Inoltre, un Alias può anche essere utilizzato qui per specificare più indirizzi IP su cui questo virtual server può accettare connessioni.

  Nota: in modalità TCP, gli indirizzi IP qui specificati non sono associati a livello del sistema operativo, il che significa che relayd come demone non è associato e in ascolto direttamente su queste porte.

Porta Questa è la porta su cui il virtual server accetterà le connessioni. Può essere diversa dalla porta utilizzata internamente dai server del pool. Un alias può essere utilizzato per definire più porte, tuttavia, se lo stesso alias di porta deve essere utilizzato qui e nella configurazione del Pool.

Pool del virtual server Dove viene selezionato il pool configurato in precedenza. Le connessioni all'indirizzo IP e alla porta definite in questa schermata verranno indirizzate agli indirizzi IP e alle porte configurate nel pool.

Pool di fall-back Pool alternativo a cui i client sono indirizzati se tutti i server nel pool primario sono inattivi. Se non esiste un server alternativo, lasciare questo impostato su *Nessuno*, anche se il risultato sarà l'inaccessibilità se tutti i server nel pool sono inattivi. Se non altro, per evitare che il server sia completamente inattivo, impostare un semplice server web per restituire una pagina di manutenzione di base per qualsiasi richiesta e utilizzarla come pool di fall-back.

Protocollo di relay Il protocollo di relay può essere *TCP* o *DNS*, a seconda di cosa farà questo relay.

- In modalità *TCP*, relayd agisce come una porta forward avanzata, dirigendo le connessioni come se stessero colpendo una regola NAT tradizionale. I server vedranno l'indirizzo IP di sorgente originale del client, non agisce come un proxy.
- In modalità *DNS*, relayd agisce come un proxy DNS. Bilancerà il carico su più server DNS, ma l'indirizzo IP del client originale viene perso. I server Pool vedranno il firewall come sorgente della richiesta del DNS. Tenetelo a mente quando si impostano viste o restrizioni di query basate sulla sorgente dei server DNS coinvolti nel bilanciamento del carico.
  - Fare click su **Presentare**
  - Fare click su **Applicare le modifiche**

Avvertimento: se tutti i membri del Pool di virtual serveri e i membri del pool di fall-back sono inattivi, relayd agirà come se il bilanciamento del carico non gestisse le connessioni per l'indirizzo IP e la porta del virtual server. Se l'indirizzo IP e la porta utilizzati sono utilizzati anche da un altro servizio o regola NAT, potrebbe essere accidentalmente esposto ai client.

20.1.3 Monitoraggi

Esistono cinque tipi di Monitor predefiniti di base: ICMP, TCP, HTTP, HTTPS e SMTP. Ulteriori tipi personalizzati possono essere aggiunti per rilevare meglio specifici tipi di guasti.

Monitoraggi predefiniti

I monitoraggi predefiniti sono inclusi nella configurazione predefinita e sono:

ICMP Invia una richiesta ICMP echo al server di destinazione e si aspetta una risposta ICMP echo.

TCP Tenta di aprire una connessione per la porta TCP all'indirizzo IP e per la porta di destinazione. Se la porta può essere aperta (un handshake TCP a 3 vie), allora riesce, se la connessione viene rifiutata o scade, fallisce.

HTTP & HTTPS Tenta di aprire una connessione al server e di richiedere l'URL utilizzando HTTP o HTTPS, a seconda di quale sia selezionato. Se viene restituito un codice di risposta come 200, è OK. Altrimenti, si considera un fallimento.

SMTP Apre una connessione alla porta definita e invia la stringa EHLO nosuchhost. Se il server risponde con qualsiasi messaggio che inizia con 250 -, è considerato OK. Altre risposte sono considerate un fallimento.

Creazione di monitoraggi personalizzati

I monitoraggi inclusi non sono sufficienti per le esigenze di un sito, o hanno bisogno di un aggiustamento, quindi i monitoraggi personalizzati possono essere creati. La maggior parte dei tipi di monitoraggio ha le proprie impostazioni specifiche che possono essere personalizzate secondo necessità.

Per creare un nuovo monitoraggio: • Passare a **Servizi>Bilanciamento del carico** • Fare clic sulla scheda **Monitoraggio** • Fare clic su  **Aggiungere** per aggiungere un nuovo Monitoraggio • Configurare le opzioni del Monitoraggio come spiegato di seguito:

Nome Nome del monitoraggio. Serve da riferimento, ma deve anche rispettare gli stessi limiti di un alias o nome dell'interfaccia. Solo lettere e numeri, l'unico separatore consentito è un trattino basso. Non ci sono spazi o barre.

Descrizione Una descrizione più lunga opzionale per il monitoraggio. Questo è solo a scopo di riferimento e non ha limiti di formattazione.

Le opzioni rimanenti variano in base al tipo selezionato.

ICMP e TCP Senza opzioni extra. Qualsiasi monitoraggio personalizzato che utilizza questi tipi si comporterà in maniera identica al monitoraggio predefinito con lo stesso nome.

HTTP e HTTPS Questi si comportano in modo identico l'uno all'altro, l'unica differenza è se la crittografia viene utilizzata o meno per parlare con il server di destinazione. Ognuno di questi ha tre opzioni per controllare il comportamento del monitoraggio:

Percorso Il percorso definisce la sezione del percorso dell'URL inviato al server. Se il sito ha contenuti per lo più dinamici, o l'URL di base fa un reindirizzamento, è meglio impostare questo su un percorso completo con un pezzo statico di contenuto, come un'immagine, che è improbabile che si muova o cambi.

Host Se il server esegue più host virtuali, questo campo definisce quale hostname viene inviato con la richiesta in modo che la risposta prevista possa essere ricevuta.

Codice HTTP Questo definisce la risposta prevista dal server, data la richiesta all'Host/Percorso. Più comunemente questo sarebbe impostato su *200 OK*, ma se il server utilizza un altro codice di ritorno che ci si aspetterebbe come una risposta sana a questa richiesta, sceglierlo qui. Se il codice di ritorno è sconosciuto, ispezionare i registri del server per trovare quali codici vengono restituiti al client per ogni richiesta.

Inviare/Aspettare Questo tipo di monitoraggio apre una connessione alla porta definita e invia una stringa e si aspetta la risposta specificata. L'esempio più comune è il monitoraggio SMTP discusso in precedenza. Le opzioni sono:

Inviare stringa La stringa inviata al server dopo aver effettuato una connessione alla sua porta.

Aspettare stringa Se la risposta dal server non inizia con questa stringa, allora è considerato verso down.

- Fare click su **Salvare**

20.1.4 Impostazioni

Oltre alle opzioni per il pool o per il server, ci sono anche alcune opzioni globali che controllano il comportamento di relayd. Queste impostazioni si trovano in **Servizi>Bilanciamento del carico** nella scheda **Impostazioni**:

Tempo di scadenza (Timeout) Il tempo di scadenza globale in millisecondi per i controlli. Lasciare vuoto per utilizzare il valore predefinito di 1000 ms (1 secondo). Se un pool di server caricato richiede più tempo per rispondere alle richieste, aumentare questo timeout.

Intervallo L'intervallo in secondi in cui verrà controllato il membro di un pool. Lasciare vuoto per utilizzare l'intervallo predefinito di 10 Secondi. Per controllare i server più (o meno) frequentemente, regolare i tempi di conseguenza.

Prima del bivio (Prefork) Numero di processi utilizzati da relayd per la gestione delle connessioni in ingresso ai relay. Questa opzione è attiva solo per i relay che utilizzano la *modalità DNS*. Non ha alcun effetto sulla modalità TCP poiché utilizza un reindirizzamento, non un relay. Lasciare vuoto per utilizzare il valore predefinito di 5 processi. Se il server è occupato, aumentare questa quantità per adattarsi al carico.

20.1.5 Regole del Firewall

L'ultimo passo nella configurazione del bilanciamento del carico è configurare le regole del firewall per consentire il traffico al pool.

Per la modalità *TCP*, le regole del firewall devono consentire il traffico agli indirizzi IP privati interni dei server, lo stesso delle regole NAT, così come la porta su cui sono in ascolto internamente. Creare un alias per i server nel pool per semplificare il processo e creare una singola regola del firewall sull'interfaccia in cui verrà avviato il traffico destinato al pool (di solito *WAN*) consentendo l'origine appropriata (di solito *qualsiasi*) a una destinazione dell'alias creato per il pool.

Un esempio specifico di questo è fornito in Configurazione delle regole del firewall. Per ulteriori informazioni sulle regole del firewall, fare riferimento a *Firewall*.

Per la modalità *DNS*, le regole del firewall devono consentire il traffico direttamente all'indirizzo IP e alla porta del virtual server, non ai server del pool.

Connessioni affini Sticky

È disponibile un'opzione di configurazione aggiuntiva per il bilanciamento del carico del server, in **Sistema>Avanzate**, nella scheda **Varie**. Sotto **bilanciamento del carico**, chiamata **Usare connessioni sticky**. Selezionando questa casella si tenterà di inviare client con una connessione attiva al server pool allo stesso server per eventuali connessioni successive.

Una volta che il client chiude tutte le connessioni attive e lo stato chiuso si interrompe, la connessione sticky viene persa. Questo può essere auspicabile per alcune configurazioni di bilanciamento del carico web in cui le richieste del client devono andare solo a un singolo server, per la sessione o per altri motivi. Questa pratica non è perfetta, perché se il browser web del client chiudesse tutte le connessioni TCP al server dopo aver caricato una pagina e si trovasse lì per 10 minuti o più prima di caricare la pagina successiva, la pagina successiva potrebbe essere servita da un server diverso. Generalmente questo non è un problema in quanto la maggior parte dei browser web non chiuderà immediatamente una connessione e lo stato esisterà abbastanza a lungo da non renderlo un problema, ma se il sito è strettamente dipendente da un client specifico che non riceve mai un server diverso nel pool indipendentemente da quanto tempo il browser si trova lì inattivo, cercherà una soluzione diversa per il bilanciamento del carico. C'è una casella sotto l'opzione per controllare il **Timeout di tracciamento della sorgente** che può consentire alla conoscenza della relazione client/server di persistere più a lungo.

Avvertimento: Sticky è generalmente inaffidabile per questo scopo e può anche avere altri effetti collaterali indesiderati. I pacchetti proxy completi come HAProxy hanno meccanismi e opzioni di gran lunga migliori per mantenere le relazioni client/server.

Vedi anche:

Per ulteriori informazioni, è possibile accedere all'archivio degli Hangouts per visualizzare l'Hangout di gennaio 2015 sul bilanciamento del carico del server e sul Failover, che include informazioni sulla configurazione di HAProxy.

Esistono quattro aree di configurazione per il bilanciamento del carico del server:

1. **Pool definisce le raccolte di server da utilizzare, quale porta** utilizzare e il metodo di monitoraggio.
2. **Server virtuale definisce l'indirizzo IP e la porta per** l'accettazione delle connessioni utente e il pool appropriato per indirizzare il traffico in entrata destinato a tale indirizzo IP e porta.
3. **Monitoraggio viene utilizzato per creare metodi di monitoraggio** personalizzati per determinare se i server del pool funzionano e sono utilizzabili.
4. **La scheda Impostazioni contiene opzioni globali che modificano il** funzionamento del bilanciamento del carico.

In un esempio tipico, esiste un **Server virtuale** per accettare le connessioni utente e contiene diversi server in un **Pool**. Il **Pool** utilizza un **Monitoraggio** per ciascun server per determinare se è in grado di accettare connessioni utente.

Un virtual server può avere un normale pool e un **pool di fall-back** da utilizzare se tutti i membri del normale **Pool di virtual serveri** sono inattivi. Questo può essere sfruttato per presentare una pagina di manutenzione o interruzione, ad esempio.

20.2 Esempio di configurazione in bilanciamento di carico del server Web

Questa sezione mostra come configurare il bilanciamento del carico dall'inizio alla fine per un ambiente con bilanciamento del carico con due server web.

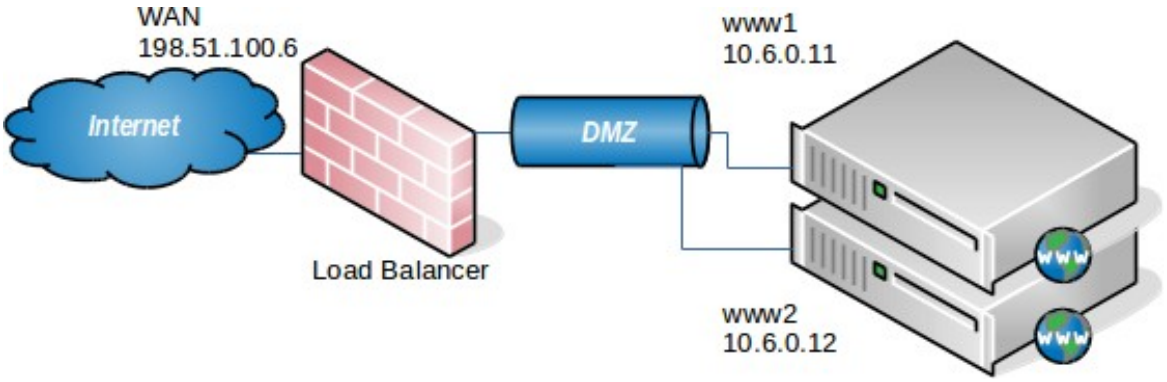


Fig. 1: Esempio di bilanciamento del carico del server della rete

20.2.1 Esempio ambiente di rete

La figura *Esempio di bilanciamento del carico del server della rete* mostra l'esempio di un ambiente configurato in questa sezione. Consiste in un singolo firewall, che utilizza il suo indirizzo IP della WAN per il pool, con due server web su un segmento DMZ.

20.2.2 Configurazione pool

Per configurare il pool:

- Passare a **Servizi>Bilanciamento del carico**
- Fare clic sulla scheda **pool**

- Fare clic su **Aggiungere** per creare un nuovo pool
- Configurare il pool come mostrato nella figura *Configurazione del pool*, che utilizza le seguenti impostazioni:

  Nome WebServers

  Modalità *Bilanciamento del carico*

  Descrizione Web Server Pool

  Porta 80

  Riprovare 5

  Membri del Pool Aggiungere entrambi i server web (10.6.0.11 e 10.6.0.12) utilizzando un **monitoraggio** *HTTP*
- Fare clic su **Salvare**

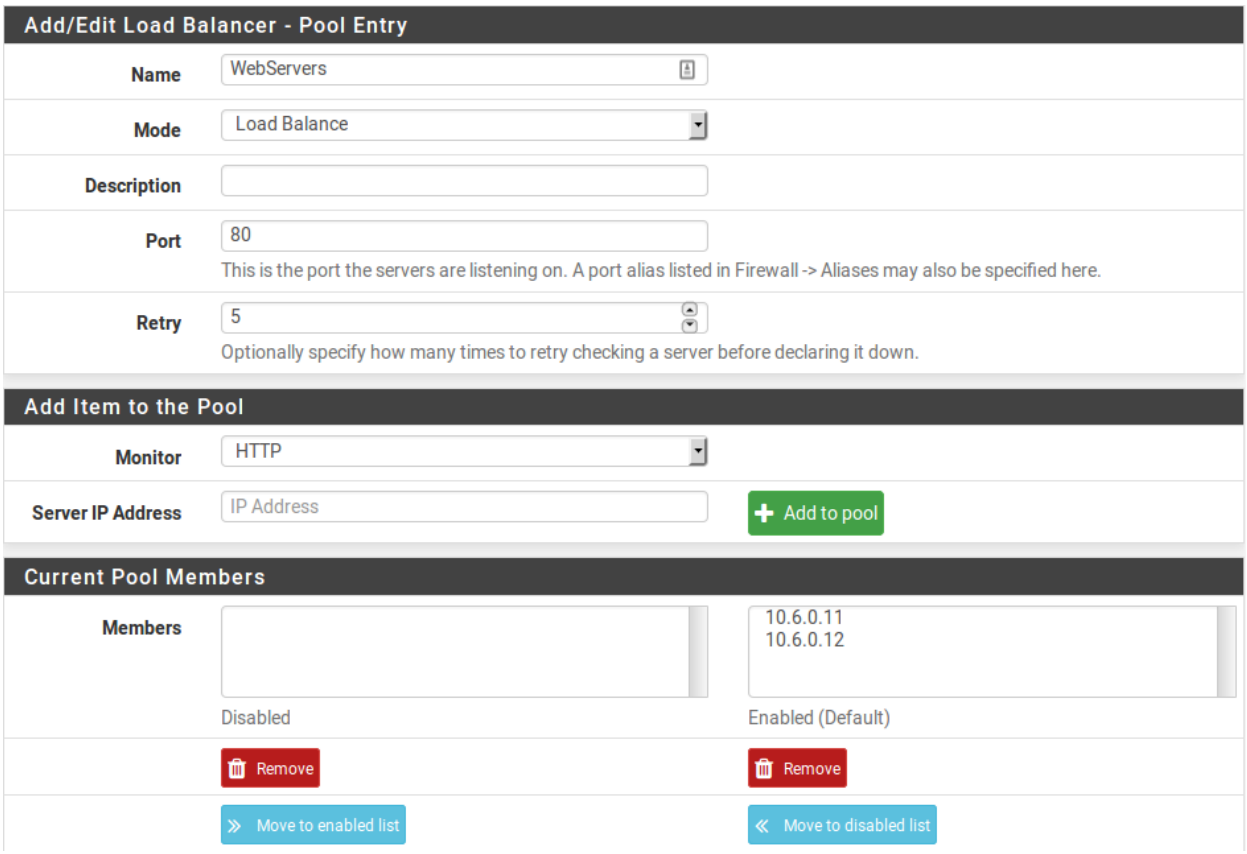


Fig. 2: Configurazione pool

20.2.3 Configurazione virtual server

- Fare clic sulla scheda **Server virtuali**
- Fare clic su **Aggiungere** per aggiungere un nuovo server virtuale
- Configurare il virtual server come mostrato nella figura *Configurazione del virtual server*, che utilizza le seguenti impostazioni:

  Nome WebVirtualServer

Descrizione Web Server

Indirizzo IP L'indirizzo IP della WAN del firewall, 198.51.100.6

Porta 80

Pool dei virtual serveri WebServer

Pool dei fall-back *Nessuno*

- Fare clic su **Presentare**
- Fare clic su **Applicare le modifiche**
-

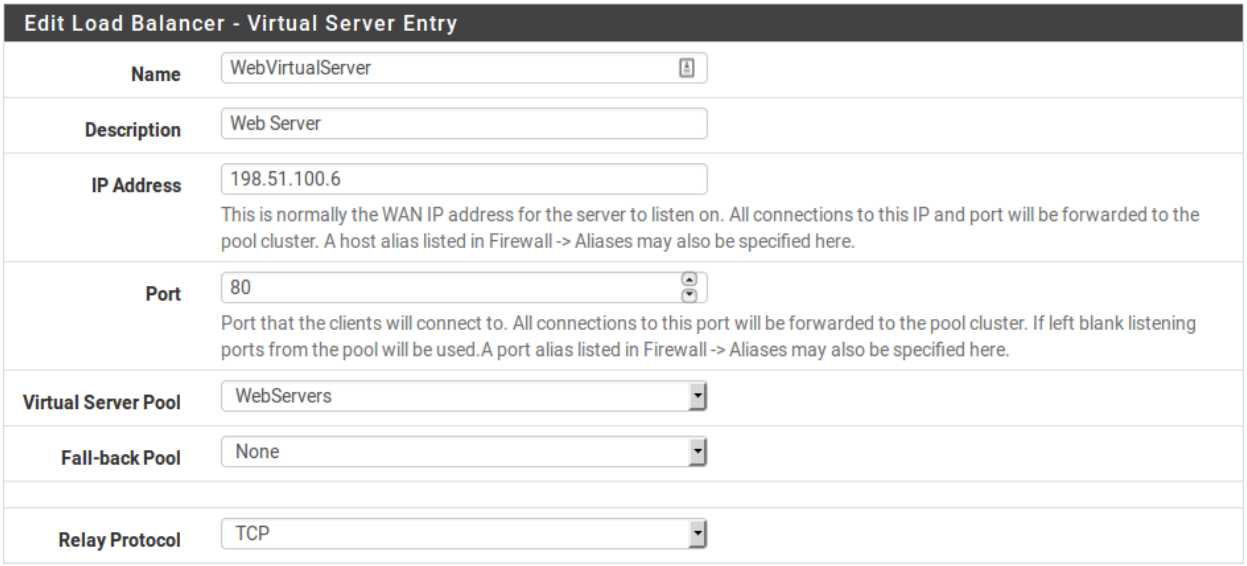


Fig. 3: Configurazione del virtual server

Avvertimento: In questo esempio, se entrambi i server del pool sono inattivi, il server virtuale è inaccessibile. Il firewall agirà come se nessun server virtuale sia configurato. Se qualcosa sul firewall è associato alla porta 80, i client lo raggiungeranno. Ciò include il reindirizzamento della GUI del Web integrato per la porta 80, in modo che debba essere disabilitato in Sistema>Avanzate nella scheda Accesso dell'amministratore.

20.2.4 Configurazione regole del firewall

Le regole del firewall devono essere configurate per consentire l'accesso ai server nel pool. Le regole devono consentire il traffico verso gli indirizzi IP interni e la porta utilizzata e non sono necessarie regole per l'indirizzo IP esterno e la porta utilizzata nella configurazione del virtual server.

Creare un alias contenente tutti i server nel pool, in modo che l'accesso possa essere consentito con una singola regola del firewall.

- Passare a **Firewall>Alias**
- Fare clic su **Aggiungere** per aggiungere un alias.
- Utilizzare le seguenti impostazioni:

  Nome www_servers

Tipo *Host*

Host Gli indirizzi IP di entrambi i server web: 10.6.0.11 e 10.6.0.12

- Fare clic su **Salvare**
- Fare clic su **Applicare le modifiche**

La figura *Alias per i server Web* mostra l'alias utilizzato per questa configurazione di esempio, contenente i due server web. Quindi, creare una regola firewall utilizzando tale alias: • Passare a **Firewall>Regole** • Passare alla scheda per l'interfaccia in cui verranno inserite le connessioni (ad esempio **WAN**) • Fare clic su  **Aggiungere** per avviare una nuova regola nella parte superiore della lista • Utilizzare le seguenti impostazioni:

Interfaccia *WAN*

Protocollo *TCP*

Sorgente *qualsiasi*

Tipo di destinazione *Singolo Host o Alias*

Indirizzo di destinazione www_servers

Intervallo della porta di destinazione *http*

Descrizione Consentire al server Web

- Fare clic su Salvare
- Fare clic su **Applicare le modifiche**

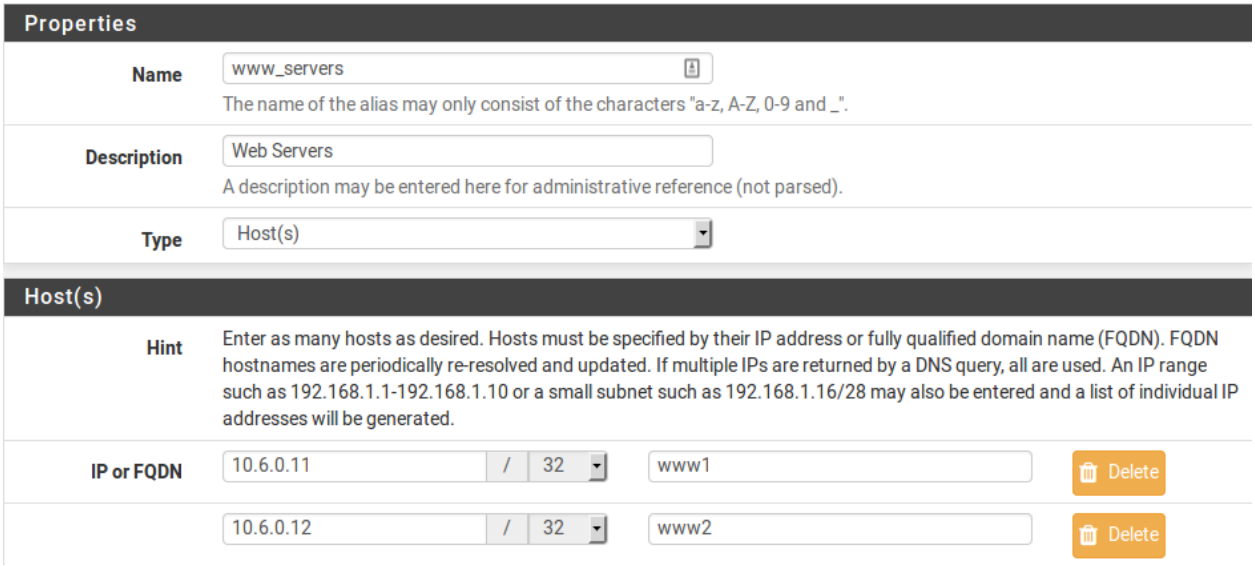


Fig. 4: Alias per i server Web

La figura *Aggiungere regola del firewall per i server Web* mostra un frammento della regola firewall aggiunta per questa configurazione. Le opzioni non mostrate vengono lasciate ai loro valori predefiniti.

La figura *Regola del firewall per i server Web* mostra la regola come appare nella lista.

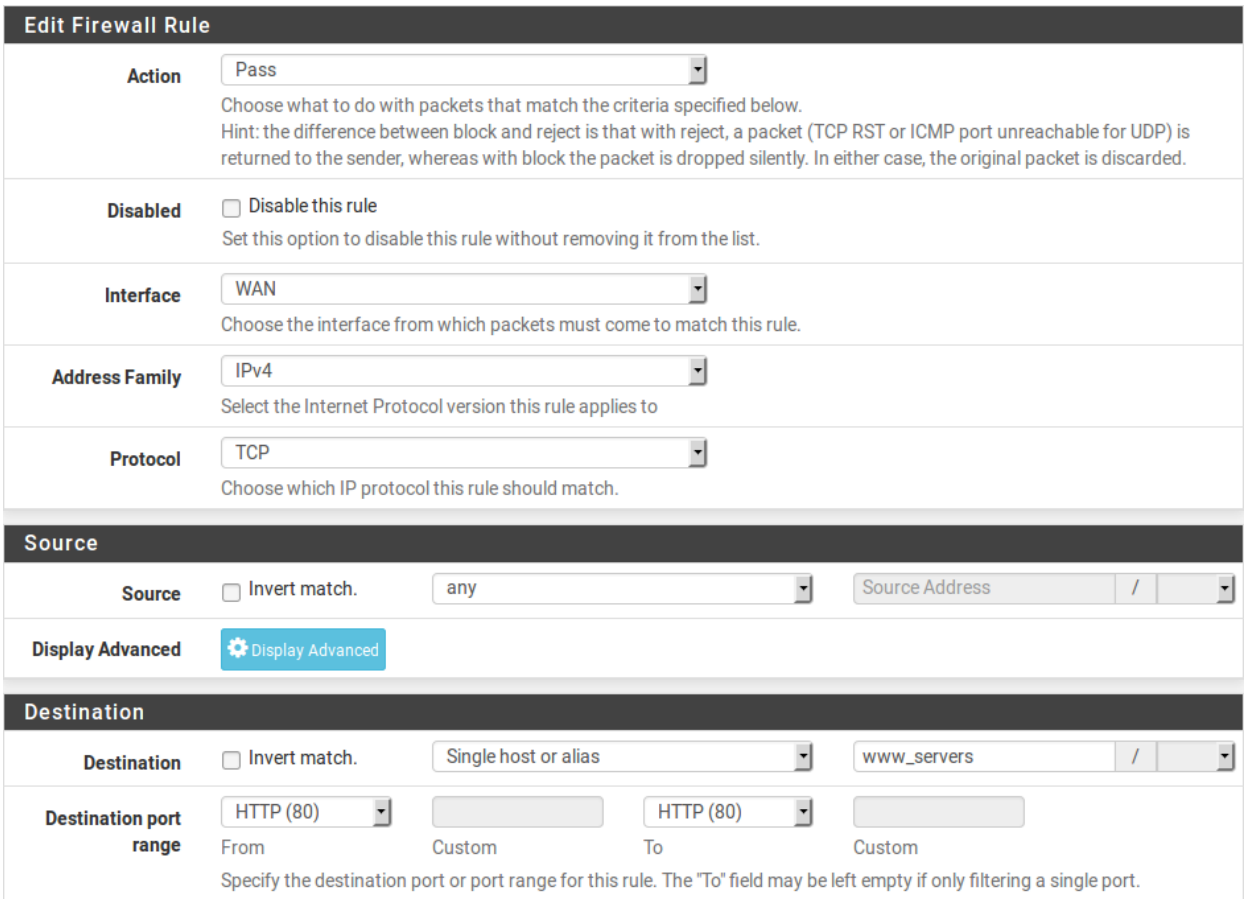


Fig. 5: Aggiungere regola del firewall per i server Web

Fig. 6: Regola del firewall per i server Web

20.2.5 Visualizzare lo stato di bilanciamento del carico

Ora che il bilanciamento del carico è configurato, per visualizzarne lo stato, passare a **Stato>Bilanciamento del carico** e fare clic sulla scheda **Server virtuali**. Questa pagina visualizza lo stato del server nel suo complesso, in genere elencato come **attivo** o in **down**.

La scheda **Pool** mostra lo stato individuale per ogni membro di un pool (come mostrato nella figura *Stato del pool*). La riga per un server è verde se è online e rossa se il server è offline.

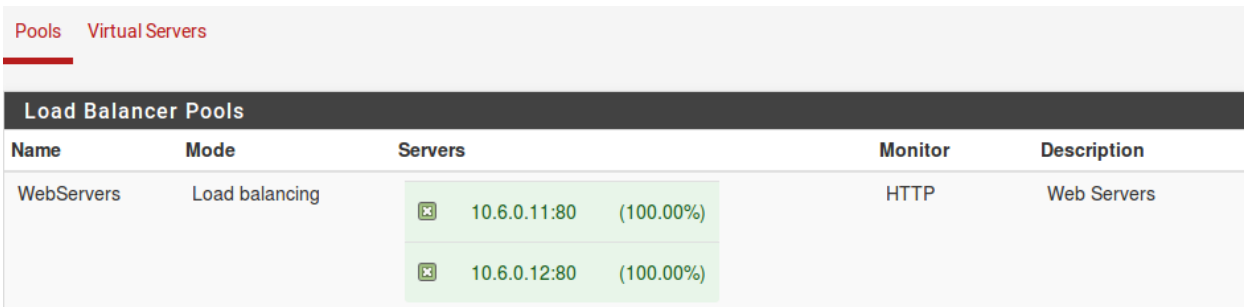


Fig. 7: Stato pool

Inoltre, ogni server nel pool ha una casella di controllo accanto ad esso. I server selezionati sono attivi nel pool e i server non selezioati sono disabilitati nel pool, lo stesso che li sposta tra l'elenco abilitato e disabilitato nella pagina di modifica del pool. Per disabilitare un server: deselezionarlo, quindi fare clic su **Salvare**.

Se il servizio server web viene arrestato su uno dei server o se il server viene rimosso completamente dalla rete se si utilizzano monitoraggi ICMP, lo stato si aggiorna su Offline e il server viene rimosso dal pool.

20.2.6 Verifica del bilanciamento del carico

Per verificare il bilanciamento del carico, curl è l'opzione migliore per garantire che la cache del browser web e le connessioni persistenti non influenzino i risultati dei test. curl è disponibile per ogni sistema operativo immaginabile e può essere scaricato dal sito web di curl. Per usarlo, è sufficiente eseguire:

```
curl http://mysite
```

In tale comando, sostituire 198.51.100.6 con l'indirizzo IP o il nome host del sito. Questo **deve** essere testato dall'esterno della rete (ad esempio da una rete remota o un client sulla WAN). Il seguente esempio illustra un test con curl dal lato WAN:

```
# curl http://198.51.100.6
```

This is server www2 - 10.6.0.12 # curl http://198.51.100.6 This is server www1 - 10.6.0.11

Quando si verifica inizialmente il bilanciamento del carico, configurare ciascun server per restituire una pagina che specifica l'hostname, l'indirizzo IP o entrambi, quindi è reso evidente quale server sta rispondendo alla richiesta. Se le connessioni sticky non sono abilitate, un server diverso risponderà a ciascuna richiesta.

20.3 Risoluzione dei problemi del bilanciamento del carico del server

Questa sezione descrive come identificare e risolvere i problemi più comuni riscontrati dagli utenti con il bilanciamento del carico del server.

20.3.1 Connessioni non vengono bilanciate

Le connessioni non bilanciate sono sempre dovute a un errore della metodologia di test utilizzata e di solito sono specifiche per HTTP. I browser web generalmente mantengono aperte le connessioni a un server web e, premendo refresh, riutilizzano la connessione esistente. Una singola connessione non verrà mai modificata in un altro server bilanciato. Un altro problema comune è la cache del browser web, in cui il browser non richiede mai più la pagina. È preferibile utilizzare uno strumento a riga di comando come curl per test di questa natura, perché assicura che il test non sia influenzato dai problemi inerenti al test con i browser web. curl non ha cache e apre una nuova connessione al server ogni volta che viene eseguita. Ulteriori informazioni su curl possono essere trovate nella *Verifica del bilanciamento del carico*.

Se le connessioni sticky sono abilitate, assicurarsi che il test venga eseguito da più indirizzi IP di origine. I test da un singolo indirizzo IP di origine andranno a un singolo server a meno che non trascorra un lungo periodo di tempo tra i tentativi di connessione.

20.3.2 Il server down non è contrassegnato come offline

Se un server va down ma non è contrassegnato come offline, è perché il monitoraggio eseguito dal demone di bilanciamento del carico ritiene che sia ancora attivo e funzionante. Se si utilizza un monitoraggio TCP, la porta TCP deve comunque accettare le connessioni. Il servizio su quella porta potrebbe essere interrotto in numerosi modi e rispondere

ancora alle connessioni TCP. Per i monitoraggi ICMP, questo problema è esacerbato, poiché i server possono essere appesi o bloccati senza alcun servizio di ascolto e continuare a rispondere ai ping.

20.3.3 Il server attivo non è contrassegnato come online

Se un server è online, ma non contrassegnato come online, è perché non è online dal punto di vista dei monitoraggio del daemon di bilanciamento del carico. Il server deve rispondere sulla porta TCP utilizzata o rispondere ai ping provenienti dall'indirizzo IP dell'interfaccia firewall più vicina al server.

Ad esempio, se il server si trova sulla LAN, il server deve rispondere alle richieste avviate dall'indirizzo IP della LAN del firewall. Per verificarlo con i monitoraggi ICMP, passare a **Diagnostica>Ping** e effettuare un ping per l'indirizzo IP del server utilizzando l'interfaccia in cui si trova il server.

Per i monitoraggi TCP, utilizzare **Diagnostica>Porta di prova** e scegliere l'interfaccia LAN del firewall come sorgente e l'indirizzo IP e la porta del server web come destinazione.

Un altro modo per testare è con un prompt della shell sul firewall, utilizzando l'opzione 8 del menu console o SSH e il comando nc:

```
# nc -vz 10.6.0.12 80
```

nc: connect to 10.6.0.12 port 80 (tcp) failed: Operation timed out

Ed ecco un esempio di una connessione riuscita:

```
# nc -vz 10.6.0.12 80
```

Connection to 10.6.0.12 80 port [tcp/http] succeeded!

Se la connessione non riesce, risolvere ulteriormente il problema sul server web.

20.3.4 Impossibile raggiungere un virtual server da un client nella stessa sottorete del server pool

I sistemi del client nella stessa sottorete dei server del pool non riescono a connettersi correttamente utilizzando questo metodo di bilanciamento del carico. relayd inoltra la connessione al server web con l'indirizzo di sorgente del client intatto. Il server cercherà quindi di rispondere direttamente al client. Se il server ha un percorso diretto verso il client, ad esempio tramite una NIC collegata localmente nella stessa sottorete, non scorrerà correttamente attraverso il firewall e il client riceverà la risposta dall'indirizzo IP locale del server e non dall'indirizzo IP in relayd. Quindi, a causa del fatto che l'indirizzo IP del server non è corretto dal punto di vista del client, la connessione viene interrotta come non valida.

Un modo per aggirare questo problema è utilizzare il NAT in uscita manuale e creare una regola del NAT in uscita manuale in modo che il traffico che lascia l'interfaccia interna (LAN) proveniente dalla sottorete LAN, andando ai server web, venga tradotto all'indirizzo dell'interfaccia di LAN. In questo modo il traffico sembra provenire dal firewall e il server risponderà al firewall, che quindi restituisce il traffico al client utilizzando gli indirizzi previsti. L'indirizzo IP di sorgente del client originale viene perso nel processo, ma l'unica altra soluzione valida è spostare i server in un segmento di rete diverso.

Due tipi di funzionalità di bilanciamento del carico sono disponibili in pfSense: Gateway e server. Il bilanciamento del carico del gateway consente la distribuzione del traffico connesso a Internet su più connessioni WAN. Per ulteriori informazioni su questo tipo di bilanciamento del carico, vedere *Connessioni WAN multiple*. Il bilanciamento del carico del server gestisce il traffico in entrata in modo che utilizzi più server interni per la distribuzione del carico e la ridondanza, ed è oggetto di questo capitolo.

Il bilanciamento del carico del Server consente di distribuire il traffico tra più server interni. È più comunemente usato con il server web e il server SMTP anche se può essere utilizzato per qualsiasi servizio TCP o per il DNS.

Mentre pfSense ha sostituito i bilanciatori di carico commerciali di fascia alta, ad alto costo, tra cui BigIP, Cisco LocalDirector e altri in ambienti di produzione seri, pfSense non è così potente e flessibile come le soluzioni di bilanciamento del carico commerciali di livello aziendale. Non è adatto per installazioni che richiedono configurazioni di monitoraggio e bilanciamento estremamente flessibili. Per le distribuzioni grandi o complesse, viene solitamente richiesta una soluzione più potente. Tuttavia, la funzionalità disponibile in pfSense si adatta a innumerevoli siti molto bene per le esigenze di base.

I pacchetti di bilanciamento del carico completi sono disponibili per pfSense, come **HAProxy** e **Varnish**, ma il bilanciamento del carico integrato basato su relayd di OpenBSD fa un ottimo lavoro per molte distribuzioni. I monitoraggi in relayd possono controllare i codici di risposta HTTP appropriati, controllare gli URL specifici, eseguire un controllo della porta ICMP o TCP, persino inviare una stringa specifica e aspettarsi una risposta specifica.

I servizi TCP nel bilanciamento del carico pfSense vengono gestiti in modalità *reindirizzamento*, il che significa che funzionano come porte forward intelligenti e non come un proxy. L'indirizzo di sorgente del client viene mantenuto quando la connessione viene passata ai server interni e le regole del firewall devono consentire il traffico all'indirizzo interno effettivo dei server del pool. Quando relayd è configurato per gestire il DNS, tuttavia, funziona come un proxy, accettando connessioni e creando nuove connessioni ai server interni.

I server nei pool di bilanciamento del carico vengono sempre utilizzati in modo round-robin. Per tecniche di bilanciamento più avanzate come l'hashing di origine, provare invece un pacchetto proxy inverso come **HAProxy**.

Per ulteriori informazioni, è possibile accedere all'archivio di Hangouts per visualizzare l'Hangout di gennaio 2015 sul bilanciamento del carico del server e sul Failover.

CAPITOLO 21

Wireless

21.1 Dispositivi Wireless Consigliati

Una varietà di schede wireless sono supportate in FreeBSD 11.2-RELEASE-p4, e Firew4LL include il supporto per ogni scheda supportata da FreeBSD. Alcuni hanno un supporto migliore di altri. La maggior parte degli sviluppatori Firew4LL lavora con l'hardware Atheros, quindi tende ad essere l'hardware più consigliato. Molti hanno successo pure con altre schede, e Ralink è un'altra scelta popolare. Altre schede possono essere supportate, ma non supportano tutte le funzionalità disponibili. In particolare, alcune schede Intel possono essere utilizzate in modalità infrastruttura come client ma non possono essere eseguite in modalità access point a causa delle limitazioni dell'hardware stesso.

21.1.1 Schede wireless di grandi poduttori

Linksys, D-Link, Netgear e altri importanti produttori cambiano comunemente il chipset utilizzato nelle loro schede wireless senza modificare il numero di modello. Non c'è modo di garantire che una scheda di uno specifico modello da questi fornitori sarà compatibile perché non esiste un modo affidabile per sapere quale revisione della scheda "minore" e quale chip contiene un pacchetto. Mentre una revisione di un particolare modello può essere compatibile e funzionare bene, un'altra scheda dello stesso modello può essere incompatibile. Per questo motivo, si consiglia di evitare le schede dei principali produttori. Se una scheda è già a portata di mano, vale la pena provare e vedere se è compatibile. Diffidare quando si fa un acquisto perché anche se lo "stesso" modello" ha funzionato per qualcuno, un nuovo acquisto potrebbe comportare un hardware completamente diverso che è incompatibile.

21.1.2 Stato del supporto 802.11n

Firew4LL 01-RELEASE-p3 è basato su FreeBSD 11.2-RELEASE-P4 che ha il supporto per 802.11n su alcuni hardware come quelli basati sui chipset Atheros AR9280 e AR9220. Abbiamo testato le schede usando quei chipset e funzionano bene. Alcune altre schede non Atheros sono documentate da FreeBSD per lavorare su 802.11n, in particolare, mwl (4) e iwn(4). Questi possono funzionare utilizzando lo standard 802.11n, ma le esperienze con la velocità di 802.11n possono variare.

L'articolo wiki di FreeBSD per il supporto 802.11n contiene le informazioni più aggiornate su chipset e driver supportati che funzionano con 802.11n.

21.1.3 Stato supporto 802.11ac

Attualmente, non esiste alcun supporto per 802.11ac in FreeBSD né in Firew4LL.

21.1.4 Frequenze radio e supporto dual band

Alcune schede hanno il supporto per 2.4 GHz e 5 GHz bande, come ad esempio l'Atheros AR9280, ma si può usare solo una banda alla volta. Attualmente non ci sono schede supportate e che lavorano in FreeBSD che opereranno in entrambe le bande contemporaneamente.

L'utilizzo di due schede separate in un'unica unità non è auspicabile in quanto le loro radio potrebbero interferire. Nei casi che richiedono supporto a banda doppia o multipla, si consiglia vivamente un AP esterno.

21.1.5 Driver Wireless inclusi in Firew4LL

Questa sezione elenca i driver wireless inclusi in Firew4LL e i chipset supportati da tali driver. Queste informazioni sono state derivate dalle pagine principali di FreeBSD per i driver in questione. I driver in FreeBSD sono indicati con il loro nome di driver, seguito da (4), come *ath(4).* Il (4) si riferisce alla sezione interfacce del kernel della collezione della pagina principale, in questo caso specificando un driver di rete. I driver sono elencati in ordine di frequenza di utilizzo con Firew4LL, in base ai rapporti degli utenti.

Per informazioni più dettagliate sulle schede supportate e le informazioni più aggiornate, fare riferimento al wiki Firew4LL.

Schede che supportano la modalità con punto di accesso (hostap)

Le schede in questa sezione supportano la funzione del punto di accesso per accettare connessioni da altri client wireless. Questo è indicato come modalità *hostap*.

ath(4)

Il driver *ath(4)* supporta le schede basate sulle API Atheros AR5210, AR5211, AR5212, AR5416 e AR92xx utilizzate da molti altri chip di Atheros con diversi numeri di modello. La maggior parte delle schede Atheros supporta quattro punti di accesso virtuali (VAP) o stazioni o una combinazione per creare un ripetitore wireless.

Sebbene non esplicitamente elencato nella pagina principale, l'articolo wiki di FreeBSD per il supporto 802.11n afferma anche che il driver ha il supporto per ar9130, AR9160, AR9280, AR9285, AR9287 e potenzialmente altri chipset correlati.

ral(4) / ural(4) / rum(4) / run(4)

Ci sono diversi driver di rete wireless 802.11 correlati a Ralink con tecnologia IEEE, ciascuno per un diverso set e tipo di scheda.

- *ral(4)* supporta schede basate sui chipset con tecnologia Ralink RT2500, RT2501 e RT2600, RT2700, RT2900 e RT3090.
- *ural(4)* supporta RT2500USB.
- *run (4)* supporta RT2700U, RT2800U, RT3000U, RT3900E, e simili.
- *rum(4)* supporta RT2501USB e RT2601USB e simili.

Di questi, solo alcuni chip supportati da *run (4)* possono supportare i VAP.

Il chip *ral(4)* RT3090 è l'unico modello elencato come capace di supportare 802.11n su FreeBSD. L'hardware con *ral(4)* RT2700 e RT2800 e *run(4)* RT3900E sono in grado di supportare 802.11n, ma i driver su FreeBSD non supportano attualmente le loro funzionalità 802.11n.

mwl(4)

Il driver di rete wireless della Marvell IEEE 802.11, mwl (4), supporta schede basate sul chipset 88W8363 e supporta completamente 802.11n. Questa scheda supporta più VAP e stazioni, fino a otto di ciascuno.

Schede che supportano solo la modalità client (stazione)

Le schede in questa sezione non sono in grado di fungere da punti di accesso, ma possono essere utilizzate come client in modalità stazione, ad esempio come WAN wireless.

uath(4)

I dispositivi wireless di Atheros USB 2.0 che utilizzano chipset AR5005UG e AR5005UX sono supportati dal driver *uath(4)*.

ipw(4) / iwi(4) / iwn(4) / wpi(4)

I driver di rete wireless Intel coprono vari modelli con driver diversi.

- *ipw (4)* supporta adattatori MiniPCI Intel PRO/Wireless 2100.
- *iwi (4)* supporta adattatori PCI 2225BG e MiniPCI Intel PRO/Wireless 2200BG/2915ABG.
- *iwn (4)* supporta adattatori PCI-Express Intel Wireless WiFi Link serie 4965, 1000, 5000 e 6000.
- *wpi (4)* supporta gli adattatori Intel 3945ABG.

Le schede supportate dal driver *iwn (4)* sono documentate da FreeBSD come in grado di supportare 802.11n in modalità client.

Diversi adattatori Intel hanno una restrizione di licenza con un avviso che appare nel registro di avvio. I driver *ipw(4)*, *iwi(4)* e *wpi(4)* dispongono di file di licenza che devono essere letti e concordati. Queste licenze sono registrate sul firewall in */usr/share/doc/legal /intel_ipw /LICENSE*, */usr/share/doc/legal/intel_iwi/LICENSE*, e

/usr/share/doc/legal/intel_wpi/LICENSE rispettivamente. Per accettare la licenza, modificare */boot/loader.conf.locale* e aggiungere una riga per indicare la conferma della licenza, ad esempio:

```
legal.intel_ipw.license_ack=1
```

Dato l'uso limitato di questi adattatori solo come client, una soluzione basata sulla GUI per riconoscere queste licenze non è stata ancora creata.

bwi(4) / bwn(4)

Il driver wireless Broadcom BCM43xx IEEE 802.11b/g è diviso in due a seconda dei modelli specifici in uso.

- *bwi(4)* supporta BCM4301, BCM4303, BCM4306, BCM4309, BCM4311, BCM4318, BCM4319 utilizzando una versione v3 precedente del firmware Broadom.

- *bwn(4)* supporta BCM4309, BCM4311, BCM4312, BCM4318, BCM4319 utilizzando una versione v4 più recente del firmware Broadcom.

Il supporto offerto dai driver si sovrappone per alcune schede. Il driver *bwn(4)* è preferito per le schede supportate mentre il driver *bwi (4)* deve essere utilizzato sulle schede più vecchie non coperte da *bwn(4)*

malo(4)

Il driver wireless Marvell Libertas IEEE 802.11b/g, malo (4), supporta le schede utilizzando il chipset 88W8335.

upgt(4)

Il driver wireless Conexant/Intersil Prismgt SoftMAC USB IEEE 802.11b/g, *upgt (4)*, supporta le schede utilizzando il chipset GW3887.

urtw(4) / urtwn(4) / rsu(4)

Il trio dei relativi driver wireless Realtek copre diversi modelli:

- *urtw(4)* supporta i modelli RTL8187B/L USB IEEE 802.11b/g con una radio RTL8225
- *urtwn(4)* supporta RTL8188CU/RTL8188EU/RTL8192CU 802.11b/g/n
- *rsu(4)* supporta RTL8188SU/RTL8192SU 802.11b/g/n

Come in altri casi simili, anche se i chip supportati da *urtwn(4)* e *rsu(4)* sono in grado di supportare 802.11n, FreeBSD non supporta le funzionalità di 802.11 n.

zyd(4)

Il driver del dispositivo di rete wireless ZyDAS ZD1211/ZD1211B USB IEEE 802.11b/g, *zyd(4)*, supporta adattatori che utilizzano il chip con USB ZD1211 e ZD1211B.

21.1.6 Specifiche supporto hardware

Abbiamo un foglio di calcolo online con dettagli più completi del supporto hardware, inclusi più chipset e modelli di dispositivi di esempio supportati da determinati driver. Attualmente queste informazioni si trovano su un foglio di calcolo pubblico di Google Docs collegato dall'articolo wiki della documentazione sul supporto wireless. Come notato in precedenza in questo capitolo, spesso i produttori cambieranno i chipset del dispositivo ma non i numeri di modello, quindi è una guida approssimativa nella migliore delle ipotesi, ma può comunque fornire alcune utili indicazioni.

21.2 Lavorare con interfacce wireless con Virtual Access Point

Firew4LL supporta interfacce wireless virtuali che utilizzano Multi-BSS. Questi sono noti come punto di accesso virtuale o interfacce VAP, anche se vengono utilizzati per la modalità client. I VAP consentono di eseguire più access point o client sulla stessa scheda wireless o di utilizzare una combinazione di access point e modalità client. Il caso d'uso più comune è per più punti di accesso con SSID diversi ciascuno con requisiti di sicurezza unici. Ad esempio, uno senza crittografia ma con il captive portal e regole di accesso rigorose e una rete separata con crittografia, autenticazione e regole di accesso meno severe.

Anche se una scheda non supporta più istanze VAP, la prima voce deve essere creata manualmente prima di poter essere assegnata.

Il supporto per i VAP varia a seconda della scheda e del driver, consultare le informazioni sul supporto del driver in *Hardware wireless consigliato* per saperne di più. È probabile, tuttavia, che se una scheda wireless Atheros è in uso, funzionerà. Mentre non esiste un limite teorico al numero di VAP che una scheda può utilizzare, il supporto driver e hardware varia, quindi il limite pratico è quattro VAP su *ath (4)* e otto su *mwl(4)*.

Tutti i VAP su una determinata scheda condividono alcune impostazioni comuni, come il canale, le impostazioni normative, le impostazioni dell'antenna e lo standard wireless. Altre impostazioni come la modalità, SSID, impostazioni di crittografia e così via possono variare tra VAP.

21.2.1 Creazione e gestione di istanze wireless

Per creare una nuova istanza wireless:

- Passare a **Interfacce>(assegnare)** nella scheda **Wireless.**
- Fare clic su **Aggiungere** per creare una nuova voce
- Selezionare l'**Interfaccia primaria**, ad esempio *ath0*
- Scegliere la **Modalità** tra *Punto di accesso*, *Infrastruttura* (BSS, modalità client) o *Ad-hoc* (IBSS)
- Inserire una **Descrizione**
- Fare clic su **Salvare**

Un esempio è mostrato nella figura Aggiungere un'istanza wireless.

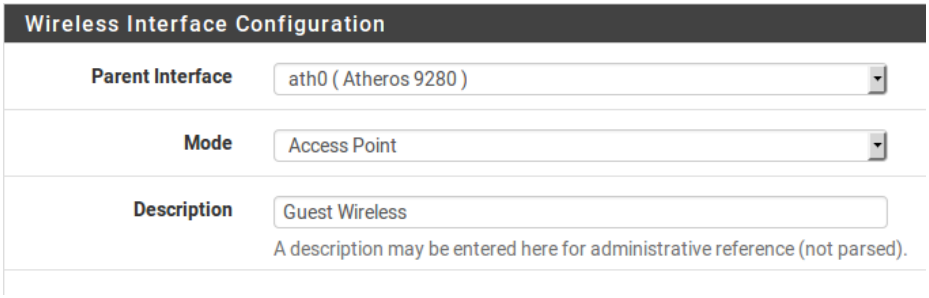


Fig. 1: Aggiungere un'istanza wireless

Una volta che la voce è stata salvata, è disponibile per l'assegnazione sotto **Interfacce>(assegnare)**. Da lì, assegnare e quindi modificare le impostazioni come qualsiasi altra interfaccia wireless.

Nota: L'interfaccia assegnata deve essere configurata per utilizzare la stessa modalità specificata quando è stato creato il VAP.

21.3 Wireless WAN

Una scheda wireless in un firewall che esegue Firew4LL può essere utilizzata come interfaccia WAN primaria o WAN aggiuntiva in una distribuzione Multi-WAN.

21.3.1 Assegnazione dell'interfaccia

Se l'interfaccia wireless non è stata ancora assegnata, ci sono due possibili scelte: aggiungerla come un'interfaccia OPT aggiuntiva o riassegnarla come WAN.

Prima di iniziare, creare l'istanza wireless come descritto in *Creazione e gestione di istanze wireless* se non esiste già. Quando si lavora come le WAN, si deve utilizzare la modalità Infrastruttura (BSS).

Per aggiungere l'interfaccia come nuova interfaccia OPT:

- Passare a **Interfacce>(assegnare)**
- Selezionare l'interfaccia wireless dal menu a discesa **Porte di rete disponibili** sotto le altre interfacce
- Fare clic su **Aggiungere** per aggiungere l'interfaccia come interfaccia OPT

Per riassegnare l'interfaccia wireless come WAN:

- Passare a **Interfacce>(assegnare)**
- Selezionare l'interfaccia wireless come **WAN**
- Fare clic su Salvare

La figura *Assegnazione dell'interfaccia WAN wireless* mostra una scheda Atheros assegnata come WAN.

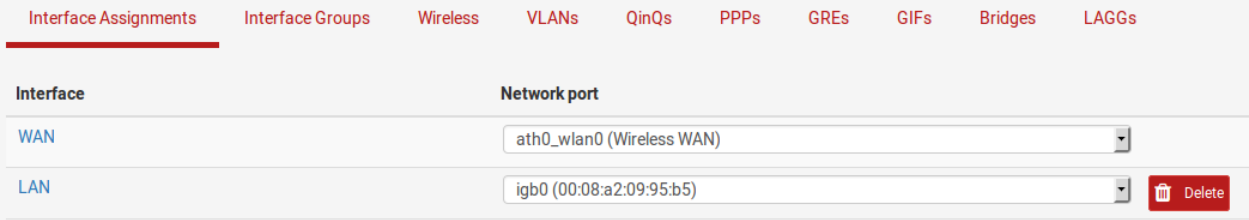


Fig. 2: Assegnazione dell'interfaccia WAN wireless

21.3.2 Configurazione della rete wireless

La maggior parte delle WAN wireless ha bisogno solo di una manciata di opzioni impostate, ma le specifiche variano a seconda del punto di accesso (AP) a cui questa interfaccia client si connetterà.

- Selezionare il menu **Interfacce** per l'interfaccia WAN wireless , ad esempio **Interfacce>WAN**
- Selezionare il tipo di configurazione (*DHCP*, *IP statico*, ecc.)
- Scorrere verso il basso per la **Configurazione wireless comune**
- Impostare lo **Standard** in base ALL'AP, ad esempio *802.11g*
- Selezionare il **Canale** appropriato per abbinare l'AP
- Scorrere verso il basso fino alla **Configurazione wireless specifica della rete**
- Impostare la **Modalità** su *Modalità infrastruttura (BSS)*
- Inserire l'**SSID** per l'AP
- Configurare la crittografia come WPA2 (Accesso protetto al Wi-Fi) se in uso dall'AP
- Rivedere le impostazioni rimanenti, se necessario, e selezionare altre opzioni appropriate per abbinare l'AP
- Fare clic su **Salvare**
- Fare clic su **Applicare le modifiche**

21.3.3 Controllo dello stato del wireless

Passare a **Stato>Interfacce** per visualizzare lo stato dell'interfaccia wireless. Se l'interfaccia è stata associata con successo con l'AP sarà indicato nella pagina di stato. Uno **Stato di associato** indica che l'interfaccia è stata collegata correttamente all'AP, come mostrato nella figura *Interfaccia WAN wireless associata*

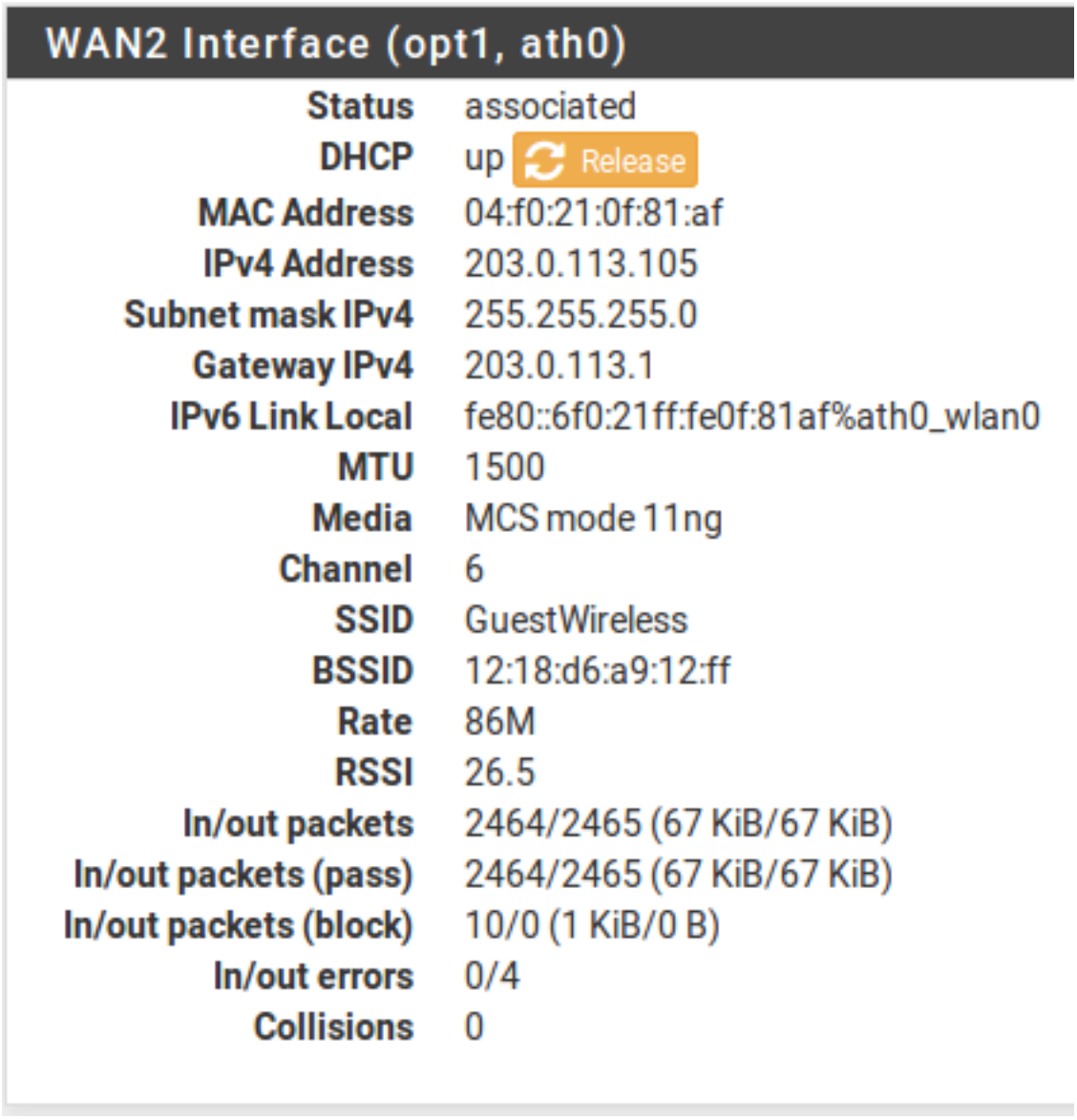


Fig. 3: Interfaccia WAN wireless associata

Se lo **Stato** dell'interfaccia non mostra **Alcun vettore**, non è stato possibile associarlo. La figura *Nessun vettore sulla WAN wireless* mostra un esempio di questo, in cui l'antenna è stata scollegata in modo che non poteva connettersi a una rete wireless che era una certa distanza.

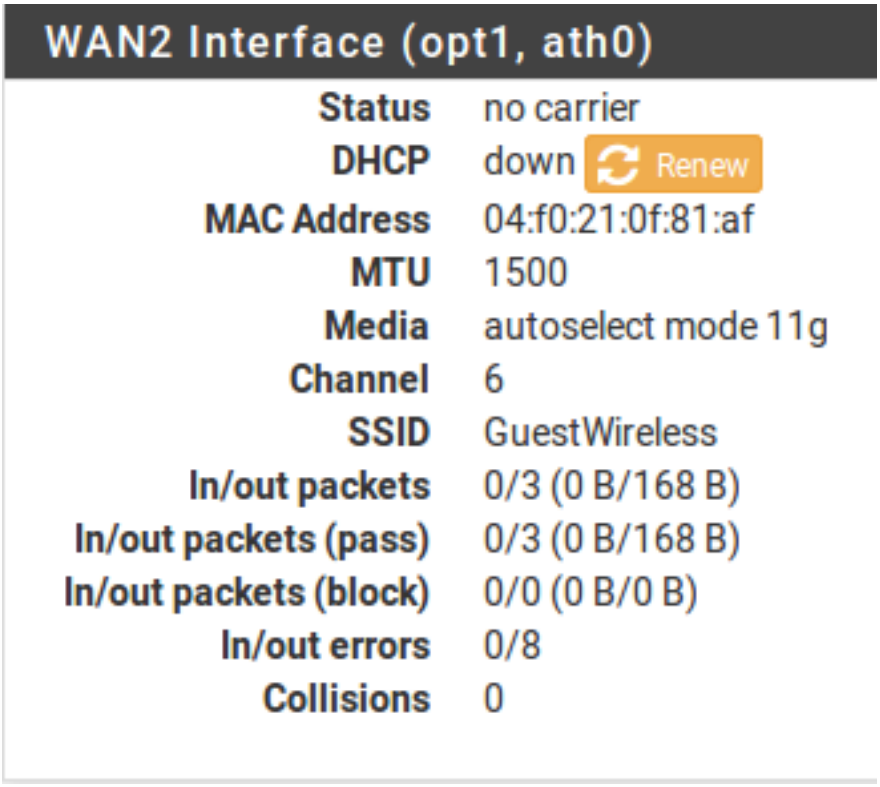


Fig. 4: Nessun vettore sulla WAN wireless

21.3.4 Visualizzazione delle reti wireless disponibili e della potenza del segnale

I punti di accesso wireless visibili dal firewall possono essere visualizzati navigando in **Stato>Wireless** come mostrato nella figura *Stato del wireless*.

Prima di visualizzare questa voce di menu, è necessario configurare un'interfaccia wireless.

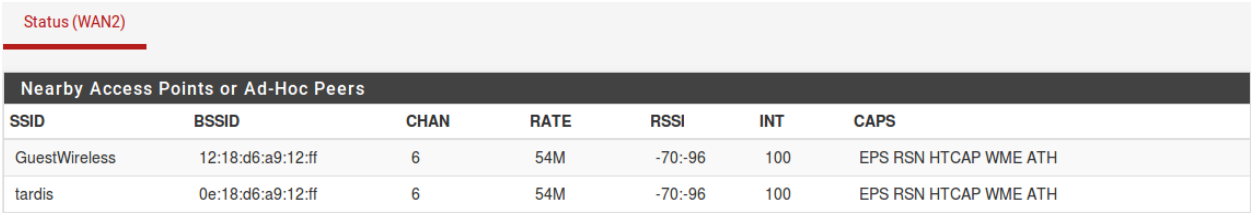


Fig. 5: Stato wireless

21.4 Bridging e wireless

Collegare due interfacce insieme le posiziona sullo stesso dominio di trasmissione come se fossero collegate allo stesso switch. In genere questo viene fatto in modo che due interfacce agiscano come se fossero sulla stessa rete piatta utilizzando la stessa sottorete IP, in questo caso un'interfaccia wireless e un'Interfaccia cablata. Quando due interfacce vengono collegate con un ponte, il traffico broadcast e multicast viene inoltrato a tutti i membri del bridge.

Alcune applicazioni e dispositivi si basano sul traffico broadcast per funzionare. Ad esempio, AirTunes di Apple non funzionerà su due domini broadcast. Quindi, se AirTunes è presente sulla rete wireless e deve essere accessibile da

un sistema sulla rete cablata, le reti cablate e wireless devono essere collegate con un ponte. Altri esempi includono servizi multimediali forniti da dispositivi come Chromecast, TiVo, Xbox 360 e Playstation 3. Questi si basano sul traffico multicast o broadcast che può funzionare solo se le reti cablate e wireless presetano un bridge.

21.4.1 Punti di accesso wireless e bridging

Solo le interfacce wireless in modalità access point (hostap) funzioneranno in una configurazione a ponte. Un'interfaccia wireless configurata per hostap può essere collegata a un'altra interfaccia che li combina sullo stesso dominio broadcast. Ciò può essere auspicabile per alcuni dispositivi o applicazioni che devono risiedere sullo stesso dominio broadcast per funzionare correttamente, come accennato in precedenza.

21.4.2 BSS e IBSS wireless e bridging

A causa del modo in cui il wireless funziona in modalità BSS (Set di servizi di base, modalità client) e IBSS (Set di servizi di base indipendente, modalità Ad-Hoc) e del modo in cui funziona il bridging, un'interfaccia wireless non può essere collegata con un bridge in modalità BSS o IBSS. Ogni dispositivo collegato a una scheda wireless in modalità BSS o IBSS deve presentare lo stesso indirizzo MAC. Con il bridging, l'indirizzo MAC passato è l'attuale MAC del dispositivo collegato. Questo è di solito un aspetto desiderabile del funzionamento del bridging. Con wireless, l'unico modo in cui questo può funzionare è se tutti i dispositivi dietro quella scheda wireless presentino lo stesso indirizzo MAC sulla rete wireless. Questo è spiegato approfonditamente dal noto esperto Wireless Jim Thompson in un post della mailing list.

Ad esempio, quando VMware Player, la Workstation o il server è configurato per collegarsi a un'interfaccia wireless, traduce automaticamente l'indirizzo MAC in quello della scheda wireless. Poiché non c'è modo di tradurre un indirizzo MAC in FreeBSD, e a causa del modo in cui funziona il bridging in FreeBSD, è difficile fornire soluzioni alternative simili a quelle offerte da VMware. Ad un certo punto Firew4LL può sostenere questo, ma non è sul piano di sviluppo pdi 2.x.

21.4.3 Scegliere il routing o il bridging

La scelta tra il bridging (che utilizza la stessa sottorete IP della LAN esistente) o il routing (che utilizza una sottorete IP dedicata per il wireless) per i client wireless dipenderà da quali servizi richiedono i client wireless. In molti ambienti di rete domestica ci sono applicazioni o dispositivi che richiedono reti cablate e wireless da colmare. Nella maggior parte delle reti aziendali, ci sono poche applicazioni che richiedono il bridging. Quale scegliere dipende dai requisiti delle applicazioni di rete in uso, nonché dalle preferenze personali.

Ci sono alcuni compromessi, un esempio è il pacchetto Avahi. Può ascoltare su due diversi domini di trasmissione e scambiare messaggi di rebroadcast da uno all'altro per consentire al DNS multicast di funzionare (anche conosciuto come Rendezvous o Bonjour) per la scoperta e i servizi di rete. Se i servizi richiesti utilizzano tutti i protocolli che possono essere gestiti da Avahi, potrebbe essere possibile utilizzare un metodo instradato.

Per i servizi in esecuzione sul firewall, il bridging può anche essere problematico. Funzionalità come i limitatori, il captive portal e i proxy trasparenti richiedono una configurazione e una gestione speciali per lavorare su reti a ponte. In particolare, il bridge stesso deve essere assegnato e l'unica interfaccia sul ponte con un indirizzo IP deve essere il bridge assegnato. Inoltre, affinché queste funzioni riescano, l'indirizzo IP sul bridge deve essere l'indirizzo utilizzato dai client come gateway.

21.5 Utilizzare un Access Point Esterno

La maggior parte dei router wireless in stile SOHO può essere utilizzata come punto di accesso se non è disponibile un vero punto di accesso (AP). Se Firew4LL ha sostituito un router wireless esistente, potrebbe comunque essere utilizzato

per gestire la parte wireless della rete, se lo si desidera. Questo tipo di distribuzione è popolare per il wireless perché è più facile mantenere il punto di accesso in una posizione con un segnale migliore e sfruttare l'hardware wireless più corrente senza fare affidamento sul supporto del driver in Firew4LL. In questo modo una rete wireless 802.11ac può ancora essere utilizzata e protetta da Firew4LL sul limite, anche se Firew4LL non ha ancora il supporto per le schede 802.11ac.

Questa tecnica è anche comunemente utilizzata con apparecchiature wireless che eseguono *WRT, Tomato o altro firmware personalizzato per l'uso di punti di accesso dedicati piuttosto che router edge.

21.5.1 Trasformare un router wireless in un Access Point

Quando si sostituisce un semplice router wireless come un Linksys, D-Link o altro dispositivo domestico con Firew4LL come firewall perimetrale, la funzionalità wireless può essere mantenuta. Per convertire il router wireless in un punto di accesso wireless, seguire questi passaggi generici per qualsiasi dispositivo. Per trovare le specifiche per un particolare router wireless, fare riferimento alla sua documentazione.

Disabilitare il server DHCP

Disabilitare il server DHCP sul router wireless per evitare un conflitto. Firew4LL gestirà questa funzione per la rete e avere due server DHCP sullo stesso dominio di trasmissione causerà problemi.

Modificare l'indirizzo IP della LAN

Modificare l'indirizzo IP della LAN sul router wireless in un indirizzo IP non utilizzato nella sottorete in cui risiederà (comunemente LAN). Se il firewall con Firew4LL ha sostituito questo router wireless, il router wireless probabilmente utilizzava lo stesso indirizzo IP ora assegnato all'interfaccia LAN di Firew4LL, quindi deve essere modificato. Un indirizzo IP funzionale sul punto di accesso è necessario per scopi di gestione e per evitare conflitti di indirizzi IP.

Collegare l'interfaccia LAN

La maggior parte dei router wireless collega la propria rete wireless alla porta LAN interna o alle porte switch. Ciò significa che il segmento wireless sarà sullo stesso dominio broadcast e sottorete IP delle porte cablate. Per i router con uno switch integrato, una qualsiasi delle porte dello switch LAN in genere funzionerà.

Nota: *Non collegare la porta WAN o Internet sul router wireless!* Questo metterà la rete wireless su un dominio di trasmissione diverso dal resto della rete e il router wireless eseguirà il NAT sul traffico tra il wireless e la LAN. Ciò si traduce anche in doppio NAT di traffico tra la rete wireless e Internet. Questa pratica non è sempre indicata, e porterà a problemi in alcune circostanze, soprattutto se la comunicazione deve avvenire tra i client LAN wireless e cablati.

Decidere dove connettere l'interfaccia LAN dal router wireless dipende dal design di rete scelto. Le sezioni successive coprono le opzioni e le considerazioni per selezionare il miglior stile di distribuzione.

21.5.2 Bridge tra Wireless e LAN

Un mezzo comune di distribuzione wireless è quello di collegare il punto di accesso direttamente allo stesso interruttore degli host LAN, in cui l'AP collega i client wireless alla rete cablata. Questo funzionerà bene, ma offre un controllo limitato sulla capacità dei client wireless di comunicare con i sistemi interni. Vedere Scegliere il routing o il bridging per i dettagli sul bridging in questo ruolo.

21.5.3 Bridge Wireless a interfacca OPT

Per un maggiore controllo sui client wireless, l'aggiunta di un'interfaccia OPT al firewall per il punto di accesso è la soluzione preferita. Per mantenere le reti wireless e cablate sulla stessa sottorete IP e sul dominio broadcast, l'interfaccia OPT può essere collegata all'interfaccia LAN. Questo scenario è funzionalmente equivalente a collegare il punto di accesso direttamente allo switch della LAN, tranne che Firew4LL può filtrare il traffico dalla rete wireless per fornire protezione agli host della LAN e viceversa.

Nota: una configurazione con il bridge assegnato come LAN è ottimale qui, piuttosto che avere solo l'OPT collegato alla LAN cablata esistente.

21.5.4 Segmento instradato su un'interfaccia OPT

La rete wireless può anche essere posizionata su una sottorete IP separata, se lo si desidera. Questo viene fatto senza collegare con un ponte l'interfaccia OPT su Firew4LL, invece assegnandolo con un indirizzo IP in una sottorete separata diversa dalla LAN. Ciò consente il routing tra reti interne e wireless, come consentito dal set di regole firewall. Questo viene comunemente fatto su reti più grandi, dove più punti di accesso sono collegati a uno switch che viene quindi collegato all'interfaccia OPT su Firew4LL. È anche preferibile quando i client wireless saranno costretti a connettersi a una VPN prima di consentire le connessioni alle risorse di rete interne.

21.6 Firew4LL come Access Point

Con una scheda wireless che supporta la modalità hostap (vedere *Schede che supportano la modalità Access Point (hostap)*), Firew4LL può essere configurato come Access Point wireless.

21.6.1 Dovrebbe un AP esterno o Firew4LL essere utilizzato per un punto di accesso?

La funzionalità del punto di accesso in FreeBSD, e quindi Firew4LL, è migliorata notevolmente nel corso degli anni ed è considerata stabile attualmente per la maggior parte degli usi. Detto questo, molti casi d'uso si comportano meglio con un punto di accesso esterno, in particolare implementazioni che hanno requisiti come 802.1ac, funzionamento simultaneo a 2,4 GHz e 5 GHz, reti a maglia wireless o casi rari con client che non si associano a un punto di accesso eseguito utilizzando Firew4LL.

I punti di accesso su Firew4LL sono stati utilizzati con successo in implementazioni di piccole e medie dimensioni, con dispositivi come MacBook Pro, Apple AirTunes, iPod Touch, iPad, telefoni e tablet Android, vari Laptop Windows, Xbox e client FreeBSD e funziona in modo molto affidabile su tutti questi dispositivi. C'è la possibilità di trovare dispositivi incompatibili con qualsiasi punto di accesso, e FreeBSD non fa eccezione.

Il principale fattore decisivo in questi giorni è il supporto 802.11n o 802.11ac; il supporto per l'hardware 802.11n in Firew4LL è in qualche modo limitato e il supporto 802.11ac non esiste. Questo è un fattore determinante per alcuni, e come tale utilizzare un punto di accesso esterno sarebbe meglio per le reti che richiedono 802.11ac e in alcuni casi 802.11n se non è possibile ottenere l'hardware adatto.

Il prossimo fattore più comune è la posizione delle antenne o il punto di accesso wireless in generale. Spesso, il firewall che esegue Firew4LL si trova in un'area dell'edificio che non è ottimale per il wireless, ad esempio una sala server in uno scaffale. Per una copertura ideale, la migliore pratica è individuare l'AP in un'area meno suscettibile alle interferenze wireless e che avrebbe una migliore potenza del segnale nell'area in cui risiedono i client wireless. Se il firewall che esegue Firew4LL si trova da solo su uno scaffale in un'area comune o in un'altra area simile favorevole a un buon segnale wireless, questo potrebbe non essere un problema.

21.6.2 Configurazione di Firew4LL come access point

Il processo di configurazione di Firew4LL per agire come un punto di accesso wireless (AP) è relativamente facile. Molte delle opzioni saranno familiari a chiunque abbia configurato altri router wireless in precedenza e alcune opzioni potrebbero essere nuove a meno che non siano state utilizzate apparecchiature wireless di livello commerciale. Esistono dozzine di modi per configurare i punti di accesso e dipendono tutti dall'ambiente in cui verranno distribuiti. In questo esempio Firew4LL è configurato come AP di base che utilizza la crittografia WPA2 con AES. In questo esempio, EsempioCo ha bisogno di accesso wireless per alcuni laptop nella sala conferenze.

Preparazione dell'interfaccia wireless

Prima di iniziare, assicurarsi che la scheda wireless sia installata nel firewall e che le trecce e le antenne siano saldamente attaccate.

Creare l'istanza wireless come descritto in *Creazione e gestione di istanze wireless* se non esiste già. Quando si lavora come punto di accesso, deve utilizzare la modalità punto di accesso. La scheda wireless deve essere assegnata come interfaccia OPT e abilitata prima che la configurazione rimanente possa essere completata.

Descrizione dell'interfaccia Quando è in uso come punto di accesso, nominare l'interfaccia *WLAN* (LAN Wireless) o *Wireless*, o denominarla dopo l'SSID rende più facile l'identificazione. Se Firew4LL guiderà più punti di accesso, ci dovrebbe essere un modo per distinguerli, come "amministratoreWLAN" e "venditeWLAN". In questo esempio, si chiama SalaConferenze.

Tipo di interfaccia Poiché questo esempio sarà un AP su una sottorete IP dedicata, il tipo di configurazione IPv4 deve essere impostato su *IPv4 statico*

Indirizzo IP Un indirizzo IPv4 e una machera di sottorete devono essere specificati. Questa è una sottorete separata dalle altre interfacce. Per questo esempio può essere 192.168.201.0/24, una sottorete altrimenti inutilizzata nella rete EsempioCo. Usando quella sottorete, l'indirizzo IPv4 per questa interfaccia sarà 192.168. 201.1.

Impostazioni wireless comuni

Queste impostazioni sono condivise per tutti i VAP su una determinata scheda wireless fisica. La modifica di queste impostazioni su un'interfaccia le cambierà su tutte le altre interfacce virtuali utilizzando lo stesso adattatore fisico.

Persistenza delle impostazioni comuni Selezionando **persistenza delle impostazioni comuni**, i valori di configurazione in questa sezione verranno conservati anche se tutte le interfacce e le VAP vengono eliminate o riassegnate, quando altrimenti verrebbero perse.

Wireless standard A seconda del supporto hardware, sono disponibili diverse opzioni per l'impostazione standard wireless, tra cui *802.11b*, *802.11g*, *802.11g turbo*, *802.11a*, *802.11a turbo*, *802.11ng*, *802.11na*, e possibilmente altri. Per questo esempio, sceglieremo *802.11ng* per un punto di accesso 802.11n che opera nella banda 2.4 GHz.

Modalità di protezione OFDM L'impostazione della **Modalità di protezione OFDM** è utile solo in ambienti standard misti in cui 802.11g e 802.11b devono interagire. Il suo uso primario è per evitare collisioni. Data l'età di 802.11b e la scarsità di dispositivi di lavoro che lo utilizzano, è meglio lasciare l'impostazione in *Modalità di protezione off*. C'è una penalità di prestazioni usandolo, dal momento che ha un po" di sovraccarico su ogni frame e richiede anche passaggi aggiuntivi durante la trasmissione di frame.

Selezione del canale Wireless Quando si seleziona un **Canale**, è necessaria la conoscenza dei trasmettitori radio vicini in bande di frequenza simili per evitare interferenze. Oltre ai punti di accesso wireless, ci sono anche telefoni cordless, Bluetooth, monitor per bambini, trasmettitori video, microonde e molti altri dispositivi che utilizzano lo stesso spettro 2.4 GHz che può causare interferenze.

Spesso qualsiasi canale funzionerà finché i client AP si trovano vicino all'antenna. Con 802.11g e precedenti, i canali più sicuri da usare erano *1*, *6* e *11* poiché le loro bande di frequenza non si sovrapponevano l'un l'altro. Questo non è più vero con 802.11n e versioni successive o anche alcune configurazioni 802.11g che utilizzano intervalli di frequenze più ampi per raggiungere velocità più elevate. Per questa rete, dal momento che non ce ne sono altri in giro, il canale *1* è una buona scelta.

Nota: Scegliere sempre un canale specifico. Non selezionare *Automatico* per il canale di un punto di accesso. La convalida dell'input sulle versioni correnti di Firew4LL impedisce che venga selezionata.

Quando si utilizzano altri standard, o si usano wireless in paesi diversi dagli Stati Uniti, ci possono essere molti più canali disponibili di quanto descritto qui. Le schede che supportano 802.11a o 802.11n possono anche supportare canali nello spettro a 5 GHz.

L'elenco completo dei canali supportati dalla scheda è mostrato nel menu a discesa del canale e deve essere d'accordo con lo *Standard* scelto. Ad esempio, non scegliere *802.11ng* per lo **Standard** e quindi scegliere un **canale** utilizzato solo per *802.11na*. L'elenco dei canali include anche alcune informazioni sullo standard, la frequenza del canale e la potenza di trasmissione massima sia della scheda che nel dominio normativo per quel particolare canale. Fare attenzione a guardare la potenza quando si seleziona un canale, perché alcuni canali, soprattutto nella banda 5GHz, variano ampiamente nei loro livelli di potenza consentiti.

Vedi anche:

Strumenti di indagine come NetSurveyor, InSSIDer, Wi-Spy, e innumerevoli altre applicazioni per vari sistemi operativi, telefoni, tablet, e così vi possono aiutare a scegliere un canale meno occupato o un'area dello spettro più libera. Il chilometraggio può variare.

Impostazione della distanza Misurata in metri e supportata solo da schede Atheros, il campo di impostazione della distanza sintonizza i timer ACK/CTS per adattarsi alla distanza tra AP e client. Nella maggior parte dei casi non è necessario configurare questo valore, ma può aiutare in alcune configurazioni wireless difficili come i client a lungo raggio.

Impostazioni normative

La sezione **Impostazioni normative** controlla il modo in cui la scheda è autorizzata a trasmettere legalmente in una regione specificata. Diversi paesi hanno in genere impostazioni normative diverse e alcuni paesi non ne hanno. In caso di dubbi, verificare con il governo locale per vedere quali leggi si applicano in una determinata area. I valori predefiniti sono generalmente OK, poiché le schede possono essere già impostate su una regione specifica. In alcuni casi le impostazioni normative devono essere impostate manualmente se la scheda ha un valore predefinito non compreso nel driver. Simili alla sezione precedente, questi valori vengono applicati alla scheda stessa e non possono variare tra i VAP sulla scheda.

Mentre si può essere tentati di impostare la scheda su *Debug*, al fine di utilizzare le impostazioni non altrimenti consentite, questa azione che potrebbe causare problemi legali dovrebbe essere considerata. La probabilità che ciò accada varia notevolmente in base al paese/area, quindi usarla con cautela.

Dominio normativo Il **Dominio normativo** è l'organismo governativo che controlla le comunicazioni wireless in una regione. Ad esempio, gli Stati Uniti e il Canada seguono i regolamenti FCC mentre nel Regno Unito è ETSI. Se non si è sicuri del dominio normativo in una regione, vedere l'impostazione **Paese**.

Paese A volte i paesi specifici all'interno di un dominio normativo hanno restrizioni diverse. L'opzione **Paese** contiene un elenco a discesa di molti paesi in tutto il mondo e dei relativi codici del paese associati e i domini normativi.

Posizione Esistono alcune restrizioni per le trasmissioni Indoor e Outdoor. L'impostazione della **Posizione** del trasmettitore regolerà ulteriormente la potenza di trasmissione consentita e/o canali.

Configurazione wireless specifica della rete

Queste impostazioni sono uniche per interfaccia, anche su interfacce wireless virtuali. La modifica di queste impostazioni non influisce su altre interfacce.

Modalità wireless Impostare il campo **Modalità** per il **punto di accesso** e Firew4LL utilizzerà hostapd per fungere da AP.

SSID (Service Set Identifier, SSID) L'**SSID** è il "nome" dell'AP visto dai client. Impostare l'SSID su qualcosa di facilmente identificabile ma unico. In linea con l'esempio, *SalaConferenze* è un buon nome da usare.

Standard wireless minimo Il menu a discesa **Standard wireless minimo** controlla se i client più anziani sono in grado di associarsi a questo punto di accesso. Consentirlo ai client più vecchi potrebbe essere necessario in alcuni ambienti se i dispositivi che sono ancora in giro lo richiedono. Alcuni dispositivi sono compatibili solo con 802.11g e richiedono una rete g/n mista per funzionare. Il rovescio della medaglia è che le velocità più lente possono essere viste come risultato di consentire tali dispositivi sulla rete in quanto il punto di accesso sarà costretto a soddisfare il minimo comune denominatore quando un dispositivo 802.11g sta trasmettendo contemporaneamente a un dispositivo 802.11n. Nella nostra sala conferenze di esempio, gli utenti utilizzeranno solo laptop di proprietà aziendale acquistati di recente che sono tutti in grado di supportare 802.11n, quindi *802.11n* è la scelta migliore.

Intra-BSS Se viene verificata la **Comunicazione tra BSS**, i client wireless saranno in grado di vedersi direttamente. Se i client avranno solo bisogno di accedere a Internet, in genere è più sicuro deselezionare questa opzione. In questo scenario, gli utenti nella sala conferenze potrebbero dover condividere i file avanti e indietro direttamente tra i laptop, quindi questo rimarrà selezionato.

Abilitare WME Le estensioni multimediali wireless (Wireless Multimedia Extensions), o **WME**, sono una parte dello standard wireless che fornisce una certa qualità di servizio al traffico wireless per garantire la corretta consegna dei contenuti multimediali. È necessario che 802.11n funzioni, ma è facoltativo per gli standard precedenti. Questa funzione non è supportata da tutte le schede/driver.

Nascondere SSID Normalmente l'AP trasmetterà il suo SSID in modo che i client possano localizzarlo e associarlo facilmente. Questo è considerato da alcuni un rischio per la sicurezza, annunciando a tutti coloro che stanno ascoltando che una rete wireless è disponibile, ma nella maggior parte dei casi la convenienza supera il (trascurabile) rischio per la sicurezza. I vantaggi di disabilitare la trasmissione SSID sono esagerati da alcuni, in quanto in realtà non nasconde la rete a nessuno in grado di utilizzare molti strumenti di sicurezza wireless liberamente disponibili che trovano facilmente tali reti wireless. Per la nostra sala conferenze AP, lasceremo questo deselezionato per rendere più facile ai partecipanti alla riunione trovare e utilizzare il servizio.

Crittografia wireless (WPA)

Sono supportati due tipi di crittografia per le reti 802.11: WPA e WPA2. WPA2 con AES è il più sicuro. Anche quando non preoccuparsi di crittografare il traffico sull'aria (over-the-air) (che dovrebbe essere fatto), fornisce un ulteriore mezzo di controllo di accesso. Tutte le moderne schede wireless e driver supportano WPA2

Avvertimento: Debolezze della crittografia wireless WEP ha seri problemi di sicurezza noti da anni e il supporto per WEP è stato rimosso da pfSense. È possibile rompere WEP in pochi minuti al massimo, e non dovrebbe mai essere accreditato per la sicurezza. Se è richiesto WEP, deve essere utilizzato un AP esterno. TKIP (Protocollo di integrità con chiave temporanea, Temporal Key Integrity Protocol), parte di AES, è diventato un sostituto per WEP

dopo che è stato rotto. Esso utilizza lo stesso meccanismo sottostante come WEP, e quindi è vulnerabile ad alcuni attacchi simili. Questi attacchi sono diventati più pratici e TKIP non è più considerato sicuro. TKIP non deve mai essere utilizzato a meno che non siano presenti dispositivi incompatibili con WPA o WPA2 utilizzando AES. WPA e WPA2 in combinazione con AES non sono soggetti a questi difetti in TKIP.

In questo esempio, il wireless *SalaConferenze* deve essere protetto con WPA2.

Abilitare Questa casella abilita la crittografia *WPA* o WPA2, quindi dovrebbe essere **selezionata**

WPA Pre-Shared Key Immettere la chiave wireless desiderata, in questo esempio excoconf213.

WPA Mode WPA o WPA2, in questo esempio, *WPA2*

WPA Key Management Mode WPA Può essere *Chiave precondivisa* (PSK) o *Protocollo di autenticazione estensibile* (Extensible Authentication Protocol, PAA). In questo esempio, PSK è sufficiente.

WPA Pairwise Questo dovrebbe quasi sempre essere impostato su A*ES*, a causa delle debolezze in TKIP menzionate in precedenza.

Group Key Rotation Questa opzione consente di impostare la frequenza con cui le chiavi di crittografia broadcast/multicast (chiave transitoria di gruppo, GTK) vengono ruotate, in pochi secondi. Può essere qualsiasi valore da 9999 ma dovrebbe essere più breve del valore di **Rigenerazione della chiave master del gruppo**. Il valore predefinito di 60 secondi (un minuto) è adeguato. I valori più bassi possono essere più sicuri, ma possono oscurare le cose con frequenti rekeying.

Group Master Key Regeneration Questo parametro controlla la frequenza con cui, in pochi secondi, viene rigenerata la chiave master (Chiave master di gruppo, Group Master Key, GMK) utilizzata internamente per generare GTK. Può essere qualsiasi valore da 9999 ma dovrebbe essere più lungo del valore di **Rotazione della chiave di gruppo**. Il valore predefinito di 3600 secondi (un'ora) è adeguato.

Strict Key Regeneration Questa opzione fa sì che il firewall cambi il GTK ogni volta che un client lascia il punto di accesso, proprio come cambiare le password quando un dipendente va via. Ci può essere una leggera penalità di prestazioni nei casi in cui vi è un elevato fatturato di client. Nei casi in cui la sicurezza non è una preoccupazione primaria, questo può essere lasciato disabilitato.

Autenticazione IEEE 802.1X (WPA Enterprise)

Un altro tipo di sicurezza wireless supportata è noto come autenticazione IEEE 802.1X o più comunemente indicato come WPA Enterprise o WPA2 Enterprise. Questa modalità consente di utilizzare un nome utente e una password più tradizionali per accedere alla rete wireless. Lo svantaggio è che questa autenticazione deve essere eseguita tramite server RADIUS. Se un server RADIUS esistente è già presente o facilmente implementato, potrebbe essere una valida fonte di controllo di accesso wireless. In questo esempio, 802.1X non viene utilizzato, ma le opzioni sono spiegate.

Vedi anche:

Il pacchetto freerADIUS di Firew4LL può essere utilizzato per questo scopo.

Nota: alcuni vecchi sistemi operativi potrebbero non gestire correttamente 802.1X o potrebbero avere lunghi ritardi dopo tentativi di autenticazione non riusciti, ma in genere esistono soluzioni alternative per tali problemi tramite aggiornamenti o patch del sistema operativo.

I client devono anche essere configurati per accedere correttamente al servizio. Alcuni possono prendere automaticamente le impostazioni corrette, altri potrebbero aver bisogno di impostare una modalità specifica (ad esempio *PEAP*) o potrebbero aver bisogno di certificati caricati. I valori specifici dipendono dalle impostazioni del server RADIUS.

Per iniziare con l'autenticazione 802.1X, impostare prima la **Gestione della chiave WPA** su *Protocollo di autenticazione estensibile*.

Abilitare l'autenticazione 802.1X Quando selezionata, il supporto per l'autenticazione 802.1X è abilitato e richiesto ai client.

Server 802.1x primario Il server preferito per l'autenticazione 802.1X.

Indirizzo IP L'indirizzo IP del server RADIUS preferito da utilizzare per l'autenticazione dei client di 802.1X

Porta La porta su cui contattare il server RADIUS per le richieste di autenticazione, di solito 1812.

Segreto condiviso La password da utilizzare quando si comunica con il server RADIUS da questo firewall. Questo deve corrispondere al segreto condiviso definito per questo firewall sul server RADIUS.

Server 802.1X secondario Gli stessi parametri di cui sopra, ma per un server RADIUS secondario nel caso in cui il primo sia irraggiungibile.

Preautenticazione del roaming di autenticazione Questa opzione imposta la pre-autenticazione per accelerare il roaming tra i punti di accesso. Ciò eseguirà parte del processo di autenticazione prima che il client si associ completamente per facilitare la transizione.

Terminare le impostazioni AP

Le impostazioni precedenti sono sufficienti per ottenere un punto di accesso wireless in esecuzione con 802.11n con crittografia WPA2 + AES. Al termine delle Impostazioni, fare clic su **Salvare**, quindi **Applicare le modifiche**.

Configurazione di DHCP

Ora che è stata creata una rete completamente separata, DHCP deve essere abilitato per fornire automaticamente ai client wireless associati un indirizzo IP. Passare a **Servizi>Server DHCP**, fare clic sulla scheda per l'interfaccia wireless (SalaConferenze per questo esempio). Selezionare la casella su **Abilitare**, impostare qualsiasi intervallo di dimensioni sia necessario, e tutte le opzioni aggiuntive desiderate, quindi fare clic su **Salvare** e **Applicare le modifiche**. Per ulteriori dettagli sulla configurazione del servizio DHCP, vedere Server DHCP con IPv4.

Aggiungere regole del firewall

Poiché questa interfaccia wireless è un'interfaccia OPT, non avrà regole firewall predefinite. Per lo meno è necessario aggiungere una regola per consentire il traffico da questa sottorete a qualsiasi destinazione. Poiché gli utenti della sala conferenze avranno bisogno di accesso a internet e l'accesso ad altre risorse di rete, una regola di permesso di default andrà bene in questo caso. Per creare la regola:

- Passare a **Firewall>Regole**
- Fare clic sulla scheda per l'interfaccia wireless (**Sala Conferenze** per questo esempio).
- Fare clic su **Aggiungere** e configura una regola come segue:

  Interfaccia *Sala Conferenze*

  Protocollo *Qualsiasi*

  Sorgente *SalaConferenze Net*

  Destinazione *Qualsiasi*
- Fare clic su **Salvare**

- Fare clic su **Applicare le modifiche**

Per ulteriori informazioni sulla creazione di regole firewall, vedere *Firewall*

Associazione dei client

L'AP di Firew4LL appena configurato dovrebbe apparire nell'elenco dei punti di accesso disponibili da un dispositivo wireless, supponendo che la trasmissione dell'SSID non sia stata disabilitata. Un client dovrebbe ora essere in grado di associarlo come farebbe con qualsiasi altro punto di accesso. La procedura esatta varierà tra i sistemi operativi, dispositivi e driver, ma la maggior parte dei produttori ha semplificato il processo per renderlo semplice per tutti.

Visualizzazione dello stato del client wireless

Quando un'interfaccia wireless è configurata per la modalità access point, i client associati verranno elencati in **Stato>Wireless**.

21.7 Protezione aggiuntiva per una rete wireless

Oltre alla crittografia forte da WPA2 con AES, alcuni utenti amano impiegare un ulteriore livello di crittografia e autenticazione prima di consentire l'accesso alle risorse di rete. Le due soluzioni più comunemente distribuite sono il captive portal e le reti private virtuali. Questi metodi possono essere utilizzati se un punto di accesso esterno viene utilizzato su un'interfaccia OPT o una scheda wireless interna come punto di accesso.

Nota: In teoria, il server PPPoE potrebbe anche essere utilizzato in questo ruolo, ma il supporto sarebbe impossibile su alcuni client e non banale sulla maggior parte degli altri, quindi in genere non è un'opzione praticabile se combinato con wireless.

21.7.1 Protezione wireless aggiuntiva con il captive portal

Abilitando il captive portal sull'interfaccia in cui risiede il wireless, è possibile richiedere l'autenticazione prima che gli utenti possano accedere alle risorse di rete oltre il firewall. Nelle reti aziendali, questo viene comunemente distribuito con l'autenticazione RADIUS alla Directory attiva di Microsoft in modo che gli utenti possano utilizzare le proprie credenziali della Directory attiva per autenticarsi mentre si è in rete wireless. La configurazione del portale captive è coperta in *captive portal*.

Nota: se l'unico requisito è l'autenticazione RADIUS per utente, una soluzione migliore per RADIUS è 802.1X anziché utilizzare il captive portal, a meno che non ci siano client presenti che non supportano 802.1X.

Il captive portal è più probabile che venga utilizzato su reti wireless ad accesso aperto o limitato, come quelle in un hotel, un ristorante o un ambiente simile in cui non vi è alcuna crittografia abilitata o una conoscenza comune/chiave condivisa.

21.7.2 Protezione aggiuntiva con VPN

L'aggiunta di un captive portal fornisce un altro livello di autenticazione, ma non offre alcuna protezione aggiuntiva dalle intercettazioni del traffico wireless. Richiedere una connessione VPN prima di consentire l'accesso alla rete interna e Internet aggiunge un altro livello di autenticazione e un ulteriore livello di crittografia per il traffico wireless.

La configurazione per il tipo di VPN scelto non sarà diversa da una configurazione di accesso remoto, ma le regole del firewall devono essere configurate sull'interfaccia Firew4LL per consentire solo il traffico VPN dai client wireless.

Configurazione delle regole del firewall per IPsec

La figura *Regole per consentire solo IPsec da wireless* mostra le regole minime necessarie per consentire solo l'accesso a IPsec sull'indirizzo IP dell'interfaccia WLAN. Anche i ping all'indirizzo IP dell'interfaccia WLAN possono aiutare nella risoluzione dei problemi.

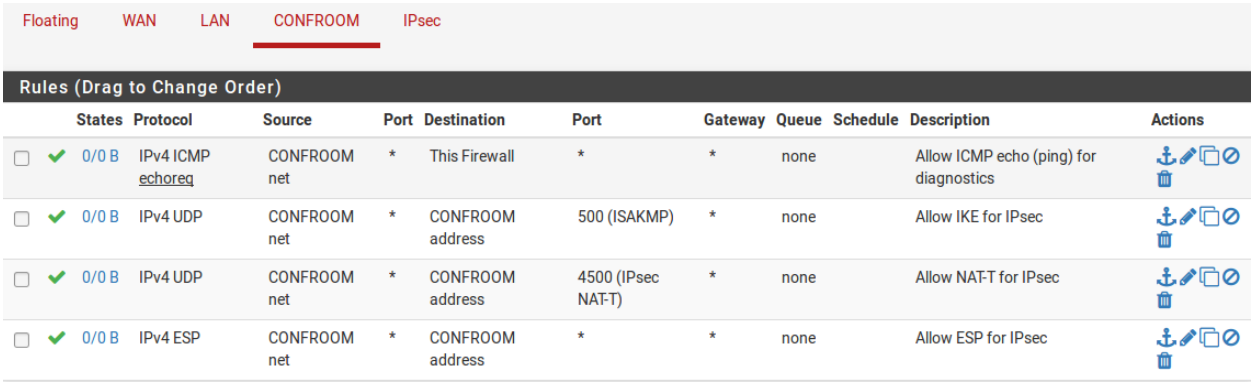


Fig. 6: Regole per consentire solo IPsec da wireless

Configurazione delle regole del firewall per OpenVPN

La figura *Regole per consentire solo OpenVPN da wireless* mostra le regole minime necessarie per consentire l'accesso solo a OpenVPN sull'indirizzo IP dell'interfaccia WLAN. Anche i ping all'indirizzo IP dell'interfaccia WLAN possono aiutare nella risoluzione dei problemi. Ciò presuppone che la porta UDP predefinita 1194 sia in uso. Se è stato scelto un altro protocollo o porta, regolare la regola di conseguenza.

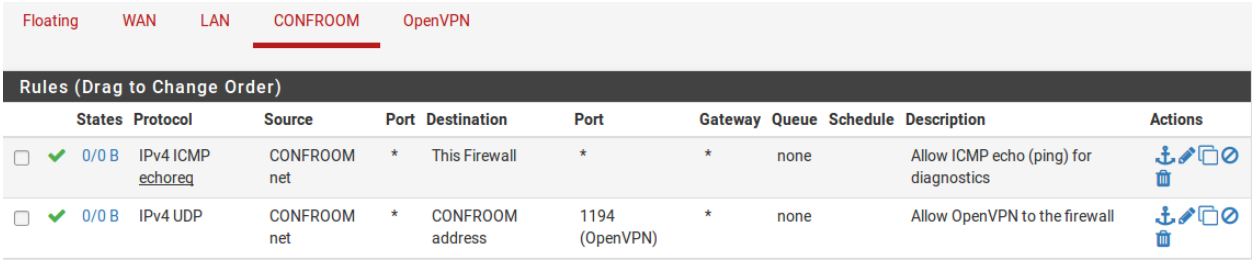


Fig. 7: Regole per consentire solo OpenVPN da wireless

21.8 Configurazione di un HOTSPOT wireless sicuro

Una società o un'organizzazione potrebbe voler fornire l'accesso a Internet per i clienti o gli ospiti utilizzando una connessione Internet esistente. Questo può essere un vantaggio per i clienti e le imprese, ma può anche esporre la rete privata esistente ad attacchi se non è fatto correttamente. Questa sezione copre i mezzi comuni per fornire l'accesso a Internet agli ospiti e ai clienti, proteggendo al contempo la rete interna.

21.8.1 Approccio al firewall multiplo

Per la migliore protezione tra una rete privata e una rete pubblica, ottenere almeno due indirizzi IP pubblici dall'ISP e utilizzare un secondo firewall per la rete pubblica. Per adattarlo, posizionare un interruttore tra la connessione Internet e l'interfaccia WAN di entrambi i firewall.

Questo ha il vantaggio di mettere la rete pubblica su un indirizzo IP pubblico diverso dalla rete privata, quindi se viene ricevuto un rapporto di abuso, è facile determinare la sorgente. Il firewall che protegge la rete privata vedrà la rete pubblica in modo diverso rispetto a qualsiasi host Internet e viceversa.

21.8.2 Approccio al firewall singolo

In ambienti in cui l'approccio firewall multiplo è proibitivo o comunque indesiderabile, la rete interna può ancora essere protetta collegando la rete pubblica a un'interfaccia OPT su un firewall che esegue Firew4LL. Assegnare una sottorete IP privata dedicata a questa interfaccia OPT e configurare le regole del firewall per consentire l'accesso a Internet ma non alla rete interna.

Nelle *Regole per consentire solo l'accesso a Internet da wireless* le regole del firewall consentono ai client di raggiungere il firewall per le richieste DNS e la richiesta echo ICMP (ping), ma impediscono tutto l'accesso ad altre reti private. L'alias RFC1918 a cui si fa riferimento nella figura include l'elenco delle reti private RFC1918, .168.0.0/16, 172.16.0.0/12, e 10.0.0.0/8.

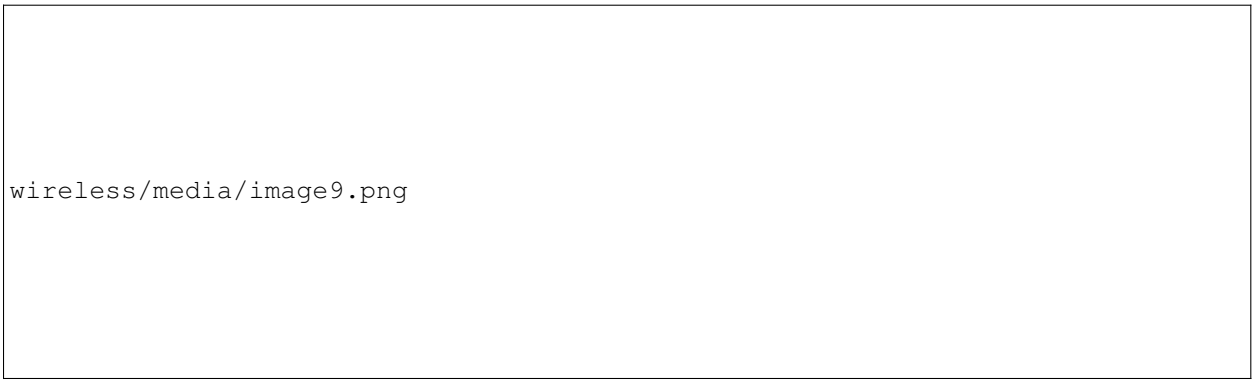


Fig. 8: Regole per consentire solo l'accesso a Internet da wireless

21.8.3 Considerazioni sul controllo degli accessi e sul filtraggio dell'uscita

Oltre a non consentire il traffico dalla rete accessibile al pubblico alla rete privata, ci sono ulteriori cose da considerare nella configurazione di un hotspot.

Limitare l'accesso alla rete

Mentre molti hotspot utilizzano reti wireless aperte senza altra autenticazione, è meglio considerare protezioni aggiuntive per prevenire l'abuso di rete. Su wireless, considerare l'utilizzo di WPA o WPA2 e fornire la passphrase agli ospiti o ai clienti. Alcune aziende che adottano questo approccio visualizzano la passphrase su un cartello nella hall o nell'area di attesa, pubblicato in una camera per gli ospiti o fornito su richiesta. Considerare anche l'implementazione del captive portal su Firew4LL (coperto in *captive portal*). Ciò aiuta a impedire alle persone in altri uffici e all'esterno dell'edificio di utilizzare la rete wireless anche se è ad accesso aperto.

Disabilitare la comunicazione Intra-BSS

Se il punto di accesso lo consente, disabilitare la comunicazione tra BSS. Questa opzione è anche talvolta chiamata «Isolamento dei client AP». Ciò impedisce ai client wireless di comunicare direttamente con altri client wireless, ciò protegge gli utenti da attacchi intenzionali da altri utenti wireless e da quelli non intenzionali come i worm.

La comunicazione tra BSS può essere necessaria per determinate funzioni come stampanti wireless, dispositivi Chromecast o casi simili in cui due dispositivi wireless devono parlare direttamente tra loro, ma questo è raramente se non mai richiesto nel contesto di un hotspot pubblico.

Filtraggio dell'uscita

Considerare che tipo di politica di uscita configurare. Il più semplice, che consente l'accesso a Internet senza consentire l'accesso alla rete privata, è probabilmente il più comunemente distribuito, ma considerare ulteriori restrizioni.

Per evitare di avere l'indirizzo IP pubblico del firewall nella lista nera a causa dei sistemi di visita infetti che agiscono come bot delle spam, considerare il blocco SMTP. Diversi ISP di grandi dimensioni bloccano già SMTP in uscita perché i client si sono spostati sull'utilizzo dell'accesso autenticato sulla porta di invio (587) anziché utilizzare direttamente la porta 25. Un'alternativa che consente ancora alle persone di utilizzare la loro e-mail SMTP ma limita l'effetto dei bot delle spam è creare una regola di permesso per SMTP e specificare le **Voci di stato massime per host** in **Opzioni avanzate** durante la modifica della regola firewall. Assicurarsi che la regola sia al di sopra di qualsiasi altra regola che corrisponda al traffico SMTP e specificare un limite basso. Poiché le connessioni potrebbero non essere sempre correttamente chiuse dal client o dal server di posta, non impostarle troppo in basso per impedire il blocco degli utenti legittimi, ma un limite di cinque connessioni dovrebbe essere ragionevole. Le **Voci di stato massime per host** possono essere impostate su tutte le regole del firewall, ma bisogna tenere presente che alcuni protocolli richiedono dozzine o centinaia di connessioni per funzionare. HTTP e HTTPS possono richiedere numerose connessioni per caricare una singola pagina web a seconda del contenuto della pagina e del comportamento del browser, quindi non impostare i limiti troppo bassi.

Bilanciare i desideri degli utenti contro i rischi inerenti alla fornitura di accesso a Internet per i sistemi incontrollati e definire una politica che si adatti all'ambiente.

21.9 Risoluzione dei problemi delle connessioni wireless

Quando si tratta di wireless, ci sono un sacco di cose che possono andare male. Dalle connessioni hardware difettose alle interferenze radio a software/driver incompatibili o semplici disallineamenti delle impostazioni, tutto è possibile e può essere una sfida per far funzionare tutto al primo tentativo. Questa sezione riguarderà alcuni dei problemi più comuni che sono stati riscontrati dagli utenti e dagli sviluppatori Firew4LL.

21.9.1 Controllare l'antenna

Prima di perdere tempo a diagnosticare un problema, effettuare un doppio e triplo controllo alla connessione dell'antenna. Se si tratta di un tipo a vite, assicurarsi che sia completamente serrato. Per le schede mini-PCI, assicurarsi che i connettori siano correttamente collegati e scattati in posizione. I connettori sulle schede dei mini-PCI sono fragili e facili da rompere. Dopo aver scollegato e ricollegato i connettori alcune volte, potrebbero essere necessario sostituirli.

21.9.2 Controllare lo stato wireless

Lo stato dei client wireless collegati e dei punti di accesso vicini può essere visualizzato navigando in **Stato>Wireless**. Questa opzione di menu viene visualizzata solo quando un'interfaccia wireless è presente e abilitata.

In questa pagina, fare clic su **Nuova scansione** e quindi aggiornare la pagina dopo 10 secondi per vedere altri punti di accesso nelle vicinanze. Se sono sullo stesso o su un canale vicino, potrebbero esserci interferenze.

Nell'elenco dei client associati sono elencati diversi Flag che spiegano le funzionalità del client connesso. Ad esempio, se il client ha un flag "H", questo indica un throughput elevato utilizzato da 802.11n. Se un client è connesso senza tale flag, potrebbe utilizzare uno standard inferiore più vecchio. Un elenco completo dei flag wireless può essere trovato sul wiki, incluse le descrizioni delle funzionalità del punto di accesso.

21.9.3 Provare con più client o schede wireless

Per eliminare una possibile incompatibilità tra le funzioni wireless su Firew4LL e un client wireless, assicurarsi di provarlo prima con più dispositivi o schede. Se lo stesso problema è ripetibile con diverse marche e modelli diversi, è più probabile che sia un problema con la configurazione o l'hardware correlato rispetto al dispositivo client

21.9.4 La potenza del segnale è bassa

Se il segnale è debole anche quando si trova vicino all'antenna del punto di accesso, controllare nuovamente l'antenna. Per le schede di mini-PCI o mini-PCIe, se solo un connettore è in uso e ci sono due connettori interni, provare ad agganciare il connettore fino all'altro connettore interno sulla scheda. Provare anche a cambiare il **canale** o regolare la potenza di trasmissione o le impostazioni dell'antenna sulla configurazione dell'interfaccia wireless. Per le schede mini-PCI E mini-PCIe, verificare la presenza di estremità rotte sui connettori a spirale fragili che si inseriscono nella scheda. Se le impostazioni del **dominio normativo** non sono state configurate, impostarle prima di eseguire nuovamente il test.

21.9.5 Errori segnale bloccato

Se nel sistema o nel registro wireless si trova un errore «Segnale bloccato», di solito è un'indicazione che il canale wireless scelto è troppo rumoroso:

```
kernel: ath0: stuck beacon; resetting (bmiss count 4)
```

La sensibilità di questo comportamento può essere sintonizzata aggiungendo una voce sintonizzabile di sistema per hw.ath.bstuck con un valore di 8 o superiore.

Se gli errori persistono, utilizzare un'app o un programma analisi del WiFi per determinare un canale aperto o meno utilizzato da utilizzare al posto del canale corrente.

21.9.6 Interfaccia non disponibile per l'assegnazione

Se un'interfaccia wireless non viene visualizzata nell'elenco delle interfacce in **Interfacce>(assegnare)** ci sono due problemi possibili:

Se la scheda wireless è supportata, è necessario prima creare un'istanza wireless come descritto in *Creazione e gestione di istanze Wireless*. Una volta creata l'istanza, sarà disponibile per l'assegnazione.

Se la scheda wireless non è supportata, non sarà disponibile per la selezione come interfaccia primaria durante la creazione di un'istanza wireless.

Firew4LL include funzionalità wireless integrate che consentono a un firewall che esegue il software Firew4LL di essere trasformato in un punto di accesso wireless, di utilizzare una connessione 802.11 wireless come connessione WAN o entrambi. Questo capitolo illustra come configurare Firew4LL per questi ruoli, nonché i mezzi suggeriti per accogliere in modo sicuro i punti di accesso wireless esterni e come distribuire in modo sicuro un hotspot wireless. Una copertura approfondita di generale non rientra nell'ambito di questo libro. Per chi cerca tali informazioni, si consiglia il libro Reti Wireless con 802.11: la guida definitiva.

CAPITOLO 22

HA - Alta affidabilità

22.1 Panoramica DI pfsync

pfsync consente la sincronizzazione della tabella dello stato del firewall tra i nodi del cluster. Le modifiche alla tabella disStato sul primario vengono inviate ai firewall secondari tramite l'interfaccia di sincronizzazione e viceversa. Quando pfsync è attivo e configurato correttamente, tutti i nodi avranno conoscenza di ogni connessione che scorre attraverso il cluster. Se il nodo master fallisce, il nodo di backup subentrerà e i client non noteranno la transizione poiché entrambi i nodi conoscevano la connessione in anticipo.

pfsync utilizza multicast per impostazione predefinita, sebbene sia possibile definire un indirizzo IP per forzare gli aggiornamenti unicast per gli ambienti con solo due firewall in cui il traffico multicast non funzionerà correttamente. Qualsiasi interfaccia attiva può essere utilizzata per l'invio di aggiornamenti di pfsync, tuttavia utilizzare un'interfaccia dedicata è meglio per la sicurezza e le prestazioni. pfsync non supporta alcun metodo di autenticazione, quindi se viene utilizzato qualcosa di diverso da un'interfaccia dedicata, è possibile per qualsiasi utente con accesso alla rete locale inserire stati nella tabella di stato. In ambienti a basso throughput che non sono paranoici per la sicurezza, l'uso dell'interfaccia LAN per questo scopo è accettabile. La larghezza di banda richiesta per questa sincronizzazione dello stato varierà in modo significativo da un ambiente all'altro, ma potrebbe raggiungere il 10% del throughput che attraversa il firewall in base al tasso di inserimenti e cancellazioni di stato in una rete.

Il failover può ancora funzionare senza pfsync, ma non sarà senza soluzione di continuità. Senza pfsync se un nodo fallisce e un altro subentra, le connessioni utente verranno eliminate. Gli utenti possono riconnettersi immediatamente attraverso l'altro nodo, ma sarebbero interrotti durante la transizione. A seconda dell'utilizzo in un particolare ambiente, questo può passare inosservato o potrebbe essere un'interruzione significativa, ma breve.

Quando pfsync è in uso, le impostazioni pfsync devono essere abilitate su tutti i nodi partecipanti alla sincronizzazione dello stato, inclusi i nodi secondari, oppure non funzioneranno correttamente.

22.1.1 Regole di pfsync e firewall

Il traffico per pfsync deve essere passato esplicitamente sull'interfaccia di sincronizzazione. La regola deve passare il protocollo pfsync da una fonte della rete di sincronizzazione a qualsiasi destinazione. Una regola che passa tutto il traffico di qualsiasi protocollo consentirebbe anche il traffico richiesto, ma una regola più specifica è più sicura.

22.1.2 pfsync e le interfacce fisiche

Gli stati in Firew4LL sono associati a specifiche interfacce del sistema operativo. Ad esempio, se la WAN è *em0*, allora uno stato sulla WAN sarebbe legato a *em0*. Se i nodi cluster hanno assegnazioni hardware e interfaccia identiche, questo funziona come previsto. Nei casi in cui viene utilizzato un hardware diverso, questo può essere un problema. Se la WAN su un nodo è *em0* ma su un altro nodo è *igb0*, gli stati non corrisponderanno e non saranno trattati allo stesso modo.

È sempre preferibile avere un hardware identico, ma nei casi in cui ciò non sia pratico, esiste una soluzione alternativa: l'aggiunta di interfacce a un LAGG astrae l'interfaccia fisica sottostante effettiva, quindi nell'esempio precedente, la WAN sarebbe *lagg0* su entrambi e gli stati sarebbero associati a *lagg0*, anche se *lagg0* su un nodo contiene *em0* e contiene *igb0* sull'altro nodo.

22.1.3 pfsync e aggiornamenti

Normalmente Firew4LL consentirebbe aggiornamenti del firewall senza alcuna interruzione di rete. Sfortunatamente, questo non è sempre il caso degli aggiornamenti in quanto il protocollo pfsync può cambiare per adattarsi a funzionalità aggiuntive. Controllare sempre la guida all'aggiornamento collegata in tutti gli annunci di rilascio prima di eseguire l'aggiornamento per vedere se ci sono considerazioni speciali per gli utenti CARP.

22.2 Panoramica della sincronizzazione della configurazione con XML-RPC su Firew4LL

Per semplificare il lavoro di mantenimento di nodi firewall praticamente identici, la sincronizzazione della configurazione è possibile utilizzando XML-RPC. Quando la sincronizzazione XML-RPC è abilitata, le impostazioni delle aree supportate vengono copiate nel secondario e attivate dopo ogni modifica di configurazione. La sincronizzazione XMLRPC è facoltativa, ma mantenere un cluster costa molto più lavoro senza di esso.

Alcune aree non possono essere sincronizzate, come la configurazione dell'interfaccia, ma molte altre aree possono: regole del firewall, alias, utenti, certificati, VPN, DHCP, percorsi, gateway e altro ancora. Come regola generale, gli elementi specifici per l'hardware o di una particolare installazione, come interfacce o valori in **Sistema>Generale** o **Sistema>Avanzate** non si sincronizzano. L'elenco delle aree supportate può variare a seconda della versione di Firew4LL in uso. Per un elenco di aree che verranno sincronizzate, vedere gli elementi della casella di selezione su **Sistema>Sincronizzazione di HA** nella sezione XMLRPC. La maggior parte dei pacchetti non si sincronizzerà, ma alcuni contengono le proprie impostazioni di sincronizzazione. Consultare la documentazione del pacchetto per maggiori dettagli.

La sincronizzazione della configurazione dovrebbe utilizzare l'interfaccia di sincronizzazione, o se non esiste un'interfaccia di sincronizzazione dedicata, utilizzare la stessa interfaccia configurata per pfsync.

In un cluster a due nodi le impostazioni XML-RPC devono essere abilitate *solo* sul nodo primario, il nodo secondario deve *disabilitare* queste impostazioni.

Affinché XML-RPC funzioni, entrambi i nodi devono avere la GUI in esecuzione sulla stessa porta e protocollo, ad esempio: HTTPS sulla porta 443, che è l'impostazione predefinita. L'account amministratore non può essere disabilitato ed entrambi i nodi devono avere la stessa password dell'account amministratore.

22.3 Esempio di configurazione ridondante

Questa sezione descrive una semplice configurazione di tre interfacce HA. Le tre interfacce sono LAN, WAN e Sync. Questo è funzionalmente equivalente a una distribuzione LAN e WAN a due interfacce, con l'interfaccia pfsync utilizzata esclusivamente per sincronizzare gli stati di configurazione e firewall tra i firewall primari e secondari.

Nota: Questo esempio copre solo una configurazione IPv4. L'HA è compatibile con IPv6, ma richiede l'indirizzamento statico sulle interfacce del firewall. Quando si prepara a configurare HA, se le assegnazioni IPv6 statiche non sono disponibili, impostare IPv6 su *Nessuno* su tutte le interfacce.

22.3.1 Determinare le assegnazioni degli indirizzi IP

Il primo compito è pianificare le assegnazioni degli indirizzi IP. Una buona strategia è quella di usare l'indirizzo IP utilizzabile più basso nella sottorete come VIP del CARP, il successivo indirizzo IP come indirizzo IP dell'interfaccia firewall principale e l'indirizzo IP susseguente come indirizzo IP dell'interfaccia del firewall secondario. Questo disegno è facoltativo, qualsiasi schema può essere utilizzato, ma consigliamo vivamente uno schema coerente e logico per semplificare la progettazione e l'amministrazione.

Indirizzamento WAN

Gli indirizzi WAN saranno selezionati tra quelli assegnati dall'ISP. Ad esempio, nelle assegnazioni degli indirizzi IP della WAN della tabella, la WAN della coppia HA è 198.51.100.0/24 e gli indirizzi 198.51.100.200 tramite 198.51.100.202 verranno utilizzati come indirizzi IP WAN.

Tabella 1: assegnazioni degli indirizzi IP della WAN

+====================+================================+ | IP Address | Usage | +"“”“”“”“”“”“”“”“”“”“”+"“”“”“”“”“”“”“”“”“”“”“”“”“”“”“”“”"+ | 198.51.100.200/24 | CARP shared IP address | +====================+================================+ | 198.51.100.201/24 | Primary node WAN IP address | +====================+================================+ | 198.51.100.202/24 | Secondary node WAN IP address | +====================+================================+

Indirizzamento LAN

La sottorete LAN è 192.168.1.0/24. Per questo esempio, gli indirizzi IP della LAN verranno assegnati come mostrato nella tabella assegnazioni degli indirizzi IP della LAN.

Tabella 2: assegnazioni degli indirizzi IP della LAN

+=================+================================+ | IP Address | Usage | +"“”“”“”“”“”“”“”“”“"+"“”“”“”“”“”“”“”“”“”“”“”“”“”“”“”“”"+ | 192.168.1.1/24 | CARP shared IP address | +=================+================================+ | 192.168.1.2/24 | Primary node LAN IP address | +=================+================================+ | 192.168.1.3/24 | Secondary node LAN IP address | +=================+================================+

Indirizzamento dell'interfaccia di sincronizzazione

Non c'è un VIP del CARP condiviso su questa interfaccia perché non ce n'è bisogno. Questi indirizzi IP vengono utilizzati solo per la comunicazione tra i firewall. Per questo esempio, 172.16.1.0/24 viene utilizzato come sottorete di Sync. Verranno utilizzati solo due indirizzi IP, ma a /24 viene utilizzato per essere coerente con l'altra interfaccia interna (LAN). Per l'ultimo ottetto degli indirizzi IP, utilizzare lo stesso ultimo ottetto dell'indirizzo IP della LAN di quel firewall per la coerenza.

Tabella 3: sincronizzazione delle assegnazioni degli indirizzi IP

+================+==================================+ | IP Address | Usage | +"“”“”“”“”“”“”“”“”"+"“”“”“”“”“”“”“”“”“”“”“”“”“”“”“”“”“+ | 172.16.1.2/24 | Primary node Sync IP address |

+=================+=================================+ | 172.16.1.3/24 | Secondary node Sync IP address | +=================+=================================+

La figura *Esempio del diagramma di rete HA* mostra il layout di esempio della coppia HA. Il primario e secondario hanno ciascuno connessioni identiche alla WAN e alla LAN, e un cavo di crossover tra di loro per collegare le interfacce di sincronizzazione. In questo esempio di base, lo switch della WAN e lo switch della LAN sono ancora potenziali singoli punti di errore. La ridondanza di commutazione è trattata più avanti in questo capitolo nella *Ridondanza del livello 2*.

22.3.2 Nozioni di base sulla configurazione del cluster

Ogni nodo richiede una configurazione di base al di fuori della configurazione HA effettiva. Non collegare entrambi i nodi nella stessa LAN prima che entrambi i nodi abbiano una configurazione LAN non in conflitto.

Installazione, assegnazione dell'interfaccia e configurazione di base

Installare il sistema operativo sui firewall come al solito e assegnare le interfacce in modo identico su entrambi i nodi. Le interfacce devono essere assegnate nello stesso ordine su tutti i nodi esattamente. Se le interfacce non sono allineate, la sincronizzazione della configurazione e altre attività non si comportano correttamente. Se sono state apportate modifiche alle assegnazioni dell'interfaccia, devono essere replicate in modo identico su entrambi i nodi.

Quindi, connettersi alla GUI e utilizzare la procedura guidata di configurazione per configurare ciascun firewall con un hostname univoco e indirizzi IP statici non conflittuali. Se necessario, fare riferimento alla *procedura guidata di configurazione*.

Ad esempio, un nodo potrebbe essere "firewall-a.example.com «e l'altro «firewall-b.example.com», o una coppia di nomi più personalizzata.

Nota: Evitare di nominare i nodi «master» o «backup» poiché si tratta di Stati e non di ruoli, invece potrebbero essere denominati «primario» e » secondario".

L'indirizzo IP della LAN predefinito è 192.168.1.1. Ogni nodo deve essere spostato al proprio indirizzo, ad esempio 192.168.1.2 per il primario e 192.168.1.3 per il secondario. Questo layout è mostrato nelle assegnazioni degli indirizzi IP della LAN. Una volta che ogni nodo ha un indirizzo IP della LAN univoco, entrambi i nodi possono essere collegati allo stesso switch LAN.

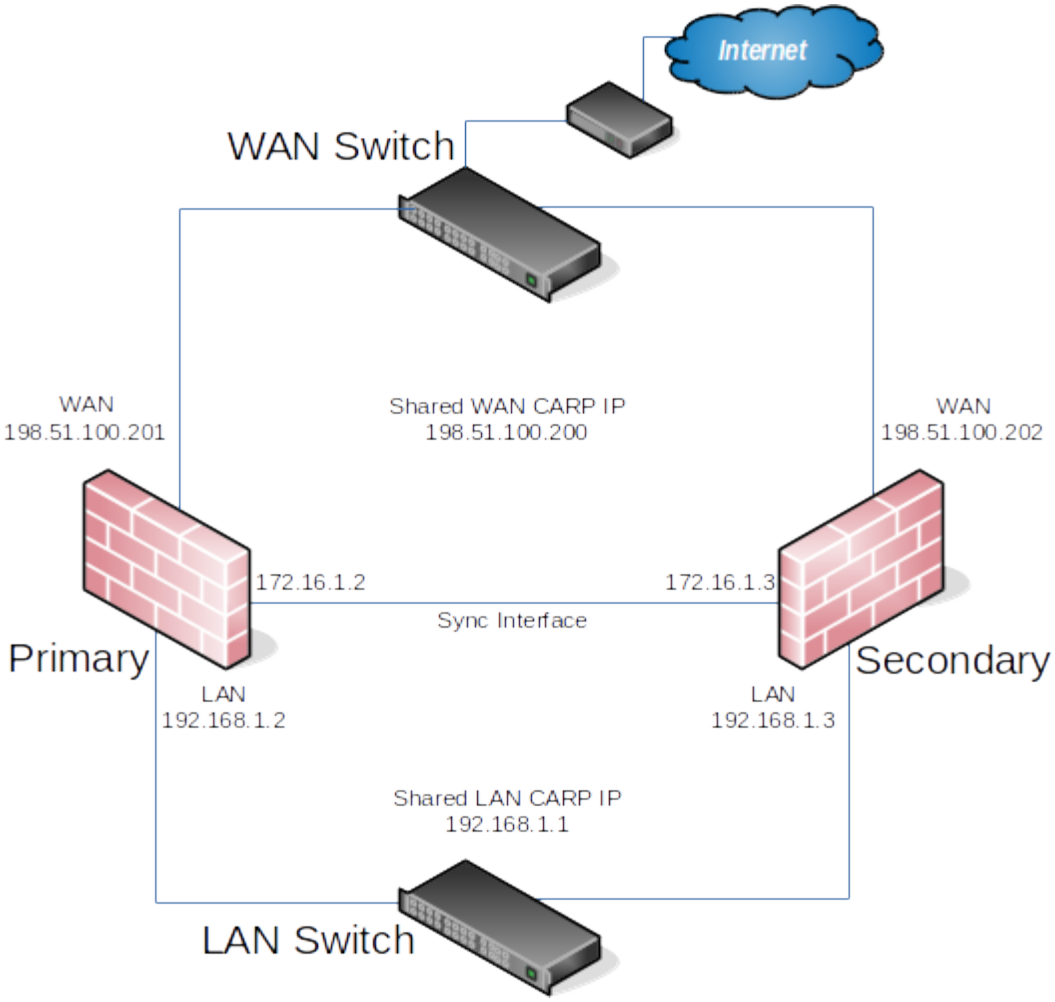


Fig. 1: Esempio del diagramma di rete HA

22.3.3 Configurazione interfaccia di sincronizzazione

Prima di procedere, è necessario configurare le interfacce di sincronizzazione sui nodi del cluster. *Sincronizzare assegnazioni di indirizzi IP* elenca gli indirizzi da utilizzare per le interfacce di sincronizzazione su ciascun nodo. Una volta completato il nodo primario, eseguirlo nuovamente sul nodo secondario con il valore di **indirizzo IPv4** appropriato.

Per completare la configurazione dell'interfaccia di sincronizzazione, le regole del firewall devono essere aggiunte a entrambi i nodi per consentire la sincronizzazione.

Come minimo, le regole del firewall devono passare il traffico di sincronizzazione della configurazione (per impostazione predefinita, HTTPS sulla porta 443) e il traffico pfsync. Nella maggior parte dei casi, viene utilizzata una semplice regola di stile "Permettere tutto".

Al termine, le regole appariranno come in figura *Esempio di sincronizzazione delle regole del firewall dell'interfaccia*, che include anche una regola per consentire echo di ICMP (ping) per scopi diagnostici.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	✔ 0/0 B	IPv4 TCP	SYNC net	*	SYNC address	443 (HTTPS)	*	none		Allow configuration synchronization
☐	✔ 0/11 KiB	IPv4 PFSYNC	SYNC net	*	*	*	*	none		Allow state synchronization
☐	✔ 0/0 B	IPv4 ICMP echoreq	SYNC net	*	SYNC net	*	*	none		Allow ICMP echo (ping) for Diagnostics

Fig. 2: Esempio di sincronizzazione delle regole del firewall dell'interfaccia

Il secondario non ha bisogno di tali regole inizialmente, solo una regola per consentire il traffico alla GUI per il funzionamento di XML-RPC. Il set completo di regole si sincronizzerà una volta che XML-RPC è stato configurato.

22.3.4 Configurare pfsync

La sincronizzazione dello stato tramite pfsync deve essere configurata su entrambi i nodi primari e secondari per funzionare. Prima sul nodo primario e poi sul secondario, eseguire quanto segue:

- Passare al **Sistema>Sincronizzazione con HA**
- Selezionare **Sincronizzare gli stati**
- Impostare Sincronizzare l'interfaccia su *SYNC*
- Impostare **IP del peer per la sincronizzazione con pfsync** per l'altro nodo. Impostarlo su 172.16.1.3 quando si configura il nodo primario o 172.16.1.2 quando si configura il nodo secondario
- Fare clic su **Salvare**

22.3.5 Configurare la sincronizzazione della configurazione (XML-RPC)

Avvertimento: La sincronizzazione della configurazione deve essere configurata solo sul nodo primario. Non attivare mai le opzioni in questa sezione sul nodo secondario di un cluster a due membri.

Solo sul nodo primario, eseguire quanto segue:

- Passare al **Sistema>Sincronizzazione con HA**
- Impostare **Sincronizzare la configurazione per l'IP** su Sincronizzare l'indirizzo IP sul nodo secondario, 172.16.1.3
- Impostare il **Nome utente del sistema remoto** su admin.

  Nota: questo deve essere sempre admin, nessun altro utente funzionerà!

- Impostare **Password del sistema remoto** su password dell'account utente dell'admin e ripetere il valore nella casella di conferma.
- Selezionare le caselle per ogni area da sincronizzare con il nodo secondario. Per questa guida, come per la maggior parte delle configurazioni, tutte le caselle sono selezionate. Il pulsante **Commutare tutto** può essere utilizzato per selezionare tutte le opzioni contemporaneamente, piuttosto che selezionarle singolarmente.
- Fare clic su **Salvare**

Per una rapida conferma che la sincronizzazione ha funzionato, sul nodo secondario passare a **Firewall>Regole** sulla scheda di **sincronizzazione**. Le regole inserite sul primario sono ora lì e la regola temporanea è sparita.

I due nodi sono ora collegati per la sincronizzazione della configurazione! Le modifiche apportate al nodo primario nelle aree supportate verranno sincronizzate con il secondario ogni volta che viene apportata una modifica.

Avvertimento: Non apportare modifiche al secondario nelle aree impostate per essere sincronizzate! Queste modifiche verranno sovrascritte la prossima volta che il nodo primario esegue una sincronizzazione.

Configurazione degli IP virtuali del CARP

Con la sincronizzazione della configurazione in atto, gli indirizzi IP virtuali CARP devono essere aggiunti solo al nodo primario e saranno copiati automaticamente al secondario.

- Passare a **Firewall>IP virtuali** sul nodo primario per gestire i VIP del CARP
- Fare clic su  **Aggiungere** nella parte superiore della lista per creare un nuovo VIP.

Nota: Un VIP deve essere aggiunto per ogni interfaccia che gestisce il traffico utente, in questo caso WAN e LAN.

Tipo Definisce il tipo di VIP, in questo caso *CARP*

Interfaccia Definisce l'interfaccia su cui risiederà il VIP, ad esempio WAN

Indirizzo(i) La casella **Indirizzo** dove vengono inseriti i valori Ddell'indirizzo IP per il VIP. È inoltre necessario selezionare una maschera di sottorete e deve corrispondere alla maschera di sottorete sull'indirizzo IP dell'interfaccia. Per questo esempio, immettere 198.51.100.200 e 24 (vedere *Assegnazioni degli indirizzi IP della WAN*).

Password dell'IP virtuale Imposta la password per il VIP del CARP. Questo deve corrispondere solo tra i due nodi, che saranno gestiti dalla sincronizzazione. La casella password e conferma della password deve essere compilata e deve corrispondere.

Gruppo Vhid Definisce l'ID per il VIP del CARP. Una tattica comune è quella di far corrispondere il vhid all'ultimo ottetto dell'indirizzo IP, quindi in questo caso scegliere 200

Frequenza degli annunci Determina la frequenza con cui vengono inviati i segnali vitali del CARP.

Base Controlla quanti secondi interi passano tra i segnali vitali, in genere *1*. Questo dovrebbe corrispondere tra i nodi del cluster.

Distorto Controlla frazioni di secondo (incrementi 1/256esimo). Un nodo primario è in genere impostato su 0 o 1, i nodi secondari saranno 100 o superiore. Questa regolazione viene gestita automaticamente dalla sincronizzazione XML-RPC.

Descrizione Breve testo per identificare il VIP, come WAN CARP VIP.

Nota: se il CARP sembra essere troppo sensibile alla latenza su una determinata rete, si consiglia di regolare l'opzione **Base** aggiungendo un secondo alla volta fino a raggiungere la stabilità.

La descrizione di sopra ha usato il VIP della WAN come esempio. Il VIP della LAN sarebbe configurato in modo simile, tranne che sarà sull'interfaccia LAN e l'indirizzo sarà 192.168.1.1 (vedere *Assegnazioni degli indirizzi IP della LAN*).

Se ci sono ulteriori indirizzi IP nella sottorete WAN che verranno utilizzati per scopi come NAT 1:1, Porta forward, VPN, ecc., possono essere aggiunti anche ora.

Fare clic su **Applicare le modifiche** dopo aver apportato modifiche ai VIP.

Dopo aver aggiunto VIP, controllare **Firewall>IP virtuali** sul nodo secondario per garantire che i VIP siano sincronizzati come previsto.

Gli indirizzi IP virtuali su entrambi i nodi sembreranno un elenco di indirizzi IP virtuali del CARP se il processo ha avuto successo.

Virtual IP Address

Virtual IP address	Interface	Type	Description
198.51.100.200/24 (vhid: 200)	WAN	CARP	WAN CARP VIP
192.168.1.1/24 (vhid: 1)	LAN	CARP	LAN CARP VIP

Fig. 3: Elenco di indirizzi IP virtuali del CARP

Configurare il NAT in uscita per il CARP

Il prossimo passo sarà configurare il NAT in modo che i client sulla LAN utilizzino l'IP della WAN condiviso come indirizzo.

- Passare a **Firewall>NAT**, scheda **In uscita**
- Fare clic per selezionare *Generazione manuale delle regole NAT in uscita*
- Fare clic su **Salvare**

  Apparirà un insieme di regole che sono le regole equivalenti a quelle in vigore per il NAT automatico in uscita. Regolare invece le regole per le sorgenti della sottorete interne per lavorare con l'indirizzo IP del CARP.

- Fare clic su  a destra della regola per modificare
- Individuare la sezione **traduzione** della pagina
- Selezionare l'indirizzo VIP della WAN del CARP dal menu a discesa di **indirizzo**
- Modificare la descrizione per ricordare che questa regola sarà NAT LAN per l'indirizzo VIP della WAN del CARP

> **Avvertimento:** Se in seguito vengono aggiunte altre interfacce locali, ad esempio una seconda LAN, DMZ, ecc., e tale interfaccia utilizza indirizzi IP privati, è necessario aggiungere ulteriori regole del NAT in uscita manuale in quel momento.

Al termine, le modifiche alle regole appariranno come quelle trovate in *Regole del NAT in uscita per la LAN con il VIP del CARP*

Mappings

		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
☐	✔	WAN	192.168.1.0/24	*	*	500	198.51.100.200	*	✔	Auto created rule for ISAKMP - LAN to WAN
☐	✔	WAN	192.168.1.0/24	*	*	*	198.51.100.200	*	⇄	Auto created rule - LAN to WAN

Fig. 4: Regole del NAT in uscita per la LAN con il VIP del CARP

Modifica del server DHCP

I demoni del server DHCP sui nodi del cluster necessitano di regolazioni in modo che possano lavorare insieme. Le modifiche si sincronizzeranno dal primario al secondario, così come con i VIP e il NAT in uscita, queste modifiche devono essere apportate solo sul nodo primario.

- Passare a **Servizi>Server DHCP**, scheda **LAN *.**
- Impostare il **Server DNS** su VIP del CARP della LAN, qui 192.168.1.1
- Impostare il **Gateway** su VIP del CARP della LAN, qui 192.168.1.1
- Impostare **IP del peer di failover** su indirizzo IP della LAN effettivo del nodo secondario, qui 192.168.1.3
- Fare clic su **Salvare**

L'impostazione del **Server DNS** e del **Gateway** per un VIP del CARP assicura che i client locali stiano parlando con l'indirizzo di failover e non direttamente su entrambi i nodi. In questo modo se il primario fallisce, i client locali continueranno a parlare con il nodo secondario.

L'"**IP del peer di failover** consente al demone di comunicare con il peer direttamente in questa sottorete per scambiare dati come le informazioni di locazione. Quando le impostazioni si sincronizzano con il secondario, questo valore viene regolato automaticamente in modo che i punti secondari ritornino al primario.

22.4 Multi-WAN con HA

HA può anche essere distribuito per la ridondanza del firewall in una configurazione Multi-WAN. Questa sezione descrive in dettaglio la configurazione VIP e NAT necessaria per una doppia distribuzione HA della WAN. Questa sezione copre solo argomenti specifici per HA e multi-WAN.

22.4.1 Determinare le assegnazioni degli indirizzi IP

Per questo esempio, quattro indirizzi IP verranno utilizzati su ogni WAN. Ogni firewall ha bisogno di un indirizzo IP, più un VIP del CARP per il NAT in uscita, più un VIP del CARP aggiuntivo per una voce NAT 1:1 che verrà utilizzata per un server di posta interno nel segmento DMZ.

Indirizzo IP di WAN e WAN2

La tabella *Indirizzamento dell'IP della WAN* mostra l'indirizzamento IP per entrambe le WAN. Nella maggior parte degli ambienti questi saranno indirizzi IP pubblici.

Tabella 4: Indirizzamento dell'IP della WAN

+==================+=====================================+ | IP Address | Usage | +"""""""""""""""""+"""""""""""""""""""""""""""""""""""+ | 198.51.100.200 | Shared CARP VIP for Outbound NAT | +==================+=====================================+ | 198.51.100.201 | Primary firewall WAN | +==================+=====================================+ | 198.51.100.202 | Secondary firewall WAN | +==================+=====================================+ | 198.51.100.203 | Shared CARP VIP for 1:1 NAT | +==================+=====================================+

Tabella 5: Indirizzamento dell'IP della WAN2

+================+=====================================+ | IP Address | Usage | +""""""""""""""""+"""""""""""""""""""""""""""""""""""+ | 203.0.113.10 | Shared CARP VIP for Outbound NAT | +================+=====================================+ | 203.0.113.11 | Primary firewall WAN2 | +================+=====================================+ | 203.0.113.12 | Secondary

firewall WAN2 | +================+====================================+ | 203.0.113.13 | Shared CARP VIP for 1:1 NAT | +================+====================================+

Indirizzamento della LAN

La sottorete LAN è 192.168.1.0/24. Per questo esempio, gli indirizzi IP della LAN verranno assegnati come segue.

Tabella 6: assegnazioni degli indirizzi IP della LAN

IP Address	Usage
192.168.1.1	CARP shared LAN VIP
192.168.1.2	Primary firewall LAN
192.168.1.3	Secondary firewall LAN

Indirizzamento di DMZ

La sottorete DMZ è 192.168.2.0/24. Per questo esempio, gli indirizzi IP di DMZ verranno assegnati come segue nella tabella *assegnazioni degli indirizzi IP di DMZ.*

Tabella 7: assegnazioni degli indirizzi IP di DMZ

IP Address	Usage
192.168.2.1	CARP shared DMZ VIP
192.168.2.2	Primary firewall DMZ
192.168.2.3	Secondary firewall DMZ

Indirizzamento di pfsync

Non ci sarà alcun VIP del CARP condiviso su questa interfaccia perché non ce n'è bisogno. Questi indirizzi IP vengono utilizzati solo per la comunicazione tra i firewall. Per questo esempio, 172.16.1.0/24 verrà utilizzato come sottorete di Sync. Verranno utilizzati solo due indirizzi IP, ma a /24 viene utilizzato per essere coerente con le altre interfacce interne. Per l'ultimo ottetto degli indirizzi IP, viene scelto lo stesso ultimo ottetto dell'IP della LAN di quel firewall per coerenza.

Tabella 8: Sincronizzazione delle assegnazioni degli indirizzi IP

IP Address	Usage
172.16.1.2	Primary firewall Sync
172.16.1.3	Secondary firewall Sync

22.4.2 Configurazione del NAT

La configurazione del NAT quando si utilizza HA con Multi-WAN è la stessa di HA con una singola WAN. Assicurarsi che vengano utilizzati solo i VIP del CARP per il traffico in entrata o il routing. Per ulteriori informazioni sulla configurazione NAT, vedere *Traduzione degli indirizzi di rete*.

22.4.3 Configurazione Del Firewall

Con Multi-WAN una regola firewall deve essere in atto per passare il traffico alle reti locali utilizzando il gateway predefinito. In caso contrario, quando il traffico tenta di raggiungere l'indirizzo del CARP o dalla LAN a DMZ, uscirà invece da una connessione WAN.

Una regola deve essere aggiunta nella parte superiore delle regole del firewall per tutte le interfacce interne che indirizzeranno il traffico per tutte le reti locali al gateway predefinito. La parte importante è che il gateway deve essere predefinito per questa regola e non uno dei gruppi di gateway di failover o di bilanciamento del carico. La destinazione di questa regola sarebbe la rete LAN locale o un alias contenente reti raggiungibili localmente.

22.4.4 Diagramma di HA delle Multi-WAN con DMZ

A causa degli elementi della WAN e di DMZ aggiuntivi, un diagramma di questo layout è molto più complesso come si può vedere nella figura *Diagramma di HA delle Multi-WAN con DMZ.*

22.5 Verifica della funzionalità di failover

Poiché l'utilizzo di HA riguarda l'HA, un test approfondito prima di mettere un cluster in produzione è un must. La parte più importante di quel test è assicurarsi che i peer HA falliscano con grazia durante le interruzioni del sistema.

Se le azioni in questa sezione non funzionano come previsto, vedere *Risoluzione dei problemi della HA*.

22.5.1 Controllare lo stato del CARP

Su entrambi i sistemi, passare a **Stato>CARP (failover)**. Se tutto funziona correttamente, il primario mostrerà 
MASTER per lo stato di tutti i VIP del CARP e il secondario mostrerà  il **BACKUP**.

Se uno mostra invece **DISABILITATO**, fare clic sul pulsante **Abilitare CARP** e quindi aggiornare la pagina.

Se un'interfaccia mostra  **INIZIALIZZAZIONE**, significa che l'interfaccia contenente il VIP del CARP non ha un collegamento. Collegare l'interfaccia a uno switch o almeno all'altro nodo. Se l'interfaccia non verrà utilizzata per qualche tempo, rimuovere il VIP del CARP dall'interfaccia in quanto ciò interferirà con il normale funzionamento del CARP.

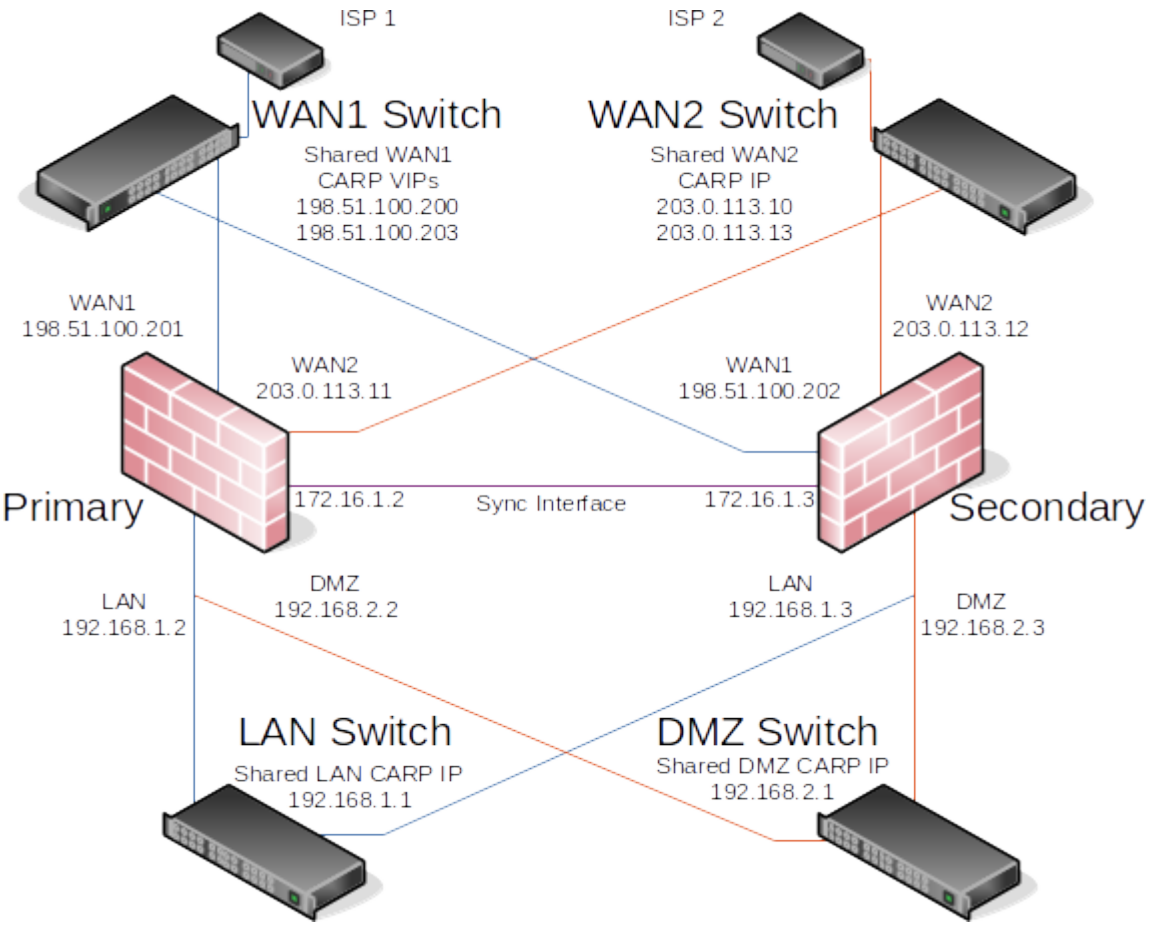


Fig. 5: Diagramma di HA delle Multi-WAN con DMZ

22.5.2 Verifica la replica della configurazione

Passare a posizioni chiave sul nodo secondario, come **Firewall>Regole** e **Firewall>NAT** e assicurarsi che le regole create solo sul nodo primario vengano replicate al nodo secondario.

Se l'esempio precedente in questo capitolo è stato seguito, la regola del firewall «temp» sull'interfaccia pfsync verrà sostituita dalla regola del primario.

22.5.3 Controllare lo stato del failover DHCP

Se il failover DHCP è stato configurato, il suo stato può essere controllato in **Stato>Locazioni di DHCP**. Una nuova sezione apparirà nella parte superiore della pagina contenente lo stato del pool di failover di DHCP, come nella figura *Stato del pool di failover di DHCP*.

Pool Status

Failover Group	My State	Since	Peer State	Since
dhcp_lan (LAN)	normal	2016/03/15 18:52:51	normal	2016/03/15 18:52:51

Fig. 6: Stato del pool di failover di DHCP

22.5.4 Testare il failover del CARP

Ora per il vero test di failover. Prima di iniziare, assicurarsi che un client locale dietro la coppia del CARP sulla LAN possa connettersi a Internet sia con entrambi i firewall di Firew4LL online che in esecuzione. Una volta che è confermato per funzionare, è un ottimo momento per fare un backup.

Per il test effettivo, scollegare il nodo primario dalla rete o spegnerlo temporaneamente. Il client sarà in grado di mantenere il caricamento del contenuto da Internet attraverso il nodo secondario. Selezionare di nuovo **Stato>CARP (failover)** sul backup e ora segnalerà che è **MASTER** per i VIP della LAN e della WAN del CARP. Ora riportare il nodo primario online e riprenderà il suo ruolo di **MASTER**, e il sistema di backup si sposterà nuovamente su **BACKUP**. In qualsiasi momento durante questo processo, la connettività Internet continuerà a funzionare correttamente.

Testare la coppia HA nel maggior numero possibile di scenari di errore. Ulteriori test includono:

- Scollegare il cavo WAN o LAN
- Tirare la spina di alimentazione del primario
- Disabilitare il CARP sul primario utilizzando sia la funzione di disattivazione temporanea sia la modalità di manutenzione
- Testare con ogni sistema singolarmente (spegnere il secondario, quindi riaccendere e spegnere il primario)
- Scaricare un file o provare lo streaming audio/video durante il failover
- Eseguire una richiesta continua di echo di ICMP (ping) su un host Internet durante il failover

22.6 Fornire ridondanza senza il NAT

Come accennato in precedenza, solo i VIP del CARP forniscono ridondanza per gli indirizzi gestiti direttamente dal firewall e possono essere utilizzati solo in combinazione con NAT o servizi sul firewall stesso. La ridondanza può anche essere fornita per sottoreti IP pubbliche instradate con HA. Questa sezione descrive questo tipo di configurazione, che è comune nelle reti di grandi dimensioni, ISP e reti ISP wireless, e ambienti di data center.

22.6.1 Assegnazioni IP pubblici

È necessario almeno un blocco IP pubblico a /29 per il lato WAN di Firew4LL, che fornisce sei indirizzi IP utilizzabili. Solo tre sono necessari per una distribuzione di due firewall, ma questa è la sottorete IP più piccola che ospiterà tre indirizzi IP. Ogni firewall richiede un IP e sul lato WAN è necessario almeno un VIP del CARP.

La seconda sottorete IP pubblica verrà instradata a uno dei VIP del CARP dall'ISP, dal data center o dal router upstream. Poiché questa sottorete viene instradata a un VIP del CARP, il routing non dipenderà da un singolo firewall. Per la configurazione di esempio descritta in questo capitolo, verrà utilizzata una sottorete IP pubblica /24 e verrà suddivisa in due sottoreti /25.

22.6.2 Panoramica della rete

La rete di esempio qui raffigurata è un ambiente di data center composto da due firewall Firew4LL con quattro interfaccie ciascuno: WAN, LAN, DBDMZ e pfsync. Questa rete contiene un certo numero di server web e database. Non è basato su alcuna rete reale, ma ci sono innumerevoli distribuzioni di produzione simili a questa.

Rete WAN

Il lato WAN si connette alla rete upstream, all'ISP, al data center o al router upstream.

Rete WEB

Il segmento WEB in questa rete utilizza l'interfaccia «LAN» ma rinominata. Contiene server web, quindi è stato chiamato WEB ma potrebbe essere chiamato DMZ, SERVER o qualsiasi cosa desiderata.

Rete DBDMZ

Questo segmento è un'interfaccia OPT e contiene i server di database. È comune separare i server web e database in due reti in ambienti con host. I server di database in genere non richiedono l'accesso diretto da Internet, e quindi sono meno soggetti a compromessi rispetto ai server web.

Sincronizzare la rete

La rete di sincronizzazione in questo diagramma viene utilizzata per replicare le modifiche di configurazione di Firew4LL tramite XML-RPC e per pfsync per replicare le modifiche della tabella di stato tra i due firewall. Come descritto in precedenza in questo capitolo, si consiglia un'interfaccia dedicata a questo scopo.

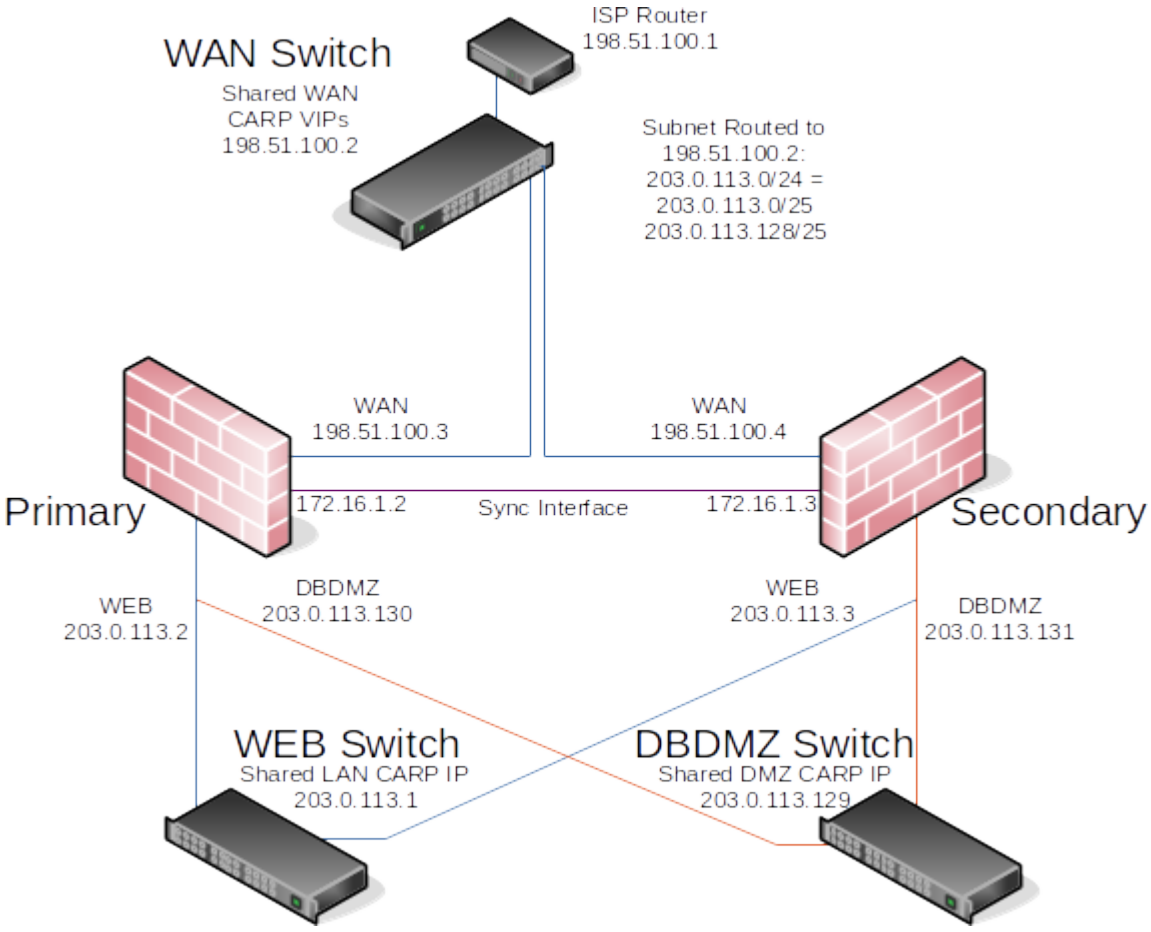


Fig. 7: Diagramma di HA con IP instradati

Layout di rete

La figura *Diagramma di HA con IP instradati* illustra questo layout di rete, compresi tutti gli indirizzi IP instradabili, la rete WEB, e il database DMZ.

Nota: i segmenti contenenti server di database in genere non devono essere accessibili pubblicamente e quindi utilizzerebbero più comunemente sottoreti IP private, ma l'esempio illustrato qui può essere utilizzato indipendentemente dalla funzione delle due sottoreti interne.

22.7 Ridondanza di livello 2

I diagrammi precedenti in questo capitolo non descrivevano la ridondanza del livello 2 (switch), per evitare di lanciare troppi concetti ai lettori contemporaneamente. Questa sezione copre gli elementi di progettazione di livello 2 da considerare quando si pianifica una rete ridondante. Questo capitolo presuppone una distribuzione di due sistemi, anche se questo si adatta a tutte le installazioni necessarie.

Se entrambi i firewall Firew4LL ridondanti sono collegati allo stesso switch su qualsiasi interfaccia, tale switch diventa un singolo punto di errore. Per evitare questo singolo punto di errore, la scelta migliore è quella di distribuire due switch per ogni interfaccia (diverso dall'interfaccia pfsync dedicata).

L'*Esempio del diagramma di rete HA* è centrato sulla rete, non mostra l'infrastruttura switch. La figura *Diagramma di HA con switch ridondanti* illustra come appare quell'ambiente con un'infrastruttura di switch ridondante.

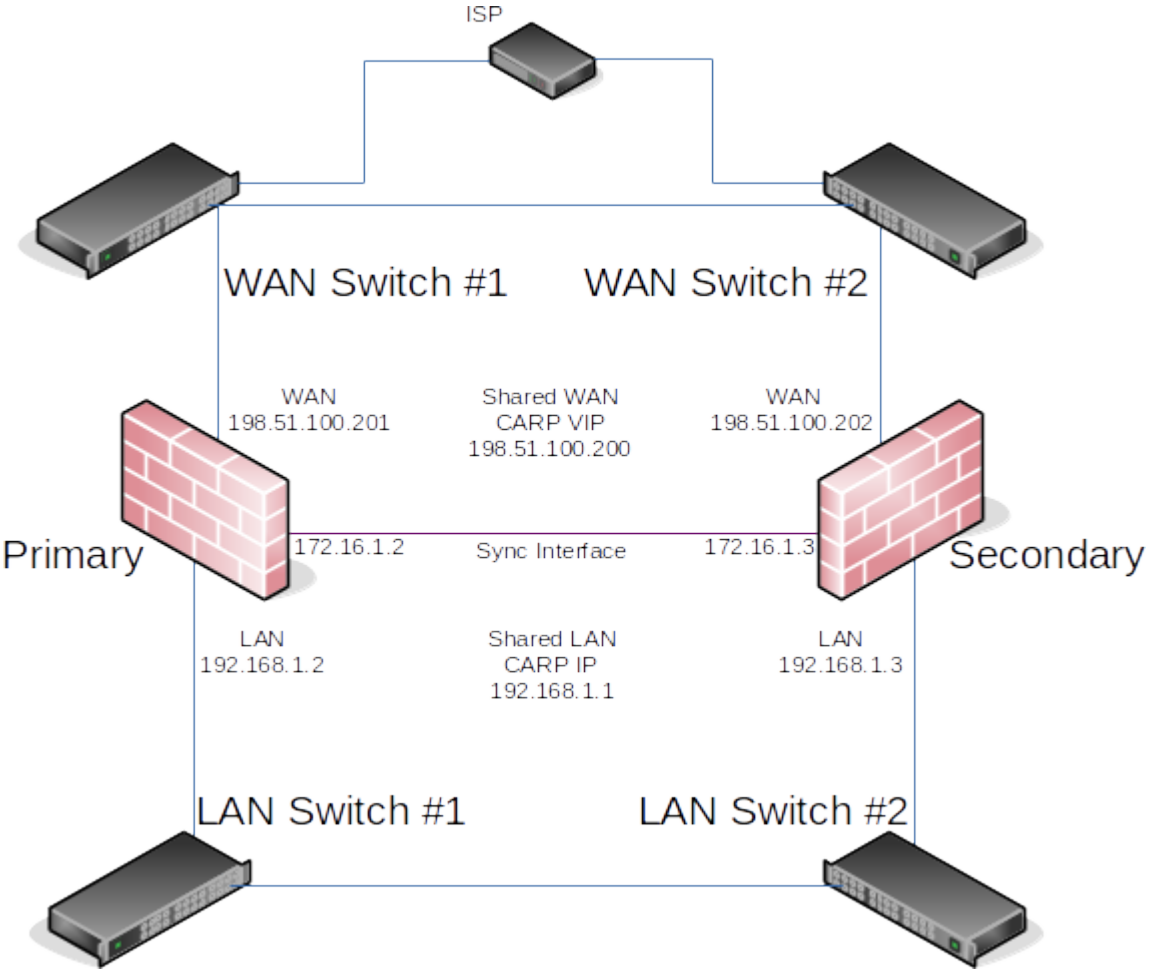


Fig. 8: Diagramma di HA con switch ridondanti

22.7.1 Configurazione dello switch

Quando si utilizzano più switch, gli switch devono essere interconnessi. Finché c'è una singola connessione tra i due switch e nessun ponte su uno dei firewall, questo è sicuro con qualsiasi tipo di switch. Dove si utilizza il bridging o dove esistono più interconnessioni tra gli switch, è necessario prestare attenzione per evitare loop di livello 2. Sarebbe necessario uno switch gestito che sia in grado di utilizzare il protocollo dell'albero di spanning (Spanning Tree Protocol, STP) per rilevare e bloccare le porte che altrimenti creerebbero loop di switch. Quando si utilizza STP, se un collegamento attivo muore, ad esempio un errore di commutazione, allora un collegamento di backup può essere automaticamente portato al suo posto.

Firew4LL ha anche il supporto per l'aggregazione del link di *lagg (4)* e interfacce di failover del link che permette più interfacce di rete per essere collegato a uno o più switch per una maggiore tolleranza ai guasti. Vedere *LAGG (Aggregazione di link)* per ulteriori informazioni sulla configurazione dell'aggregazione dei link.

22.7.2 Ridondanza dell'host

È più difficile ottenere la ridondanza dell'host per i sistemi critici all'interno del firewall. Ogni sistema potrebbe avere due schede di rete e una connessione a ciascun gruppo di switch utilizzando il protocollo del controllo di aggregazione del link (Link Aggregation Control Protocol, LACP) o funzionalità specifiche del fornitore simili. I server potrebbero anche avere più connessioni di rete e, a seconda del sistema operativo, potrebbe essere possibile eseguire il CARP o un protocollo simile su un set di server in modo che siano anche ridondanti. Fornire la ridondanza dell'host è più specifico per le funzionalità degli switch e dei sistemi operativi del server, che è al di fuori dell'ambito di questo libro.

22.7.3 Altri singoli punti di guasto

Quando si tenta di progettare una rete completamente ridondante, ci sono molti singoli punti di errore che a volte vengono persi. A seconda del livello di uptime da raggiungere, ci sono sempre più cose da considerare rispetto a un semplice errore di switch. Ecco alcuni altri esempi di ridondanza su scala più ampia:

- Alimentazione isolata per ogni segmento ridondante.
  - Utilizzare switch separati per sistemi ridondanti.
  - Utilizzare più banche/generatori UPS.
  - Utilizzare più fornitori di energia, inserendo lati opposti dell'edificio, ove possibile.
- Anche una configurazione Multi-WAN non è garanzia di uptime di Internet.
  - Utilizzare più tecnologie di connessione a Internet (DSL, cavo, fibra, Wireless).
  - Se due vettori utilizzano lo stesso polo/tunnel/percorso, entrambi potrebbero essere eliminati allo stesso tempo.
- Avere raffreddamento di backup, refrigeratori ridondanti o un condizionatore d'aria portatile/di emergenza.
- Considerare di posizionare il secondo set di apparecchiature ridondanti in un'altra stanza, in un altro piano o in un altro edificio.
- Avere una configurazione duplicata in un'altra parte della città o in un'altra città.
- Ho sentito che l'hosting è economico su Marte, ma la latenza è assassina.

22.8 HA con bridging

L'HA non è attualmente compatibile con il bridging in una capacità nativa che è considerata affidabile o degna di uso in produzione. Richiede un significativo intervento manuale. I dettagli del processo possono essere trovati in HA.

22.9 Utilizzare gli Alias di IP per ridurre il traffico di heartbeat

Se ci sono un gran numero di VIP del CARP su un segmento, questo può portare a un sacco di traffico multicast. Un heartbeat al secondo viene inviato per il VIP del CARP. Per ridurre questo traffico, i VIP aggiuntivi possono essere «impilati» in cima a un VIP del CARP su un'interfaccia. In primo luogo, scegliere un VIP del CARP per essere il VIP "principale" per l'interfaccia. Quindi, cambiare gli altri VIP CARP in quella stessa sottorete per essere un IP dell'Alias di tipo VIP, con l'interfaccia «principale» del VIP del CARP selezionata per essere la loro **interfaccia** sulla configurazione VIP.

Ciò non solo riduce i segnali vitali che verranno visualizzati su un determinato segmento, ma fa sì che tutti i VIP dell'alias IP cambino stato insieme al VIP del CARP "principale", riducendo la probabilità che un problema di livello 2 causi il mancato superamento dei singoli VIP del CARP come previsto.

I VIP dell'Alias IP normalmente non si sincronizzano tramite sincronizzazione di configurazione XML-RPC, tuttavia, i VIP dell'alias IP impostati per utilizzare le interfacce CARP in questo modo si sincronizzano.

22.10 Interfaccia

Se sono richieste più sottoreti su una singola interfaccia con HA, ciò può essere ottenuto utilizzando Alias dell'IP. Come per gli indirizzi IP dell'interfaccia principale, si consiglia a ciascun firewall di avere un indirizzo IP all'interno della sottorete aggiuntiva, per un totale di almeno tre IP per sottorete. Le voci dell'alias IP separate devono essere aggiunte a ciascun nodo all'interno della nuova sottorete, assicurandosi che le relative maschere di sottorete corrispondano alla maschera di sottorete effettiva per la nuova sottorete. I VIP dell'alias dell'IP che sono direttamente su un'interfaccia non si sincronizzano, quindi questo è sicuro.

Una volta che il VIP dell'alias dell'IP è stato aggiunto a entrambi i nodi per ottenere un punto d'appoggio nella nuova sottorete, il VIP del CARP può essere aggiunto utilizzando gli indirizzi IP dalla nuova sottorete.

È possibile omettere gli alias IP e utilizzare un VIP CARP direttamente nell'altra sottorete purché non sia richiesta la comunicazione tra la sottorete aggiuntiva ed entrambi i singoli nodi HA.

22.11 Risoluzione dei problemi di alta affidabilità

Le configurazioni ad HA possono essere complesse e con tanti modi diversi per configurare un cluster di failover, quindi può essere difficile far funzionare correttamente le cose. In questa sezione, alcuni problemi comuni (e non così comuni) saranno discussi e, si spera, risolti per la maggior parte dei casi. Se i problemi sono ancora presenti dopo aver consultato questa sezione, c'è una scheda CARP/VIP dedicata sul forum Firew4LL.

Prima di procedere, prendersi il tempo necessario per controllare tutti i membri del cluster HA per assicurarsi che abbiano configurazioni coerenti. Spesso, è d'aiuto fare riferimento alla configurazione di esempio, effettuare un doppio controllo su tutte le impostazioni corrette. Ripetere il processo sul nodo secondario e osservare i luoghi in cui la configurazione deve essere diversa sul secondario. Assicurarsi di controllare lo stato del CARP (*controllare lo stato del CARP*) e assicurarsi che il CARP sia abilitato su tutti i membri del cluster.

Gli errori relativi a HA verranno registrati in **Stato>Registro di sistema**, nella scheda **Sistema**. Controllare i registri di ciascun sistema coinvolto per vedere se ci sono messaggi relativi a XMLRPC Sync, transizioni degli stati del CARP o altri errori correlati.

22.11.1 Errori di configurazione comuni

Ci sono tre errori di configurazione comuni che possono accadere che impediscono a HA di funzionare correttamente.

Utilizzare un VHID diverso su ogni VIP del CARP

Un VHID diverso deve essere utilizzato su ogni VIP del CARP creato su una determinata interfaccia o dominio di trasmissione. Con una singola coppia HA, la convalida dell'input impedirà i VHID duplicati. Purtroppo non è sempre così semplice. CARP è una tecnologia multicast, e come tale qualsiasi cosa utilizzi il CARP sullo stesso segmento di rete deve utilizzare un VHID unico. VRRP utilizza anche un protocollo simile a CARP, quindi assicurarsi che non ci siano conflitti con i VHID di VRRP, come ad esempio se l'ISP o un altro router sulla rete locale utilizzi VRRP.

Il modo migliore per aggirare questo problema è usare un set unico di VHID. Se è in uso una rete privata sicura, iniziare a numerare da 1. Su una rete in cui VRRP o CARP sono in conflitto, consultare l'amministratore di tale rete per trovare un blocco gratuito di VHID

Tempi errati

Verificare che tutti i sistemi coinvolti sincronizzino correttamente i loro orologi e abbiano fusi orari validi, specialmente se in esecuzione in una macchina virtuale. Se gli orologi sono troppo distanti, alcune attività di sincronizzazione come il failover DHCP non funzioneranno correttamente.

Maschera di sottorete non corretta

La vera maschera di sottorete deve essere utilizzata per un VIP del CARP, non /32. Questo deve corrispondere alla maschera di sottorete per l'indirizzo IP sull'interfaccia a cui è assegnato l'IP CARP.

Indirizzo IP per l'interfaccia del CARP

L'interfaccia su cui risiede il VIP del CARP deve già avere un altro IP definito direttamente sull'interfaccia (VLAN, LAN, WAN, OPT) prima che possa essere utilizzato.

22.11.2 Errore di hash non corretto

Ci sono alcuni motivi per cui questo errore si presenta nei registri di sistema, alcuni più preoccupanti di altri.

Se il CARP non funziona correttamente quando questo errore è presente, potrebbe essere dovuto a una mancata corrispondenza nella configurazione. Assicurarsi che per un determinato VIP, il VHID, la password e l'indirizzo IP/maschera di sottorete corrispondano tutti.

Se le impostazioni sembrano essere corrette e il CARP ancora non funziona durante la generazione di questo messaggio di errore, allora ci possono essere più istanze CARP sullo stesso dominio broadcast. Disabilitare il CARP e monitorare la rete con tcpdump (*Cattura dei pacchetti*) per verificare la presenza di altri CARP o traffico simile al CARP e regolare i VHID in modo appropriato.

Se la CARP funziona correttamente e questo messaggio si trova nei registri quando il sistema si avvia, potrebbe essere ignorato. È normale che questo messaggio venga visualizzato durante l'avvio, purché il CARP continui a funzionare correttamente (il principale mostra **MASTER**, il secondario mostra **BACKUP** sullo stato).

22.11.3 Entrambi i sistemi appaiono come MASTER

Ciò accadrà se il secondario non può vedere gli annunci CARP del rimario primario. Verificare la presenza di regole del firewall, problemi di connettività, configurazioni di switch. Controllare anche i registri di sistema per eventuali errori rilevanti che possono portare a una soluzione. Se ciò si verifica in un prodotto VM (Virtual Machine) come ESX, vedere *Problemi all'interno delle macchine virtuali (ESX).*

22.11.4 Il sistema primario è bloccato in BACKUP

In alcuni casi, questo può accadere normalmente per un breve periodo dopo che un sistema torna online. Tuttavia, alcuni guasti hardware o altre condizioni di errore possono causare a un server di assumere silenziosamente un alto advskew di 240 per segnalare che ha ancora un problema e non dovrebbe diventare master. Questo può essere selezionato dalla GUI, o tramite la shell o **Diagnostica>Comando**.

Nella GUI, questa condizione viene stampata in un messaggio di errore su **Stato>CARP**.

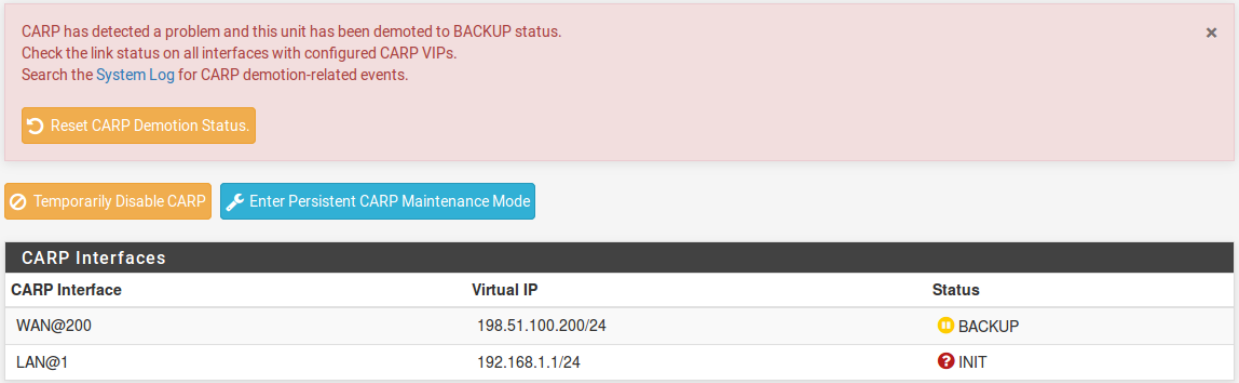


Fig. 9: Stato del CARP quando il primario è retrocesso

Dalla shell o da **Diagnostica>Comando**, eseguire il seguente comando per verificare la presenza di una retrocessione:

```
# sysctl net.inet.carp.demotion
```

net.inet.carp.demotion: 240

Se il valore è maggiore di 0, il nodo è retrocesso.

In tal caso, isolare il firewall, controllare le connessioni di rete ed eseguire ulteriori test hardware.

Se il valore di retrocessione è 0 e il nodo primario sembra ancora essere retrocesso a BACKUP o sta salternandosi, controllare la rete per assicurarsi che non ci siano loop di livello 2. Se il firewall riceve indietro i propri heartbeat dallo switch, può anche attivare una modifica allo stato di BACKUP.

22.11.5 Problemi all'interno delle macchine virtuali (ESX)

Quando si utilizza HA all'interno di una macchina virtuale, in particolare VMware ESX, sono necessarie alcune configurazioni speciali:

1. Attivare la modalità promiscua sul vSwitch.
2. Abilitare «modificare l'"indirizzo MAC».
3. Abilitare » Trasmissioni forgiate".

Espediente della modalità promiscua VDS di ESX

Se è in uso uno switch distribuito virtuale (Virtual Distributed Switch), è possibile creare un gruppo di porte per le interfacce firewall con modalità promiscua abilitata e un gruppo di porte non promiscue separato per altri host. Questo è stato segnalato come un modo funzionante dagli utenti sul forum per trovare un equilibrio tra i requisiti per lasciare la funzione CARP e per proteggere le porte dei client.

Problema con l'aggiornamento VDS di ESX

Se un VDS (switch distribuiti virtuali, Virtual Distributed Switch) è stato utilizzato in 4.0 o 4.1 e l'aggiornamento da 4.1 o 5.0, il VDS non passerà correttamente il traffico CARP. Se è stato creato un nuovo VDS su 4.1 o 5.0, funzionerà, ma il VDS aggiornato non lo farà.

È stato riferito che disabilitare la modalità promiscua sul VDS e quindi riattivarlo risolverà il problema.

Problema di mirroring della porta VDS di ESX

Se il mirroring della porta è abilitato su un VDS, si interromperà la modalità promiscua. Per risolvere il problema, disabilitare e quindi riattivare la modalità promiscua.

Problemi con la porta client di ESX

Se un cluster HA fisico è collegato a uno switch con un host ESX utilizzando più porte sull'host ESX (gruppo lagg o simili) e solo determinati dispositivi/IP sono raggiungibili dalla VM di destinazione, le impostazioni del gruppo di porte potrebbero dover essere regolate in ESX per impostare il bilanciamento del carico per il gruppo su hash basato sull'IP, non sull'interfaccia di origine.

Gli effetti collaterali di avere quell'impostazione in modo errato includono:

- Il traffico raggiunge solo la VM di destinazione in modalità promiscua sul suo NIC.
- Incapacità di raggiungere il VIP del CARP dalla VM di destinazione quando è possibile raggiungere l'indirizzo IP "reale" del firewall primario.
- Le porte forward o altre connessioni in ingresso alla VM di destinazione funzionano da alcuni indirizzi IP e non da altri.

L'errore NIC fisico di ESX non riesce a attivare il Failover

L'auto-retrocessione nel CARP si basa sulla perdita di collegamento su una porta switch. In quanto tale, se un'istanza firewall primaria e secondaria si trova su unità ESX separate e l'unità primaria perde un collegamento con la porta switch e non lo espone alla VM, CARP rimarrà MASTER su tutti i suoi VIP lì e il secondario crederà anche che dovrebbe essere MASTER. Un modo per aggirare questo problema è quello di usare uno script di un evento in ESX che manderà down la porta switch sulla VM se la porta fisica perde il collegamento. Ci possono essere altri modi per aggirare questo problema in ESX puro.

Problemi KVM+Qemu

Utilizzare *(em (4))* di NIC e1000, non *ed(4)* di NIC o i VIP del CARP non lasceranno mai lo stato dell'inizializzazione.

Problemi con VirtualBox

Impostare la «Modalità promiscua: Permettere tutto» sulle interfacce pertinenti della VM consente al CARP di funzionare su qualsiasi tipo di interfaccia (ponte, solo Host, interno)

22.11.6 Altri problemi di switch e livello 2

- Se le unità sono collegate a switch separati, assicurarsi che gli switch stiano effettuando correttamente il trunking e passando il traffico broadcast/multicast.
- Alcuni switch hanno funzioni di filtraggio broadcast/multicast, limitanti o con il "controllo tempesta" ("storm control") che possono rompere il CARP.
- Alcuni iswitch hanno rotto il firmware che può causare caratteristiche come lo snooping di IGMP che interferisce con il CARP.
- Se si utilizza uno switch sul retro di un modem/CPE, provare invece uno switch reale. Questi switch integrati spesso non gestiscono correttamente il traffico del CARP. Spesso collegare i firewall in un switch corretto e quindi collegarsi al CPE eliminerà i problemi.

22.11.7 Problemi di sincronizzazione della configurazione

Controllare due volte i seguenti elementi quando si riscontrano problemi con la sincronizzazione della configurazione:

- Il nome utente deve essere **admin** su tutti i nodi.
- La password nelle impostazioni di sincronizzazione della configurazione sul primario deve corrispondere alla password del backup.
- La WebGUI deve essere sulla stessa porta su tutti i nodi.
- La WebGUI deve utilizzare lo stesso protocollo (HTTP o HTTPS) su tutti i nodi.
- Il traffico deve essere consentito alla porta WebGUI sull'interfaccia che gestisce il traffico di sincronizzazione.
- L'interfaccia pfsync deve essere abilitata e configurata su tutti i nodi.
- Verificare che solo il nodo di sincronizzazione del primario abbia abilitato le opzioni di sincronizzazione della configurazione.
- Assicurarsi che non venga specificato alcun indirizzo IP nella configurazione di sincronizzazione sull'IP del nodo secondario.
- Assicurarsi che gli orologi su entrambi i nodi siano correnti e siano ragionevolmente accurati.

22.11.8 Risoluzione dei problemi HA e Multi-WAN

Se si riscontrano problemi nel raggiungere i VIP del CARP da quando si ha a che fare con Multi-WAN, controllare due volte che una regola sia presente come quella menzionata nella configurazione del firewall

Firew4LL è una delle pochissime soluzioni open source che offre funzionalità di HA di classe aziendale con failover stateful, consentendo l'eliminazione del firewall come un singolo punto di errore. L'HA si ottiene attraverso una combinazione di funzionalità:

- CARP per la ridondanza degli indirizzi IP
- Xmlrpc per la sincronizzazione della configurazione
- pfsync per la sincronizzazione della tabella di stato

Con questa configurazione, le unità fungono da cluster «attivo/passivo» con il nodo primario che funziona come unità master e il nodo secondario nel ruolo di backup, subentrando se necessario se il nodo primario fallisce.

Sebbene spesso erroneamente chiamato «Cluster CARP», due o più firewall Firew4LL ridondanti sono più giustamente chiamati «Cluster ad elevata disponibilità» o «cluster HA», poiché il CARP è solo una delle diverse tecnologie utilizzate per ottenere un'HA con Firew4LL e in futuro il CARP potrebbe essere scambiato per un diverso protocollo di ridondanza.

Un'interfaccia su ciascun nodo cluster sarà dedicata per le attività di sincronizzazione. Questa è in genere indicata come l'interfaccia «Sync», ed è utilizzata per la sincronizzazione della configurazione e la sincronizzazione dello stato di pfsync. Qualsiasi interfaccia disponibile può essere utilizzata.

Nota: alcuni la chiamano l'interfaccia «CARP» ma questo nome è errato e molto fuorviante. Gli heartbeat del CARP si vengono inviati su ogni interfaccia con un VIP del CARP; il traffico del CARP e failover non utilizzano l'interfaccia di sincronizzazione.

La configurazione del cluster ad HA più comune include solo due nodi. È possibile avere più nodi in un cluster, ma non forniscono un vantaggio significativo.

È importante distinguere tra tre funzioni (ridondanza dell'indirizzo IP, sincronizzazione della configurazione e sincronizzazione della tabella di stato), poiché si verificano in luoghi diversi. La sincronizzazione della configurazione e la sincronizzazione dello stato avvengono sull'interfaccia di sincronizzazione, comunicando direttamente tra le unità firewall. Gli heartbeat del CARP vengono inviati su ogni interfaccia con un VIP del CARP. La segnalazione di failover non vengono inviate sull'interfaccia di sincronizzazione, ma piuttosto su ogni interfaccia abilitata al CARP.

Vedi anche:

Per ulteriori informazioni, è possibile accedere all'archivio degli Hangouts che contiene l'Hangout di giugno 2015 che copre anche l'elevata disponibilità.

22.12 Panoramica CARP

Protocollo di ridondanza dell'indirizzo comune (Common Address Redundancy Protocol, CARP) è stato creato dagli sviluppatori OpenBSD come soluzione di ridondanza libera e aperta per la condivisione di indirizzi IP tra un gruppo di dispositivi di rete. Soluzioni simili esistevano già, principalmente lo standard IETF per il protocollo di ridondanza dei router virtuali (Virtual Router Redundancy Protocol, VRRP). Tuttavia Cisco sostiene VRRP che è coperto dal brevetto sul loro protocollo del router in hot standby (Hot Standby Router Protocol, HSRP), e ha detto agli sviluppatori OpenBSD che dovrebbero rispettare il brevetto. Quindi, gli sviluppatori OpenBSD hanno creato un nuovo protocollo libero e aperto per ottenere essenzialmente lo stesso risultato senza violare il brevetto di Cisco. CARP è diventato disponibile nell'ottobre OpenBSD e successivamente è stato aggiunto anche a FreeBSD.

Un indirizzo IP virtuale di tipo CARP (VIP) viene condiviso tra i nodi di un cluster. Un nodo è master e riceve traffico per l'indirizzo IP e gli altri nodi mantengono lo stato di backup e monitorano i suoi segnali vitali per vedere se devono assumere il ruolo master se il master precedente fallisce. Poiché solo un membro del cluster alla volta utilizza l'indirizzo IP, non vi è alcun conflitto di indirizzi IP per i VIP CARP.

Affinché il failover funzioni correttamente è importante che il traffico in entrata che arriva al cluster, come traffico upstream instradato, VPN, NAT, gateway del client locale, richieste DNS, ecc., sia inviato a un VIP CARP e il traffico in uscita come NAT in uscita sia inviato da un VIP CARP. Se il traffico viene indirizzato direttamente a un nodo e non a un VIP CARP, il traffico non verrà prelevato da altri nodi.

Il CARP funziona in modo simile a VRRP e HSRP, e può anche essere in conflitto in alcuni casi. I segnali vitali vengono inviati su ogni interfaccia contenente un VIP del CARP, un heartbeat per VIP per interfaccia. Ai valori predefiniti per distorto e base, un VIP invia heartbeat circa una volta al secondo. L'inclinazione determina quale nodo è il master in un dato punto nel tempo. Qualunque nodo trasmetta i bgli heartbeat, il più veloce assume il ruolo

principale. Un valore di inclinazione più alto fa sì che i segnali vitali vengano trasmessi con più ritardo, quindi un nodo con un inclinazione inferiore sarà il master a meno che una rete o un altro problema non causi il ritardo o la perdita dei segnali vitali.

Nota: non accedere mai alla GUI, SSH o ad altri meccanismi di gestione del firewall utilizzando un VIP del CARP. Per scopi di gestione, utilizzare solo l'indirizzo IP effettivo sull'interfaccia di ciascun nodo separato e non il VIP. Altrimenti non può essere determinato in anticipo quale unità è accessibile.

22.12.1 Requisiti indirizzamento IP per il CARP

Un cluster ad HA che utilizza il CARP ha bisogno di tre indirizzi IP in ogni sottorete insieme a una sottorete separata inutilizzata per l'interfaccia di sincronizzazione. Per le WAN, ciò significa che è necessaria una sottorete a /29 o più grande per una configurazione ottimale. Un indirizzo IP viene utilizzato da ciascun nodo, più un indirizzo VIP CARP condiviso per il failover. L'interfaccia di sincronizzazione richiede solo un indirizzo IP per nodo.

È tecnicamente possibile configurare un'interfaccia con un VIP CARP come unico indirizzo IP in una determinata sottorete, ma non è generalmente raccomandato. Quando viene utilizzato su una WAN, questo tipo di configurazione consentirà solo la comunicazione dal nodo primario alla WAN, il che complica notevolmente l'attività come aggiornamenti, installazioni di pacchetti, monitoraggio gateway o qualsiasi cosa che richieda connettività esterna dal nodo secondario. Può essere più adatto per un'interfaccia interna, tuttavia le interfacce interne in genere non soffrono delle stesse limitazioni dell'indirizzo IP di una WAN, quindi è comunque preferibile configurare gli indirizzi IP su tutti i nodi.

22.12.2 Preoccupazioni riguardo switch/livello 2

I segnali vitali del CARP utilizzano multicast e possono richiedere una gestione speciale sugli switch coinvolti nel cluster. Alcuni iswitch filtrano, limitano la velocità o altrimenti interferiscono con il multicast in modi che possono causare il fallimento del CARP. Inoltre, alcuni switch utilizzano metodi di sicurezza delle porte che potrebbero non funzionare correttamente con il CARP.

Come minimo, lo switch deve:

- Consentire il traffico multicast di essere inviato e ricevuto senza interferenze sulle porte utilizzando un VIP del CARP.
- Consentire al traffico di essere inviato e ricevuto utilizzando più indirizzi MAC.
- Consentire all'indirizzo MAC del VIP del CARP di spostarsi tra le porte.

Quasi tutti i problemi con il CARP che non riescono a riflettere correttamente lo stato previsto presentano guasti dello switch o altri problemi di livello 2, quindi assicurati che gli switch siano configurati correttamente prima di continuare.

CAPITOLO 23

Servizi

23.1 Server DHCP IPv4

Il **server DHCP** IPv4 assegna indirizzi IPv4 e relative opzioni di configurazione ai PC client su una rete. È abilitato per impostazione predefinita sull'interfaccia LAN con un intervallo predefinito da of 192.168.1.100 a 192.168.1.199. In questa configurazione predefinita, il firewall assegna il suo indirizzo IP della LAN (192.168.1.1) come gateway e server DNS se il risolutore del DNS o il forwarder del DNS è abilitato. Ci sono numerose opzioni disponibili nell'interfaccia web, che sono coperte nella sezione successiva.

23.1.1 Configurazione

Per modificare il comportamento del server DHCP IPv4, passare a **Servizi> Server DHCP** nell'interfaccia web. Il comportamento del server DHCP IPv4 è controllato lì, insieme alle mappature degli indirizzi IP statici e alle opzioni correlate come l'ARP statico.

Scegliere un'interfaccia

La pagina di configurazione DHCP contiene una scheda per ogni interfaccia con un indirizzo IP statico. Ogni interfaccia ha una propria configurazione server DHCP separata e può essere abilitata o disabilitata indipendentemente l'una dall'altra. Prima di apportare modifiche, visitare la scheda per l'interfaccia corretta.

Opzioni generali

Abilitare La prima impostazione della scheda abilita o disabilita il servizio DHCP per l'interfaccia. Per attivare DHCP per l'Interfaccia, selezionare Ab**ilitare server DHCP sull'interfaccia [nome].** Per disabilitare il servizio, deselezionare invece la casella.

Negare client sconosciuti In circostanze normali, il server DHCP risponderà alle richieste di qualsiasi client che richiede una lease. Nella maggior parte degli ambienti questo è un comportamento normale e accettabile, ma in ambienti ristretti o sicuri questo comportamento è indesiderabile. Con questo set

di opzioni, solo i client con mappature statiche definite riceveranno le lease. Questa è una pratica più sicura, ma è molto meno comoda. Questa opzione è per il pool, il che significa che se i client sconosciuti vengono negati nell'intervallo predefinito, potrebbe essere definito un altro pool di indirizzi IP che non ha l'impostazione selezionata. Il server DHCP assegnerà invece gli indirizzi IP dei client da quel pool alternativo.

Nota: ciò proteggerà dagli utenti a bassa conoscenza e dalle persone che inseriscono casualmente i dispositivi. Essere consapevoli, tuttavia, che un utente con conoscenza della rete potrebbe codificare un indirizzo IP, una maschera di rete, un gateway, e un DNS che darà ancora loro accesso. Potrebbero anche alterare/falsificare il loro indirizzo MAC per abbinare un client valido e ottenere ancora una lease. Se possibile, accoppiare questa impostazione con voci ARP statiche, con il controllo di accesso in uno switch che limiterà gli indirizzi MAC a determinate porte switch per una maggiore sicurezza e disattivare o disabilitare le porte switch inutilizzate.

Subnet L'indirizzo di rete della Subnet dell'interfaccia.

Subnet Maskt La Subnet Mask per la Subnet dell'interfaccia.

Range disponibile L'intervallo di indirizzi disponibili all'interno della Subnet dell'interfaccia, per riferimento e per determinare l'intervallo desiderato per i client DHCP. L'indirizzo di rete e l'indirizzo di trasmissione sono esclusi, ma gli indirizzi di interfaccia e gli indirizzi IP virtuali non sono esclusi.

Range Definisce l'intervallo di indirizzi DHCP, indicato anche come ambito o pool. Le due caselle per l'intervallo indicano al firewall il primo e l'ultimo indirizzo da utilizzare come pool DHCP. Gli indirizzi tra i valori inseriti, inclusi, verranno utilizzati per i client che richiedono indirizzi tramite DHCP. L'intervallo deve essere inserito prima con il numero inferiore, seguito dal numero più alto. Ad esempio, l'intervallo DHCP della LAN predefinito è basato sulla Subnet per l'indirizzo IP della LAN predefinito. È da 192.168.1.100 a 192.168.1.199. Questo intervallo può essere grande o piccolo quanto il bisogno della rete, ma deve essere interamente contenuto all'interno della Subnet per l'interfaccia configurata.

Pool aggiuntivi

La sezione dei pool aggiuntivi definisce pool extra di indirizzi all'interno della stessa Subnet. Questi pool possono essere utilizzati per creare set di indirizzi IP specifici per determinati client, o per un eccesso da un pool originale più piccolo, o per dividere il pool principale in blocchi più piccoli con uno spazio di indirizzi IP non DHCP nella metà di quello che era il pool. Una combinazione delle opzioni di controllo degli indirizzi MAC può essere utilizzata per guidare i client dello stesso produttore in un pool specifico, come i telefoni VoIP.

Per aggiungere un nuovo pool, fare clic su  **Aggiungere un pool** e lo schermo passerà alla vista della modifica del pool, che è quasi la stessa delle normali opzioni DHCP, ad eccezione di alcune opzioni che non sono attualmente possibili nei pool. Le opzioni si comportano come le altre discusse in questa sezione. Gli elementi lasciati vuoti, per impostazione predefinita, cadranno e utilizzeranno le opzioni dall'intervallo DHCP principale.

Nota: Vedere la sezione di controllo degli indirizzi MAC qui sotto per le specifiche su come indirizzare i client verso o lontano dai pool.

Server

Server WINS Possono essere definiti due server WINS (Servizio dei nomi di internet di Windows, Windows Internet Name Service) che verranno trasmessi ai client. Se è necessario uno o più server WINS,

inserire qui i loro indirizzi IP. I server effettivi non devono essere su questa Subnet, ma assicurarsi che le regole di routing e firewall corrette siano in atto per consentire loro di essere raggiunti dai PC client. Se questo viene lasciato vuoto, nessun server WINS verrà inviato al client.

Server DNS I server DNS devono o non devono essere compilati, a seconda della configurazione del firewall. Se il risolutore del DNS integrato o il forwarder del DNS viene utilizzato per gestire il DNS, lasciare questi campi vuoti e Firew4LL si assegnerà automaticamente come server DNS per i PC client. Se il forwarder del DNS è disabilitato e questi campi sono lasciati vuoti, Firew4LL passerà su qualsiasi server DNS sia definito in **Sistema>Configurazione generale**. Per utilizzare i server DNS personalizzati al posto delle scelte automatiche, compilare gli indirizzi IP per un massimo di quattro server DNS qui. Nelle reti con server Windows, in particolare quelli che impiegano la directory attiva, si consiglia di utilizzare tali server per i DNS del client. Quando si utilizza il risolutore DNS o il forwarder DNS in combinazione con il CARP, specificare l'indirizzo IP virtuale del CARP su questa interfaccia qui.

Altre opzioni

Gateway Questo può anche essere lasciato vuoto se questo firewall agisce come gateway per la rete su questa interfaccia. Se questo non è il caso, compilare l'indirizzo IP per il gateway utilizzato dai client su questa interfaccia. Quando si utilizza il CARP, compilare l'indirizzo IP virtuale nel CARP su questa interfaccia qui.

Nome di dominio Specifica il nome di dominio passato al client per formarne l'hostname completo. Se il **nome di dominio** viene lasciato vuoto, il nome di dominio del firewall inviato al client. In caso contrario, al client viene inviato questo valore.

Elenco di domini di ricerca Controlla i domini di ricerca DNS forniti al client tramite DHCP. Se sono presenti domini multipli e sono desiderati nomi host brevi, fornire un elenco di nomi di dominio qui, separati da un punto e virgola. I client tenteranno di risolvere i nomi host aggiungendo i domini, a loro volta, da questo elenco prima di cercare di trovarli esternamente. Se lasciato vuoto, viene utilizzata l'opzione di dominio.

Nota: L'elenco di **domini di ricerca** viene fornito tramite l'opzione 119 di DHCP. A partire da questa scrittura, nessun client DHCP di Windows di qualsiasi versione supporta l'opzione 119 DHCP. Altri sistemi operativi come BSD, Linux e OS X supportano l'ottenimento dell'elenco dei domini di ricerca tramite l'opzione 119 di DHCP.

Tempo di lease predefinito Controlla per quanto tempo una lease durerà quando un client non richiede una specifica lunghezza di lease. Specificato in secondi, il valore predefinito è 7200 secondi (2 ore)

Tempo massimo di lease Limita la durata della lease richiesta a un tempo massimo dichiarato. Specificato in secondi, il valore predefinito è 86400 secondi (1 giorno).

IP del peer di failover Se questo sistema fa parte di un cluster di failover a elevata disponibilità, immettere qui l'indirizzo IP reale dell'altro sistema in questa Subnet. Non inserire un indirizzo IP virtuale CARP.

ARP statica Questa casella di selezione funziona in modo simile a negare gli indirizzi MAC sconosciuti dall'ottenimento della lease, ma fa un ulteriore passo avanti in quanto limita anche qualsiasi indirizzo MAC sconosciuto dalla comunicazione con questo firewall. Questo arresta gli aspiranti abusatori dalla codificazione di un indirizzo non utilizzato su questa Subnet, eludendo le restrizioni DHCP.

Nota: Quando si utilizza l'ARP statica, tutti i sistemi che devono comunicare con il firewall devono essere elencati in mappature statiche prima di attivare questa opzione, in particolare il sistema utilizzato per connettersi alla GUI di Firew4LL. Bisogna essere consapevoli del fatto

che questa opzione può impedire alle persone di codificare un indirizzo IP e parlare con il firewall, ma non impedisce loro di raggiungere l'altro sul segmento di rete locale.

Modificare il formato dell'ora Per impostazione predefinita, il demone DHCP di ISC mantiene i tempi di lease in UTC. Quando questa opzione è selezionata, i tempi nella pagina di stato delle lease DHCP vengono convertiti nel fuso orario locale definito sul firewall.

Grafici delle statistiche Questa opzione, disabilitata per impostazione predefinita, attiva il grafico RRD per il monitoraggio dell'utilizzo del pool DHCP.

DNS dinamico

Per le impostazioni del DNS dinamico, fare clic su **Visualizzare avanzate** a destra di quel campo, che visualizza le seguenti opzioni:

Abilitare Selezionare la casella per abilitare la registrazione dei nomi client DHCP in DNS utilizzando un server DNS esterno (non Firew4LL).

Dominio DDNS Il nome di dominio utilizzato per la registrazione dei client in DNS

Indirizzo del DDNS primario Il server DNS utilizzato per la registrazione dei client in DNS

Chiave del dominio DNS La chiave di crittografia utilizzata per la registrazione DNS

Segreto della chiave del dominio DNS Il segreto per la chiave utilizzata per la registrazione DNS

Controllo dell'indirizzo MAC

Per il controllo degli indirizzi MAC, fare clic su **Visualizzare avanzate** per visualizzare gli elenchi degli indirizzi MAC dei client consentiti e negati. Ogni elenco è separato da virgole e contiene porzioni di indirizzi MAC. Ad esempio, un gruppo di telefoni VoIP dello stesso produttore può iniziare con l'indirizzo MAC aa:bb:cc. Questo può essere sfruttato per dare opzioni separate agli utenti DHCP o ai gruppi di dispositivi.

Consentire Un elenco di indirizzi MAC da consentire in questo pool. Se un indirizzo MAC si trova nella casella consentire, tutti gli altri verranno negati tranne l'indirizzo MAC specificato nella casella consentire.

Negare Un elenco di indirizzi MAC da negare da questo pool. Se un indirizzo MAC è nell'elenco negare, sono consentiti tutti gli altri.

È meglio usare una combinazione di permessi e negazione per ottenere il risultato desiderato,come ad esempio: nel pool principale, lasciare Consentire vuoto e Negare con aa:bb:cc. Quindi nel pool dei VoIP, consentire aa:bb:cc. Se tale passaggio aggiuntivo non viene eseguito per consentire il prefisso MAC nel pool aggiuntivo, altri client di telefonia non VoIP potrebbero ricevere indirizzi IP da tale pool, il che potrebbe portare a comportamenti indesiderati.

Questo comportamento può essere assunto anche per alcuni dispositivi delle lista nera per la ricezione di una risposta DHCP. Ad esempio, per evitare che le stampanti di marca ricevano un indirizzo DHCP, se gli indirizzi MAC iniziano tutti con ee:ee:ee, posizionarlo nell'elenco negare di ciascun pool.

Server NTP

Per specificare i server NTP (Server del protocollo dell'orario di rete, Network Time Protocol Server), fare clic sul pulsante **Visualizzare avanzate** a destra di quel campo e immettere gli indirizzi IP per un massimo di due server NTP.

Server TFTP

Fare clic sul pulsante **Visualizzare avanzate** accanto a **TFTP** per visualizzare l'opzione server TFTP. Il valore nella casella server TFTP, se lo si desidera, deve essere un indirizzo IP o un hostname di un server TFTP. Questo è più spesso utilizzato per i telefoni VoIP, e può anche essere indicato come «opzione 66» in altra documentazione per VoIP e DHCP.

URI di LDAP

Fare clic sul pulsante **Visualizzare avanzate** accanto a **LDAP** per visualizzare l'opzione **URI server LDAP**. **L'URI del server LDAP** invierà un URI del server LDAP al client se richiesto. Questo può anche essere indicato come opzione 95 di DHCP. Prende la forma di un URI di LDAP completo, come ldap://ldap.example.com/dc=example,dc=com. Questa opzione può aiutare i client che utilizzano determinati tipi di sistemi, come OpenDirectory, a trovare il loro server.

Opzioni aggiuntive BOOTP/DHCP

Altre opzioni DHCP numeriche possono essere inviate ai client utilizzando i controlli delle **opzioni aggiuntive di BOOTP/DHCP.** Per visualizzare queste opzioni, fare clic su **Visualizzare avanzate** in questa sezione. Per aggiungere una nuova opzione, fare clic su **Aggiungere**.

Numero Il numero di codice dell'opzione DHCP. IANA mantiene un elenco di tutte le opzioni DHCP valide.

Tipo Le scelte e i formati per ogni tipo possono essere un po' contro-intuitivi, ma le etichette vengono utilizzate direttamente dal demone DHCP. Gli usi e i formati appropriati sono:

Testo Testo in forma libera da inviare in risposta, come ad esempio http://www.example.com/wpad/wpad.dat o società di esempio.

Stringa Una stringa di cifre esadecimali separate da due punti, come c0:a8:05:0c.

Booleana Vero o falso.

Numero intero a 8, 16 o 32 bit non firmato Un numero intero positivo che si adatta all'interno della data dimensione dei dati, come 86400.

Numero intero a 8, 16 o 32 bit firmato Un numero intero positivo o negativo che si adatta all'interno della data dimensione dei dati, come -512.

Indirizzo IP o host Un indirizzo IP come 192.168.1.1 o un nome host come www.example.com.

Valore Il valore associato a questa opzione numerica e tipo.

Per ulteriori informazioni su quali opzioni assumono un tipo o un formato specifico, vedere l'elenco collegato sopra la IANA.

Avvio della rete

Per visualizzare le impostazioni di avvio della rete, fare clic su sulla barra dell'intestazione della sezione di **avvio della rete**.

Abilitare Controllare per abilitare le opzioni di avvio di rete in DHCP

Server Successivo L'indirizzo IP da cui sono disponibili le immagini di avvio

Nome file del BIOS predefinito Nome file per l'immagine di avvio (non UEFI)

Nome file UEFI a 32 bit File per l'avvio UEFI a 32 bit

Nome file UEFI a 64 bit File per l'avvio UEFI a 64 bit

Percorso root Stringa per indirizzare un dispositivo specifico come dispositivo del filesystem della root del client, ad esempio iscsi:(servername):(protocol):(port):(LUN):targetname.

Salvare le impostazioni

Dopo aver apportato le modifiche, fare clic su **Salvare** prima di tentare di creare mappature statiche. Le modifiche alle impostazioni andranno perse se il browser lascia questa pagina senza salvare.

Mappa statica

Le mappature DHCP statiche esprimono una preferenza per cui l'indirizzo IP verrà assegnato a un determinato client in base al suo indirizzo MAC. In una rete in cui vengono negati client sconosciuti, questo serve anche come un elenco di client "noti" che possono ricevere lease o avere voci ARP statiche. Le mappature statiche possono essere aggiunte in uno dei due modi:

- Da questa schermata, fare clic su  Aggiungere.
- Aggiungerli dalla vista delle lease DHCP, di cui si discute più avanti in questo capitolo.

  In questa schermata, è necessario solo l'indirizzo MAC.

  Indirizzo MAC L'indirizzo MAC del client che identifica l'host per distribuire le opzioni in questa pagina o inserendo solo l'indirizzo MAC, verrà aggiunto all'elenco dei client noti da utilizzare quando è impostata l'opzione **Negare i client sconosciuti**.

  Nota: L'indirizzo MAC del client può essere ottenuto da un prompt dei comandi sulla maggior parte delle piattaforme. Su sistemi operativi basati su UNIX o che lavorano come Unix tra cui Mac OS X, digitando ifconfig-a verrà mostrato l'indirizzo MAC per ogni interfaccia. Su piattaforme basate su Windows, `ipconfig /all` mostrerà l'indirizzo MAC. L'indirizzo MAC può anche a volte essere trovato su un adesivo sulla scheda di rete, o vicino al jack di rete per adattatori integrati. Per gli host sulla stessa Subnet, il MAC può essere determinato eseguendo il ping dell'indirizzo IP dell'host e quindi eseguendo arp - a.

  Identificativo del client Un ID inviato dal cliente per identificarsi.

  Indirizzo IP Il campo dell'indirizzo IP è necessario se si tratta di una mappatura degli indirizzi IP statici invece di informare solo il server DHCP che il client è valido. Questo indirizzo IP è una preferenza, non una prenotazione. L'assegnazione di un indirizzo IP qui non impedirà a qualcun altro di utilizzare lo stesso indirizzo IP. Se questo indirizzo IP è in uso quando questo client richiede un lease, riceverà invece un indirizzo dal pool generale. Per questo motivo, la WebGUI di Firew4LL non consente di assegnare mappature IP statiche all'interno del pool DHCP.

  Hostname L'hostname del client. Questo non deve corrispondere al hostname effettivo impostato sul client. L'hostname impostato qui verrà utilizzato quando si registrano gli indirizzi DHCP nel forwarder del DNS.

  Descrizione Solo estetica, e disponibile per aiutare a tenere traccia di eventuali ulteriori informazioni su questa voce. Potrebbe essere il nome della persona che utilizza il PC, la sua funzione, il motivo per cui aveva bisogno di un indirizzo statico o l'amministratore che ha aggiunto la voce. Può anche essere lasciato vuoto.

Voce statica della tabella ARP Se selezionata, questa voce riceverà una voce ARP statica nel sistema operativo che lega questo indirizzo IP a questo indirizzo MAC.

> **Nota:** Se questa opzione viene utilizzata piuttosto che utilizzare l'opzione ARP statica globale, non impedisce che l'indirizzo MAC utilizzi altri indirizzi IP, impedisce solo ad altri indirizzi MAC di utilizzare questo indirizzo IP. In altre parole, impedisce a un'altra macchina di utilizzare quell'IP per raggiungere il firewall, ma non impedisce all'utente di cambiare il proprio indirizzo IP in qualcosa di diverso.

Le restanti opzioni disponibili per impostare questo client sono le stesse nel comportamento di quelle che si trovano in precedenza in questa sezione per le impostazioni DHCP principali.

Fare clic su **Salvare** per terminare la modifica della mappatura statica e tornare alla pagina di configurazione del server DHCP.

23.1.2 Stato

Lo stato del servizio del server DHCP stesso è in **Stato>Servizi**. Se il server DHCP è abilitato, il suo stato verrà visualizzato come in esecuzione, come nella figura *Stato del servizio del demone di DHCP*. I pulsanti sul lato destro consentono di riavviare o arrestare il demone del server DHCP. Il riavvio non è normalmente necessario in quanto Firew4LL riavvierà automaticamente il servizio quando vengono apportate modifiche alla configurazione che richiedono un riavvio. È probabile che anche l'arresto del servizio non sia necessario, poiché il servizio si arresta quando tutte le istanze del server DHCP sono disabilitate.

Services

Service	Description	Status	Actions
bsnmpd	SNMP Service	Running	
dhcpd	DHCP Service	Running	
dpinger	Gateway Monitoring Daemon	Running	
ipsec	IPsec VPN	Running	

Fig. 1: Stato del servizio del demone di DHCP

23.1.3 Lease

Le lease DHCP attualmente assegnate sono visualizzabili in **Stato>lease DHCP**. Questa pagina mostra vari aspetti dei contratti di lease del cliente. Questi includono:

- Indirizzo IP assegnato
- Indirizzo MAC del client
- L'hostname (se presente) che il client ha inviato come parte della richiesta DHCP
- La descrizione di un host con una mappatura statica DHCP
- Gli orari di inizio e fine della lease
- Se la macchina è attualmente online o meno (nella tabella ARP del firewall)
- Se la lease è attiva, scaduta o una registrazione statica

Visualizzazione delle lease inattive

Per impostazione predefinita, vengono visualizzati solo le lease attive e statiche, ma tutto, incluse le lease scade, può essere visualizzato facendo clic su **Mostrare tutte le lease configurate**. Per ridurre la visualizzazione alla normalità, fare clic solo su Mostrare solo lease attive e statiche.

Risvegliare l'integrazione della LAN

Facendo clic su  l'icona a destra del lease si invia un pacchetto Svegliare la LAN (WOL) su quell'host. Fare clic su  per creare una voce WOL per l'indirizzo MAC. Per maggiori dettagli sul risveglio della LAN, vedere *Svegliare la LAN*.

Aggiungere alla mappa statica

Per creare una mappatura statica da un lease dinamico, fare clic su  a destra del lease. Questo pre-riempirà l'indirizzo MAC di quell'host nella schermata **Modificare la mappatura statica**. Aggiungere l'indirizzo IP, l'hostname e la descrizione desiderati e fare clic su **Salvare**.

Eliminare la lease

Durante la visualizzazione delle lease, lease inattive o scadute possono essere eliminate manualmente facendo clic su  alla fine della sua riga. Questa opzione non è disponibile per i leasing attivi o statici, solo per i leasing offline o scaduti.

23.1.4 Registri del servizio DHCP

Il demone DHCP registrerà la sua attività in **Stato>Registro di sistema**, nella scheda DHCP. Verrà visualizzata ogni richiesta e risposta DHCP, insieme ad altri messaggi di stato e di errore.

23.2 Annunci del router e server DHCP con IPv6

L'assegnazione automatica degli indirizzi per IPv6 funziona in modo leggermente diverso rispetto a IPv4. Anche così, la maggior parte delle opzioni DHCP sono simili, ma ci sono notevoli differenze del comportamento nel modo in cui le cose vengono assegnate e anche come gli elementi come il gateway vengono consegnati ai client. Se non diversamente specificato, le opzioni con lo stesso nome funzionano allo stesso modo per DHCP e DHCPv6. DHCPv6 e gli annunci del router (Router Advertisements, RA) sono configurati in **Servizi>Server/RA DHCPv6**. Sotto quella pagina ci sono due schede: una per il **server DHCPv6** e una per gli **annunci del router**.

23.2.1 DHCPv6 vs autoconfigurazione dell'indirizzo senza stato

Ci sono alcuni client che non hanno il supporto per DHCPv6. Alcuni client supportano solo l'autoconfigurazione degli indirizzi senza stato (stateless Address Autoconfiguration), o SLAAC in breve. Non c'è modo per il firewall di avere conoscenza diretta di un elenco di host sul segmento utilizzando indirizzi SLAAC, quindi per alcuni ambienti è molto meno desiderabile a causa della mancanza di controllo e segnalazione di indirizzi. Considerare il monitoraggio degli

indirizzi e i requisiti di supporto del sistema operativo al momento di decidere come allocare gli indirizzi IPv6 ai client sulla rete.

Molti sistemi operativi come Windows, OS X, FreeBSD, Linux e i loro cugini contengono client DHCPv6 che sono in grado di ottenere indirizzi come previsto tramite DHCPv6. Alcuni sistemi operativi leggeri o mobili come Android non contengono un client DHCPv6 e funzioneranno solo su un segmento locale con IPv6 utilizzando SLAAC.

23.2.2 Annunci del router (o "dov'è l'opzione del gateway DHCPv6")

In IPv6, un router si trova attraverso i messaggi degli annunci del router (RA) inviati da router invece che da DHCP; router abilitati IPv6 che supportano l'assegnazione dell'indirizzo dinamico sono tenuti ad annunciare se stessi sulla rete a tutti i client. Come tale, DHCPv6 non include alcuna informazione gateway. Quindi i client possono ottenere i loro indirizzi da DHCPv6 o SLAAC, ma a meno che non siano configurati staticamente, individuano sempre il loro prossimo hop utilizzando i pacchetti RA inviati dai gateway disponibili.

Per abilitare il servizio RA:

- Passare a Servizi>Server/RA DHCPv6
- Fare clic sulla scheda Interfaccia per l'interfaccia configurata
- Fare clic sulla scheda **Annunci del router**
- Selezionare una modalità diversa da *disabilitata* dall'elenco a discesa della **Modalità del router**
- Fare clic su **Salvare**

Le altre opzioni per controllare il comportamento del RA possono essere impostate secondo necessità per la rete:

Modalità di annunci del router Le modalità per il demone RA controllano i servizi offerti da Firew4LL, annunciano il firewall come router IPv6 sulla rete e indirizzano i client su come ottenere gli indirizzi.

Disabilitato Il demone RA è disabilitato e non verrà eseguito. I gateway IPv6 devono essere inseriti manualmente su qualsiasi host client.

Solo router Questo firewall invierà pacchetti RA che si annunciano come un router IPv6. DHCPv6 è disabilitato in questa modalità.

Non gestito Il firewall invierà pacchetti RA e i client sono diretti ad assegnare loro stessi indirizzi IP all'interno della Subnet dell'interfaccia utilizzando SLAAC. DHCPv6 è disabilitato in questa modalità.

Gestito Il firewall invierà pacchetti RA e gli indirizzi saranno assegnati solo ai client che utilizzano DHCPv6.

Assistito Il firewall invierà pacchetti RA e gli indirizzi possono essere assegnati ai client da DHCPv6 o SLAAC.

DHCP senza stato Il firewall invierà pacchetti RA e gli indirizzi possono essere assegnati ai client da SLAAC fornendo informazioni aggiuntive come DNS e NTP da DHCPv6.

Priorità del router Se esistono più router IPv6 sullo stesso segmento di rete, possono indicare ai client in quale ordine devono essere utilizzati. Se un router ad elevata priorità non è disponibile, i client proveranno un router a priorità normale e, infine, un router a bassa priorità. Selezionare *Basso*, *Normale* o *Alto* dall'elenco. Se c'è solo un router sulla rete, utilizzare *Normale*.

Durata valida predefinita Periodo di tempo, specificato in secondi, in cui il prefisso annunciato sarà valido. Il valore predefinito è 86400 secondi (un giorno)

Durata preferita predefinita Periodo di tempo, specificato in secondi, in cui gli indirizzi client generati in questo prefisso utilizzando SLAAC sono validi. Il valore predefinito è 86400 secondi (un giorno)

Sottoreti RA Questa sezione consente di definire un elenco di sottoreti per i quali questo firewall invierà pacchetti RA. Immettere tutte le sottoreti necessarie, ognuna con un prefisso appropriato (in genere 64.).

Per creare una riga aggiuntiva per un'altra Subnet, fare clic su  Aggiungere.

Impostazioni DNS Ottenere informazioni DNS dai messaggi RA non è universalmente supportato, ma per i client che lo supportano, utilizzare SLAAC per fornire un indirizzo IP e DNS da RA può eliminare completamente la necessità di utilizzare DHCPv6.

Server DNS Immettere fino a tre indirizzi IP per i server DNS o lasciare vuoti i campi per utilizzare i server DNS predefiniti di sistema o il forwarder del DNS/Risolutore del DNS se abilitato.

Elenco dei domini di ricerca Funziona in modo identico all'opzione DHCP con lo stesso nome.

Utilizzare le stesse impostazioni del server DHCPv6 Quando selezionato, questi valori verranno estratti automaticamente dalle opzioni DHCPv6.

23.2.3 Range DHCPv6

Il parametro **Intervallo** funziona in modo simile alla stessa impostazione su IPv4, ma vale la pena menzionarlo di nuovo qui a causa delle differenze nell'indirizzamento IPv6.

Data la grande quantità di spazio disponibile all'interno di un /64, un buon trucco è creare un intervallo che limiti gli host a utilizzare un intervallo facile da ricordare o riconoscere. Ad esempio, all'interno di un /64 come 2001:db8:1:1::, impostare l'intervallo DHCPv6 in modo che sia: da 2001:db8:1:1::d:0000 a 2001:db8:1:1::d:FFFF, usando la D nel secondo all'ultima sezione dell'indirizzo come una sorta di stenografia per "DHCP". Tale intervallo di esempio contiene 2^16 (65,536) IP, che è estremamente grande per gli standard IPv4 di oggi, ma solo una piccola parte dell'intero /64.

23.2.4 Delega del prefisso DHCPv6

La delega del prefisso, coperto in precedenza in *Delega del prefisso DHCPv6* e *Tracciare l'interfaccia*, consente di dividere e allocare automaticamente un blocco di indirizzi IPv6 alle reti che vivranno dietro altri router e firewall che risiedono downstream di Firew4LL (ad esempio nella LAN, DMZ, ecc). La maggior parte degli utenti che agiscono in una capacità del client non ne avrà bisogno e probabilmente lo lascerà vuoto.

La delega del prefisso può essere utilizzata per distribuire automaticamente /64 blocchi di a /48 per i router o qualsiasi altra combinazione, purché l'intervallo sia impostato sui limiti della dimensione della delega desiderata. Il router downstream ottiene un indirizzo IPv6 e richiede una delega, e il server ne alloca uno e aggiunge dinamicamente un percorso in modo che sia raggiungibile tramite l'indirizzo DHCPv6 assegnato al client.

L**'intervallo di delega del prefisso** imposta l'inizio e la fine del pool di delega. L'intervallo di indirizzi IPv6 specificato qui deve essere indirizzato a questo firewall dal router upstream. Ad esempio, per allocare /60 reti al firewall downstream fuori da un determinato intervallo, è possibile specificare da 2001:db8:1111:F000:: a 2001:db8:1111:FF00:: con una dimensione di delega del prefisso di 60. Questo assegna un /60 (16 sottoreti di dimensione /64) a ciascun firewall downstream che richiede una delega in modo che possano a loro volta utilizzare quelli per LAN, VPN, DMZ, ecc. I firewall downstream possono anche delegare ulteriormente la propria allease ai router dietro di loro. Si noti che in questo esempio, 16 delegazioni sarebbero possibili. Regolare l'intervallo e le dimensioni, se necessario.

Quando si creano i valori per l'intervallo e la dimensione della delega, tenere presente che l'intervallo deve iniziare e terminare sui confini che si allineano con la dimensione del prefisso desiderata. In questo esempio /60, l'intervallo non può iniziare o terminare su qualsiasi cosa che abbia un valore nei punti a destra del secondo valore nella quarta sezione dell'indirizzo, quindi può iniziare su 2001:db8:1111:F500:: ma **non** 2001:db8:1111:F550::.

23.2.5 Mappature statiche DHCPv6

Le mappature statiche su DHCPv6 funzionano in modo diverso rispetto a IPv4. Su IPv4, le mappature sono state eseguite utilizzando l'indirizzo MAC del PC. Per IPv6, i progettisti hanno deciso che non era abbastanza buono, dal momento che l'indirizzo MAC di un PC potrebbe cambiare, ma comunque essere lo stesso PC.

Immettere, l'**identificatore univoco DHCP** o **DUID**. Il DUID dell'host viene generato dal sistema operativo del client e, in teoria, rimarrà unico per quell'host specifico fino a quando l'utente non costringe un nuovo DUID o il sistema operativo viene reinstallato. Il DUID può variare da 20 byte e varia a seconda del tipo.

Il campo **DUID** nella pagina di mappatura statica prevede un DUID per un PC client in un formato speciale, rappresentato da coppie di cifre esadecimali, separate da due punti, come 00:01:00:01:1b:a6:e7:ab:00:26:18:1a:86:21.

Come ottenere questo DUID dipende dal sistema operativo. Il modo più semplice è consentire al PC di ottenere un lease tramite DHCPv6, quindi aggiungere una voce dalla Vista delle lease DHCPv6 (lease DHCPv6 di stato). In Windows, può essere trovato come DUID del client di DHCPv6 nell'output di ipconfig /all..

Nota: su Windows, il DUID viene generato al momento dell'installazione, quindi se viene utilizzata un'immagine di base e le workstation vengono clonate da lì, possono finire con lo stesso DUID, e quindi tutti finiscono per tirare lo stesso indirizzo IPv6 su DHCPv6.

Deselezionare il DUID dal registro di sistema prima di creare un'immagine da clonare, emettendo il seguente comando:

reg delete HKLMSYSTEMCurrentControlSetServicesTcpip6Parameters /f /v Dhcpv6DUID

Tale comando può anche essere eseguito su un sistema di lavoro per reimpostare il suo DUID, se necessario.

23.3 Relay di DHCP e DHCPv6

Le richieste DHCP sono traffico broadcast. Il traffico broadcast è limitato al dominio broadcast in cui viene avviato. Per fornire il servizio DHCP su un segmento di rete senza un server DHCP, utilizzare il relay DHCP per inoltrare tali richieste a un server definito su un altro segmento.

Per configurare il relay DHCP: - Disabilitare il server DHCP su ogni interfaccia - Passare a **Servizi>Relay DHCP** - Fare clic sulla scheda per l'interfaccia da utilizzare con relay DHCP - Configurare le opzioni come segue:

> **Abilitare il relay DHCP** Selezionato
>
> **Aggiungere un ID del circuito e un ID agente alle richieste** Selezionare questo per aggiungere un ID del circuito (numero dell'interfaccia Firew4LL) e l'ID agente alla richiesta DHCP. Questo può essere richiesto dal server DHCP sull'altra parte e può aiutare a distinguere dove sono originate le richieste.
>
> **Server di destinazione** Una casella di immissione manuale per impostare il server DHCP di destinazione

- Fare clic su **Salvare**

La funzione relay di DHCPv6 funziona in modo identico alla funzione relay di DHCP per IPv4.

23.4 Risolutore DNS

Il risolutore del DNS in Firew4LL utilizza unbound, che è un risolutore DNS di convalida, ricorsivo e che utilizza la cache che supporta DNSSEC e un'ampia varietà di opzioni. Il Resolver DNS è abilitato di default nelle versioni correnti di Firew4LL.

Per impostazione predefinita, il risolutore del DNS interroga direttamente i server DNS della root e non utilizza server DNS configurati in **Sistema>Configurazione generale** o quelli ottenuti automaticamente da una WAN dinamica. Questo comportamento può essere modificato, comunque, utilizzando l'opzione di inoltro delle Query del DNS. Contattando la root direttamente per impostazione predefinita, elimina molti problemi tipicamente riscontrati dagli utenti con configurazioni DNS locali errate e i risultati DNS sono più affidabili e verificabili con le estensioni di sicurezza del sistema dei nomi di dominio (Domain Name System Security Extensions, DNSSEC).

23.4.1 Opzioni avanzate del risolutore DNS

Firew4LL fornisce una GUI per configurare alcune delle opzioni avanzate più comuni disponibili in unbound. Le opzioni di seguito sono documentate come trovate nella pagina principale di unbound.conf.

Nascondere identità Quando impostato, i tentativi di interrogare l'identità del server (id.server e nomehost.bind) sono rifiutati.

Nascondere versione Quando impostato, i tentativi di interrogare la versione del server (version.server e version.bind) sono rifiutati.

Prefetch del supporto Quando abilitato, gli elementi della cache dei messaggi vengono prefetchati prima della scadenza per mantenere aggiornata la cache. Questa opzione può causare un aumento di circa il 10% in più di traffico DNS e del carico sul server, ma gli elementi richiesti di frequente non scadono dalla cache.

Prefetch del supporto della chiave DNS Quando abilitato, le chiavi DNS vengono recuperate in precedenza nel processo di convalida quando viene rilevato un record del firmatario della delega. Questo aiuta a ridurre la latenza delle richieste ma utilizza un po' più di CPU e richiede che la cache sia impostata sopra lo zero.

Indurire i dati DNSSEC Se questa opzione è disabilitata e non vengono ricevuti dati DNSSEC, la zona viene resa insicura. I dati DNSSEC sono necessari per le zone ancorate alla fiducia. Se tali dati sono assenti, la zona diventa falsa.

Dimensione della cache per i messaggi La cache dei messaggi memorizza i codici di risposta DNS e gli stati di convalida. La cache RRset (Set di record di risorse, resources record set) verrà automaticamente impostata su due volte tale importo. La cache RRset contiene i dati effettivi del record di risorse. Il valore predefinito è *4 MB*.

Buffer del TCP in uscita Il numero di buffer del TCP in uscita da allocare per filo. Il valore predefinito è *10*. Se impostato su *0*, le query TCP non verranno inviate a server autorevoli.

Buffer TCP in entrata Il numero di buffer del TCP in entrata da allocare per filo. Il valore predefinito è *10*. Se impostato su *0*, le query TCP non verranno accettate da server autorevoli.

Dimensione del buffer EDNS Numero di byte da annunciare come dimensione del buffer di riassemblaggio EDNS. Questo valore viene inserito nei datagrammi UDP inviati ai peer. La raccomandazione per RFC è *4096* (il valore predefinito). Se si verificano problemi di riassemblaggio della frammentazione, di solito osservati come timeout, può essere d'aiuto un valore di *1480*. Il valore *512* ignora la maggior parte dei problemi di percorso MTU, ma è eccessivo e può generare una quantità eccessiva di fallback del TCP.

Numero di query per filo Il numero di query che ogni filo servirà contemporaneamente. Se arrivano ulteriori query che devono essere servite e nessuna query può essere spintonata, le nuove query vengono eliminate

Spingere il timeout Timeout utilizzato quando il server è molto occupato. Questo protegge dalla negazione del servizio attraverso query lente o alti tassi di query. Il valore predefinito è *200* millisecondi. Impostare un valore che approssima il tempo di andata e ritorno ai server dell'autorità. Quando arrivano nuove query, il 50% può essere eseguito e il 50% viene sostituito da nuove query se sono più vecchie del timeout dichiarato.

TTL massimo per RRset e messaggi Il tempo massimo di vita (TTL) per RRset e messaggi nella cache, specificato in secondi. Il valore predefinito è 86400 secondi (1 giorno). Quando il TTL interno scade l'elemento cache è scaduto. Questo può essere configurato per forzare il risolutore a interrogare i dati più spesso e non fidarsi dei valori TTL (molto grandi)

TTL minimo per RRset e messaggi Il tempo minimo di vita per RRset e messaggi nella cache, specificato in secondi. Il valore predefinito è 0 secondi. Se un record ha un TTL inferiore al valore minimo configurato, i dati possono essere memorizzati nella cache più a lungo del proprietario del dominio previsto e quindi vengono effettuate meno query per cercare i dati. Il valore 0 garantisce che i dati nella cache non vengano mantenuti più a lungo del proprietario del dominio previsto. Valori elevati possono causare problemi in quanto i dati nella cache potrebbero non corrispondere ai dati effettivi se cambiano.

TTL per le voci della cache dell'host Tempo di vita, in secondi, per le voci nella cache dell'host dell'infrastruttura. La cache dell'host dell'infrastruttura contiene i tempi di andata e ritorno, le inadeguatezze e le informazioni di supporto EDNS per i server DNS. Il valore predefinito è *15 minuti*.

Numero di host da memorizzare nella cache Numero di host dell'infrastruttura per i quali le informazioni sono memorizzate nella cache. Il valore predefinito è *10,000*.

Soglia di risposta indesiderata Se abilitato, un numero totale di risposte indesiderate viene tracciato in ogni filo. Quando viene raggiunta la soglia, viene eseguita un'azione difensiva e viene stampato un avviso sul file di registro. L'azione difensiva è quella di cancellare le cache RRset e dei messagi, sperando di eliminare qualsiasi veleno. Il valore predefinito è disabilitato, ma se abilitato viene suggerito un valore di 10 milioni.

Livello Di Registro Selezionare la verbosità del registro. Il valore predefinito è il *livello 1*.

> **Livello 0** Nessuna verbosità, solo errori. **Livello 1** Informazioni operative. **Livello 2** Informazioni operative dettagliate. **Livello 3** Informazioni sul livello di query, output per query. **Livello 4** Informazioni a livello dell'algoritmo. **Livello 5** Registra l'identificazione del client per errori di cache.

Disabilitare il controllo di accesso aggiunto automaticamente Disabilita le voci di controllo degli accessi aggiunte automaticamente. Per default, sono consentite reti IPv4 e IPv6 che risiedono su interfacce interne di questo firewall. Le reti consentite devono essere configurate manualmente nella scheda **Elenchi di accesso** se selezionata.

Supporto a 0x20 bit sperimentale Utilizzare bit casuali codificati 0x20 nella query DNS per sventare i tentativi di spoofing. Vedere le implementazione progetto dns-0x20 per ulteriori informazioni.

23.4.2 DNS Resolver liste di accesso

Unbound richiede elenchi di accesso (ACL) per controllare quali client sono autorizzati a inviare query. Per impostazione predefinita, le reti IPv4 e IPv6 che risiedono su interfacce interne di questo firewall sono consentite. Le reti aggiuntive devono essere consentite manualmente.

Nota: Gli ACL automatici possono essere disabilitati utilizzando l'opzione **Disattivare il controllo dell'accesso automaticamente aggiunto** nella scheda **Impostazioni avanzate**.

Per gestire gli elenchi di accesso per il risolutore del DNS, passare a **Servizi>Risolutore del DNS**, scheda **Elenchi di accesso**. Da questo elenco possono essere aggiunte nuove voci e le voci esistenti possono essere modificate o cancellate.

Quando si aggiunge o si modifica una voce, sono disponibili le seguenti opzioni:

> **Nome della lista di accesso** Il nome dell'elenco di accesso, che viene visualizzato come commento nel file di configurazione dell'elenco di accesso.

Azione Metodo di gestione delle reti contenute in questo elenco di accesso

Negare Arresta le query dai client nelle reti configurate

Rifiutare Arresta le query dai client nelle reti configurate e invia un codice di risposta come RIFIUTATO

Consentire Consente le query dai client nelle reti configurate

Consentire lo snoop Consente query ricorsive e non ricorsive dai client nelle reti configurate, utilizzate per lo snooping della cache e in genere configurate solo su host amministrativi.

Descrizione Un campo di testo più lungo per le note di riferimento su questa voce.

Reti Un elenco di reti da governare con questa voce di elenco di accesso.

23.4.3 DNS Resolver e IPv6

Il risolutore del DNS è pienamente compatibile con IPv6. Accetta e fa query su IPv6, supporta i record AAAA e non ha problemi noti con alcun aspetto di IPv6 e gestione DNS.

23.4.4 Configurazione del risolutore del DNS

Per configurare il risolutore del DNS, passare a **Servizi>Risolutore del DNS**

Abilitare Selezionare questa casella per attivare il risolutore del DNS o deselezionare per disabilitare questa funzionalità. Il forwarder del DNS e il risolutore del DNS non possono essere entrambi attivi contemporaneamente sulla stessa porta, quindi disabilitare il forwarder del DNS o spostare un servizio o l'altro su una porta diversa prima di tentare di abilitare il risolutore del DNS.

Porta in ascolto Per impostazione predefinita, il risolutore del DNS ascolta sulla porta TCP e UDP 53. Questo è normale per qualsiasi server DNS, in quanto è la porta che il client cercherà di utilizzare. Ci sono alcuni casi in cui è desiderabile spostare il risolutore del DNS su un'altra porta di ascolto, come 5353 o 54, quindi è possibile inoltrare fonti specifiche tramite la porta forward.

Interfacce Per impostazione predefinita, il risolutore del DNS ascolta su ogni interfaccia disponibile e indirizzo IPv4 e IPv6. Il controllo dell'interfaccia limita le interfacce in cui il forwarder del DNS accetterà e risponderà alle query. Questo può essere utilizzato per aumentare la sicurezza oltre alle regole del firewall. Se è selezionata un'interfaccia specifica, gli indirizzi IPv4 e IPv6 su tale interfaccia verranno utilizzati per rispondere alle query. Il demone unbound si legherà solo all'interfaccia selezionata. Le query inviate ad altri indirizzi IP sul firewall verranno scartate silenziosamente.

Interfacce di rete in uscita Per impostazione predefinita, il risolutore del DNS utilizza tutte le interfacce per le query in uscita, quindi genererà la query da qualsiasi interfaccia e indirizzo IP sia più vicino al server di destinazione da una prospettiva di routing. La selezione di interfacce specifiche limiterà le scelte solo a interfacce specifiche che possono essere utilizzate come fonte di query.

Tipo di zona locale del dominio di sistema Questa opzione determina il tipo di zona locale configurata in unbound per il dominio di sistema. Il tipo di zona regola il tipo di risposta da dare ai client quando non c'è corrispondenza nei dati locali come le sovrascritture degli host, gli host DHCP, ecc. In ogni caso, se c'è una corrispondenza locale, la query viene risolta normalmente. I tipi disponibili per governare le risposte non corrispondenti sono:

Negare Elimina la query e non risponde al client.

Rifiutare Notifica al client che la query è stata rifiutata (utilizzando rcode RIFIUTATO).

Statico Restituisce una risposta NESSUNDATO o NXDOMAIN al client.

Trasparente Questo è il comportamento predefinito. Se la query è per un nome che non esiste localmente, viene risolta come al solito. Se il nome ha una corrispondenza locale ma il tipo è diverso, una risposta NESSUNERRORE, NESSUNDATO viene inviata al client

Tipo Trasparente Analogo a trasparente, passa anche le query in cui il nome corrisponde ma il tipo no. Ad esempio, se un client esegue una query per un record AAAA ma esiste solo un record A, la query AAAA viene trasmessa anziché ricevere una risposta negativa.

Reindirizzare Gestisce le query dai dati locali e reindirizza le query per le zone sotto la zona locale (ad esempio sottodomini). Questo può essere utilizzato per controllare le query per tutti i sottodomini sotto il dominio specificato.

Informare Risponde normalmente, ma registra la query del client.

Negare e informare Nega e registra la query.

Nessun valore predefinito Disabilita qualsiasi contenuto predefinito per la zona senza influire sul comportamento delle query.

DNSSEC Abilita le estensioni della sicurezza di sistema per il nome del dominio (Domain Name System Security Extensions, DNSSEC), che consente ai client di fidarsi della sorgente e del contenuto delle risposte DNS. Questo è abilitato per impostazione predefinita. DNSSEC protegge dalla manipolazione delle risposte DNS, come l'avvelenamento della cache DNS o altre intercettazioni di query, ma non rende segreto il contenuto delle risposte. DNSSEC funziona meglio quando si utilizzano direttamente i server root, a meno che i server di inoltro supportino DNSSEC. Se i server DNS upstream non supportano DNSSEC in modalità di inoltro o con sovrascritture di dominio, se è noto che le query DNS vengono intercettate upstream o che i client presentano problemi con risposte DNS di dimensioni eccessive, potrebbe essere necessario disabilitare DNSSEC.

Inoltro di query del DNS Disabilitato per impostazione predefinita. Se abilitato, unbound utilizzerà i server DNS di sistema da **Sistema>Configurazione generale** o quelli ricevuti da una WAN dinamica, piuttosto che usare direttamente i server root. Questo è meglio per uno scenario Multi-WAN in cui è desiderato un controllo accurato del routing delle query DNS, ma in genere richiede anche la disabilitazione di DNSSEC a causa della mancanza di supporto da parte dei server DNS upstream o di altri problemi che inoltrano le query.

Registrazione DHCP Quando è attivo, i nomi delle macchine interne per i client DHCP possono essere risolti utilizzando il DNS. Funziona solo per i client che specificano un hostname nelle loro richieste DHCP. Il nome di dominio da **Sistema>Configurazione generale** viene utilizzato come nome di dominio sugli host.

DHCP statico Funziona come **Registrare le lease DHCP nel forwarder del DNS**, tranne che registra invece gli indirizzi di mappatura statica DHCP.

Opzioni personalizzate Un'area di testo per l'immissione di direttive avanzate per unbound che non sono supportate direttamente dalla GUI. Se unbound non si avvia correttamente dopo aver inserito le opzioni personalizzate, Aggiungere server: su una riga prima delle opzioni personalizzate.

Sovrascritture Host

Le voci DNS personalizzate possono essere create nella sezione **sovrascritture host** della pagina. Le sovrascritture host possono definire nuovi record o sovrascrivere i record esistenti in modo che i client locali ricevano le risposte configurate anziché le risposte dai server DNS upstream. Questo è utile anche per le configurazioni del DNS diviso (vedi *DNS diviso*) e come mezzo semi-efficace per bloccare l'accesso a determinati siti web specifici.

È possibile definire più record per lo stesso hostname e tutti gli indirizzi IP verranno restituiti nel risultato. Questo può essere utilizzato per fornire sia un risultato IPv4 (A) che IPv6 (AAAA) per un singolo hostname.

Nota: Non è consigliabile utilizzare solo la funzionalità di override del DNS come mezzo per bloccare l'accesso a determinati siti. Ci sono innumerevoli modi per aggirare questo. Fermerà gli utenti non tecnici, ma è facile da aggirare per quelli con più attitudine tecnica.

Host Questo campo definisce solo la parte del hostname del record DNS (senza il dominio), ad esempio www.. Può essere lasciato vuoto per creare un record di override per il dominio stesso (simile a un record "@" in un legame.)

Dominio Questo campo è obbligatorio e definisce il nome di dominio per la voce override, ad es. esempio.com.

Indirizzo IP L'indirizzo IP (IPv4 o IPv6) da restituire come risultato per una ricerca DNS di questa voce.

Descrizione Una descrizione di testo utilizzata per identificare o fornire ulteriori informazioni su questa voce.

Nome aggiuntivo per questo host Definisce i nomi host aggiuntivi per lo stesso indirizzo IP (proprio come i record CNAME) per mantenerli in una singola voce di override.

Sovrascritture di dominio

Le sovrascritture di dominio si trovano nella parte inferiore della pagina del risolutore del DNS. Queste voci specificano un server DNS alternativo da utilizzare per risolvere un dominio specifico.

Un esempio di dove questo è comunemente distribuito è nelle reti di piccole imprese con un singolo server interno con Active Directory, di solito il Server per piccoli business di Microsoft (Microsoft Small Business Server). Le richieste DNS per il nome di dominio di Active Directory devono essere risolte dal server Windows interno affinché Active Directory funzioni correttamente. L'aggiunta di un override per il dominio di Active Directory che punta all'indirizzo IP interno di Windows server assicura che questi record siano risolti correttamente se i client utilizzano questo firewall come server DNS o il server Windows direttamente.

In un ambiente Active Directory, la migliore pratica è quella di far sì che i client utilizzino sempre il server DNS di Windows come server DNS primario, in modo che la registrazione dinamica dei nomi e altre attività DNS correlate al dominio funzionino correttamente. In ambienti con un solo server DNS di Windows, abilitare il risolutore del DNS con un override per il dominio Active Directory e utilizzare questo firewall come server DNS secondario per le macchine interne. Ciò garantisce che la risoluzione DNS (ad eccezione di Active Directory) non abbia un singolo punto di errore e che la perdita del singolo server non significhi un'interruzione completa di Internet. La perdita di un singolo server in un tale ambiente di solito avrà conseguenze significative, ma gli utenti saranno più inclini a lasciare l'amministratore da solo per risolvere il problema se possono ancora controllare i loro Facebook, Twitter, e tutti gli altri nel frattempo.

Un altro uso comune delle sovrascritture DNS è quello di risolvere i domini DNS interni in siti remoti utilizzando un server DNS nel sito principale accessibile tramite VPN. In tali ambienti tutte le query DNS vengono in genere risolte nel sito centrale per il controllo centralizzato sul DNS, tuttavia alcune organizzazioni preferiscono consentire la risoluzione DNS di Internet con Firew4LL in ciascun sito e inoltrare solo le query per i domini interni al server DNS centrale.

Nota: per funzionare su IPsec è necessario un percorso statico. Per

ulteriori informazioni, vedere *Traffico avviato da \firew4ll\ e IPsec*.

Dominio Il campo del dominio imposta il nome di dominio che verrà risolto utilizzando questa voce. Questo non deve essere un TLD valido, può essere qualsiasi cosa (ad esempio locale, test, lab), o può essere un vero nome di dominio (esempio.com).

Indirizzo IP Specifica l'indirizzo IP del server DNS a cui vengono inviate le query per i nomi host nel dominio. Se il server DNS di destinazione è in esecuzione su una porta diversa da 53, aggiungere il numero di porta dopo l'indirizzo IP con un @ che separa i valori, ad esempio:

```
192.0.2.3@5353
```

Descrizione Una descrizione di testo utilizzata per identificare o fornire ulteriori informazioni su questa voce.

23.4.5 Il risolutore del DNS e Multi-WAN

Con le impostazioni predefinite, il risolutore DNS avrà problemi in un ambiente Multi-WAN. Il problema principale è che il risolutore DNS vuole interrogare direttamente i server DNS della root. Queste query verranno inviate solo utilizzando il gateway predefinito. Se la WAN contenente il gateway predefinito fallisce, è probabile che anche le query DNS falliscano. Tuttavia, ci sono modi per aggirare questa limitazione:

Modalità di inoltro

Abilitare l'inoltro delle query DNS e configurare almeno un server DNS per gateway della WAN in **Sistema>Configurazione generale**. Potrebbe anche essere necessario disabilitare DNSSEC, a seconda del supporto del server DNS upstream.

Commutazione predefinita del gateway

Abilitare la **Commutazione predefinita del gateway** sotto **Sistema>Avanzate**, nella scheda **Varie**. Questo sposterà il gateway predefinito al prossimo gateway disponibile se il default preferito fallisce. Tuttavia, questa opzione è ancora considerata sperimentale e può avere problemi in alcuni casi.

23.4.6 Il risolutore del DNS Resolver e la protezione del rebinding del DNS

Per impostazione predefinita, la protezione del rebinding del DNS è abilitata e le risposte agli indirizzi IP privati vengono rifiutate. Per consentire le risposte degli indirizzi IP privati da un dominio noto, utilizzare la casella delle **Opzioni personalizzate** nelle impostazioni del risolutore DNS per configurare i domini consentiti come segue:

server: private-domain: «example.com»

23.5 Il DNS Forward

Il forwarder DNS in Firew4LL è un risolutore DNS che memorizza nella cache che utilizza il demone dnsmasq. È disabilitato per impostazione predefinita nelle versioni correnti, con il *Risolutore del DNS* (unbound) attivo per impostazione predefinita. Il forwarder DNS rimarrà abilitato su sistemi più vecchi o sistemi aggiornati in cui era attivo in precedenza.

Il forwarder DNS utilizza server DNS configurati in **Sistema>Configurazione generale** o quelli ottenuti automaticamente da un ISP per interfacce WAN configurate dinamicamente (DHCP, PPPoE, PPTP). Per le connessioni WAN degli indirizzi IP statici, i server DNS devono essere inseriti in **Sistema>Configurazione generale** o durante la procedura guidata di configurazione per il funzionamento del forwarder DNS. I server DNS configurati staticamente possono essere utilizzati anche con interfacce WAN configurate dinamicamente **Consentire che l'elenco dei server DNS sia sovrascritto da DHCP/PPP** nella casella WAN nella pagina **Sistema>Configurazione generale**.

Per impostazione predefinita, lo forwarder DNS interroga tutti i server DNS contemporaneamente e viene utilizzata e memorizzata nella cache l'unica risposta ricevuta. Ciò si traduce in un servizio DNS molto più veloce dal punto di vista del client e può aiutare a risolvere i problemi derivanti da server DNS che sono intermittenti lenti o hanno un'elevata latenza, specialmente in ambienti Multi-WAN. Questo comportamento può essere disabilitato attivando l'opzione **Interrogare i server DNS in sequenza**.

23.5.1 Il forwarder DNS e IPv6

Il forwarder DNS è pienamente compatibile con IPv6. Accetta e fa interrogazioni su IPv6, supporta i record AAAA e non ha problemi noti con alcun aspetto di IPv6 e gestione DNS.

23.5.2 Configurazione del forwarder del DNS

Per configurare il forwarder DNS, passare a **Servizi> Forwarder DNS**

Le opzioni disponibili per il forwarder DNS sono:

Abilitare Selezionare questa casella si attiva il forwarder DNS o deselezionarla per disabilitare questa funzionalità. Il forwarder DNS e il risolutore DNS non possono essere entrambi attivi contemporaneamente sulla stessa porta, quindi disabilitare il risolutore DNS o spostare un servizio o l'altro su una porta diversa prima di tentare di abilitare il forwarder DNS.

Registrazione di DHCP Quando è attivo, i nomi delle macchine interne per i client DHCP possono essere risolti utilizzando DNS. Funziona solo per i client che specificano un hostname nelle loro richieste DHCP. Il nome di dominio da **Sistema>Configurazione generale** viene utilizzato come nome di dominio sugli host.

DHCP statico Funziona come **Registrare lease DHCP nel forwarder DNS**, tranne che registra invece gli indirizzi di mappatura statica DHCP.

Prefererire DHCP Quando un indirizzo IP ha più nomi host, fare una ricerca inversa può dare un risultato non protetto se uno dei nomi host è tra le sovrascritture di host e il sistema utilizza un altro hostname su DHCP. Selezionando questa opzione verranno posizionati i nomi host ottenuti da DHCP sopra le mappature statiche nel file degli host sul firewall, facendoli prima consultare. Ciò influisce solo sulle ricerche inverse (PTR), poiché restituiscono solo il primo risultato e non di più. Ad esempio, ciò produrrebbe un risultato come labserver01.example.com, il DHCP di un server di prova ha ottenuto l'indirizzo IP, piuttosto che un nome di override host come testwww.example.com che sarebbe stato restituito altrimenti.

Interrogare i server DNS in sequenza Per impostazione predefinita, il firewall interroga tutti i server DNS contemporaneamente e utilizza il risultato più veloce. Questo non è sempre desiderabile, specialmente se esiste un server DNS locale con nomi host personalizzati che potrebbero essere aggirati utilizzando un server DNS più veloce ma pubblico. Selezionando questa opzione, le query vengono eseguite su ciascun server DNS in sequenza dall'alto verso il basso e il firewall attende un timeout prima di passare al server DNS successivo nell'elenco.

Richiedere il dominio Richiede che un nome di dominio sui nomi host venga inoltrato ai server DNS di upstream. Gli host senza nome verranno comunque controllati rispetto alle sovrascritture host e ai risultati DHCP, ma non verranno interrogati sui nomi del server configurati sul firewall. Invece, se un hostname breve non esiste localmente, un risultato NXDOMAIN ("non trovato") viene restituito al client.

Non inoltrare ricerche inverse private Se selezionata, questa opzione impedisce a dnsmasq di effettuare ricerche DNS inverse (Record PTR) per gli indirizzi IP privati RFC1918 sui nomi del server upstream. Restituirà comunque i risultati dalle voci locali. È possibile utilizzare una voce di override del dominio per la zona di ricerca inversa, ad esempio 1.168.192 .in-addr.arpa, in modo che le query per una Subnet specifica saranno ancora inviate a un server DNS specifico.

Porta in ascolto Per impostazione predefinita, il forwarder DNS ascolta sulla porta TCP e UDP 53. Questo è normale per qualsiasi server DNS, in quanto è la porta che il client cercherà di utilizzare. Ci sono alcuni casi in cui è desiderabile spostare il forwarder del DNS su un'altra porta di ascolto, come 5353 o 54, quindi è possibile inoltrare query specifiche tramite la porta forward.

Interfacce Per impostazione predefinita, il forwarder del DNS ascolta su ogni interfaccia disponibile e tutti gli indirizzi IPv4 e IPv6 disponibili. Il controllo dell'interfaccia limita le interfacce in cui il forwarder DNS accetterà e risponderà alle query. Questo può essere utilizzato per aumentare la sicurezza oltre alle

regole del firewall. Se è selezionata un'interfaccia specifica, gli indirizzi IPv4 e IPv6 su tale interfaccia verranno utilizzati per rispondere alle query. Le query inviate ad altri indirizzi IP sul firewall verranno scartate silenziosamente.

Binding rigoroso dell'interfaccia Quando è impostato, il forwarder DNS si legherà solo alle interfacce contenenti gli indirizzi IP selezionati nel controllo dell'interfaccia, piuttosto che collegarsi a tutte le interfacce e scartare le query ad altri indirizzi. Questo può essere utilizzato in modo simile alla porta di ascolto per controllare il modo in cui il servizio si lega in modo che possa coesistere con altri servizi DNS con opzioni simili.

Nota: Questa opzione non è compatibile con IPv6 nella versione corrente del demone del forwarderDNS Forwarder, dnsmasq. Se questa opzione è selezionata, il processo dnsmasq non verrà associato a nessun indirizzo IPv6.

Opzioni avanzate

I parametri di configurazione dnsmasq personalizzati che non sono configurabili nella GUI possono essere inseriti in **Opzioni avanzate**. Ad esempio, per impostare un TTL inferiore per i record DNS, immettere max-ttl=30. Oppure crea un record DNS wild card da risolvere .lab.example.com to 192.2.5.6 specificando address=/lab.example.com/192.2.5.6.

I comandi devono essere separati da uno spazio o da una nuova riga. Per ulteriori informazioni sui possibili parametri che possono essere utilizzati, consultare la documentazione dnsmasq.

Sovrascrittura degli host

Le voci di override dell'host forniscono un mezzo per configurare le voci DNS personalizzate. La configurazione è identica alle *Sovrascritture dell'host* nel risolutore DNS, usarlo come riferimento per i dettagli.

Sovrascrittura dei domini

Le sovrascritture di dominio configurano un server DNS alternativo da utilizzare per risolvere un dominio specifico. La configurazione è identica alle sovrascritture di dominio nel risolutore DNS, con alcune leggere differenze:

Dominio Il campo del dominio imposta il nome di dominio che verrà risolto utilizzando questa voce. Questo non deve essere un TLD valido, può essere qualsiasi cosa (ad esempio locale, test, lab), o può essere un vero nome di dominio (esempio.com).

Indirizzo IP Questo campo può essere utilizzato in uno di questi tre modi. Innanzitutto, può essere utilizzato per specificare l'indirizzo IP del server DNS a cui vengono inviate le query per i nomi host nel dominio. In secondo luogo, può essere utilizzato per sovrascrivere un'altra voce inserendo #. Ad esempio, per inoltrare example.com a 192.2.66.2, ma avere lab.example.com inoltrato ai nomi del server standard, inserire un # in questo campo. In terzo luogo, può essere utilizzato per evitare ricerche non locali inserendo un !. Se esistono voci di override host per www.example.org e mail.example.org, ma altre ricerche per gli host sotto *example.org* non devono essere inoltrate ai server DNS remoti, immettere un ! in questo campo.

IP di sorgente Questo campo è facoltativo e viene utilizzato principalmente per contattare un server DNS attraverso una VPN. In genere solo specifici indirizzi IP locali sono in grado di attraversare una VPN, questo campo specifica quale indirizzo IP sul firewall viene utilizzato per l'a sorgente del DNS in modo che le query passino correttamente.

Descrizione Una descrizione di testo utilizzata per identificare o fornire ulteriori informazioni su questa voce.

23.5.3 Forwarder DNS e Multi-WAN

Il forwarder DNS è pienamente compatibile con Multi-WAN. Configurare almeno un server DNS per il gateway WAN in Sistema>Configurazione generale.

23.5.4 Forwarder DNS e protezione con il rebinding del DNS

Per impostazione predefinita, la protezione con il rebinding del DNS è abilitata e le risposte agli indirizzi IP privati vengono rifiutate. Per consentire le risposte degli indirizzi IP privati da un dominio noto, utilizzare la casella **Opzioni avanzate** nelle impostazioni del forwarder DNS per configurare i domini consentiti come segue:

rebind-domain-ok=/example.com/

23.6 DNS dinamico

Il client del DNS dinamico integrato in Firew4LL registra l'indirizzo IP di un'interfaccia WAN con una varietà di fornitori di servizi DNS dinamici. Questo viene utilizzato per accedere in remoto ai servizi su host che dispongono di WAN con indirizzi IP dinamici, più comunemente VPN, server web e così via.

Qualsiasi numero di client DNS dinamici può essere configurato utilizzando uno qualsiasi degli oltre 20 diversi fornitori di DNS dinamici o anche fornitori di DNS dinamici personalizzati. I client dei DNS dinamici possono utilizzare qualsiasi WAN e possono persino registrare l'indirizzo IP pubblico reale in ambienti in cui il firewall riceve un indirizzo IP privato per la sua WAN ed è upstream.

Oltre ai tipici provider di DNS dinamici basati su HTTP/HTTPS, Firew4LL supporta anche gli aggiornamenti di DNS dinamici in stile RFC 2136 direttamente sui server DNS.

23.6.1 DNS dinamico e IPv6

Al momento della stesura di questo documento, ci sono pochissimi provider di DNS dinamici che offrono supporto IPv6. Le scelte disponibili sono limitate a HE.net quando ospitano DNS per un dominio, tipi personalizzati e server RFC 2136.

Configurazione di un client del DNS dinamico

Firew4LL consente la registrazione con molti diversi provider di DNS dinamici. I provider disponibili possono essere visualizzati facendo clic sul selettore del **Tipo di servizio**. Ulteriori informazioni sui fornitori possono essere trovate cercando il loro nome per trovare il loro sito web. Diversi offrono un servizio di livello base senza alcun costo, e alcuni offrono servizi premium aggiuntivi ad un costo. C'è anche un'opzione personalizzata che consente a un URL *personalizzato* di ospitare un provider non supportato.

Selezionare un provider, visitare il loro sito web, registrarsi per un account e impostare un hostname. Le procedure variano con ogni fornitore, ma tutti hanno istruzioni sui loro siti web. Dopo aver configurato un hostname con un provider, configurare Firew4LL con le impostazioni corrispondenti.

La maggior parte dei fornitori hanno le stesse opzioni o simili. Ci sono alcuni tipi con opzioni personalizzate che saranno coperti più avanti in questa sezione.

Per configurare un client DNS dinamico:

- Passare a **Servizi>DNS dinamico**
- Fare clic su  **Aggiungere** per aggiungere una nuova voce
- Configurare le opzioni come segue:

  Disabilitare Selezionare per disabilitare la voce, o lasciare deselezionato in modo che sia attivo.

  Tipo di servizio Selezionare il provider DNS dinamico qui.

  Interfaccia da monitorare Selezionare l'interfaccia che dispone dell'indirizzo IP da tenere aggiornato, ad esempio WAN o un'interfaccia OPTx. La selezione di un gruppo di gateway per l'interfaccia consente alla voce DNS dinamica di passare la WAN in modo che possa consentire il failover Multi-WAN in entrata dei servizi su questo hostname.

  Hostname Immettere l'hostname creato presso il provider DNS dinamico. Questo è in genere il nome di dominio completo qualificato, come ad esempio myhost.example.com, eccetto per Namecheap dove questa è solo la parte host dell'indirizzo.

  Nome di dominio Per gli host di Namecheap, questa casella deve essere impostata sulla parte di dominio del hostname completo.

  MX Un record MX (scambiatore di posta, mail Exchanger) è il modo in cui i server di posta Internet sanno dove consegnare la posta per un dominio. Alcuni provider DNS dinamici consentono di configurare i record MX tramite il client del DNS dinamico. Se il provider scelto lo consente, immettere l'hostname del server di posta che riceverà posta Internet per il dominio DNS dinamico.

  Wildcard Quando il DNS wildcard è abilitato su un nome DNS dinamico, tutte le query dei nomi host sotto il dominio specificato si risolveranno all'indirizzo IP del hostname del DNS dinamico. Ad esempio, se l'hostname è example.dyndns.org, abilitare il wildcard farà in modo che *.example.dyndns. org (a.example.dyndns.org, b.example.dyndns.org, etc.) risolva lo stesso come example.dyndns.org.

  Registrazione dettagliata Selezionare questa opzione per aumentare la registrazione per il processo di aggiornamento del DNS dinamico, utile per la risoluzione dei problemi di aggiornamento.

  Verificare il peer SSL Una volta selezionato, il certificato SSL del server del provider DynDNS sarà validizzato. Alcuni server con certificati autofirmati, o quelli che utilizzano una CA meno comune, possono richiedere che questo sia impostato.

  Nome utente Immettere il nome utente per il provider del DNS dinamico. I requisiti specifici del fornitore sono:

  Nome a buon mercato (Namecheap), FreeDNS Lasciare vuoto

  Route 53 Immettere l'**ID della chiave di accesso**

  GleSYS Immettere l'**utente API**

  Personalizzato Il nome utente viene utilizzato con l'autenticazione HTTP di base e può essere lasciato vuoto.

  Password Immettere la password per il provider del DNS dinamico. Requisiti specifici del fornitore sono:

  Nome a buon mercato (Namecheap), FreeDNS questo è il **Token di autenticazione **

  Route 53 Inserire la **chiave di accesso segreto**

  GleSYS Immettere la **chiave API**

  DNS semplice (DNSimple) Immettere il **Token API**

  Descrizione Un campo di testo per riferimento.

- Fare click su **Salvare**

Provider con impostazioni extra o diverse

Alcuni provider hanno impostazioni speciali o determinati campi che devono essere impostati in un modo specifico che potrebbe non essere ovvio. Le differenze sono delineate in questa sezione.

Namecheap

Come accennato in precedenza nelle impostazioni di cui sopra, Namecheap richiede che il nome di dominio completo sia suddiviso nella parte del hostname e nella parte del nome di dominio in campi separati.

Quando si imposta il DNS dinamico per un dominio *Namecheap*, un token di autenticazione viene fornito da Namecheap. Questo va nel campo **Password** e il campo **Username** viene lasciato vuoto.

Tunnelbroker di HE.net

La scelta dell'*intermediario del tunnel (tunnel broker) di HE.net* aggiorna un indirizzo IP dell'endpoint del tunnel IPv6 quando l'IP della WAN cambia. Il **hostname** in questo caso è l'**ID del tunnel** da HE.net.

Route 53

Quando si utilizza un tipo di *Route 53* di Amazon, Il nome utente è l'**ID della chiave di accesso** fornito da Amazon.

Le seguenti opzioni aggiuntive sono disponibili quando si utilizza *Route 53*:

Verificare il peer SSL Abilitare per verificare il certificato del server quando si utilizza HTTPS

L'ID di zona Ricevuto durante la creazione del dominio nella Route 53. Deve essere compilato.

TTL Tempo di vita per il record DNS.

Personalizzato

Il tipo DNS dinamico *personalizzato* configura le opzioni che consentono l'aggiornamento di servizi altrimenti non supportati. Quando si utilizza il tipo di DNS dinamico personalizzato, i campi **Nome utente** e **Password** vengono inviati utilizzando l'autenticazione HTTP di base.

Le seguenti opzioni aggiuntive sono disponibili quando si utilizza *Personalizzato*:

Interfaccia per inviare l'aggiornamento da Quasi sempre uguale all'interfaccia, ma può essere modificata secondo necessità.

Forzare la risoluzione IPv4 Quando selezionata, l'host di aggiornamento verrà risolto solo utilizzando IPv4

Verificare il peer SSL Abilitare per verificare il certificato del server quando si utilizza HTTPS

Aggiornare l'URL L'URL fornito dal provider del DNS dinamico per gli aggiornamenti. Se l'indirizzo IP deve apparire nell'URL, inserirlo come %IP% e il valore reale verrà sostituito se necessario.

Corrispondenza dei risultati Definisce l'output previsto dalla query della DNS dinamica. Se riesce e corrisponde all'output dato, Firew4LL saprà che l'aggiornamento ha avuto successo. Se non corrisponde esattamente, si presume che l'aggiornamento non sia riuscito. Lasciare vuoto per disabilitare il controllo dei risultati.

DNSSimple

Verificare il peer SSL Abilitare per verificare il certificato del server quando si utilizza HTTPS

ID di zona Ricevuto durante la creazione del dominio.

TTL Tempo di vita per il record DNS.

Configurazione degli aggiornamenti DNS dinamici RFC 2136

DNS dinamico RFC 2136 registra un hostname su qualsiasi server DNS che supporta gli aggiornamenti di stile RFC 2136. Questo può essere utilizzato per aggiornare i record DNS sui server DNS BIND e Windows, tra gli altri.

Le voci DNS dinamiche RFC 2136 possono essere utilizzate contemporaneamente ai fornitori di servizi DNS dinamici in stile regolare e, come tali, è possibile creare un numero qualsiasi di voci. RFC 2136 aggiornerà il record A e il record AAAA se IPv6 è configurato sull'interfaccia monitorata.

La configurazione dell'infrastruttura del server per l'hosting del DNS dinamico RFC 2136 va oltre lo scopo di questo libro, ma esiste un how-to di base sulla documentazione wiki di Firew4LL che copre l'impostazione di BIND per gestire gli aggiornamenti RFC 2136.

Per configurare un client DNS dinamico RFC 2136:

- Passare a **Servizi>DNS dinamico**
- Fare clic sulla scheda **RFC 2136**
- Fare clic su  **Aggiungere** per aggiungere una nuova voce
- Configurare le opzioni come segue:

  Abilitare Controlla se la voce è attiva o meno. Se non è selezionata, gli aggiornamenti non verranno eseguiti per questa voce.

  Interfaccia L'indirizzo IP sull'interfaccia scelta verrà inviato durante l'esecuzione dell'aggiornamento DNS.

  Hostname Il nome di dominio completo (FQDN) della voce del DNS dinamico da aggiornare. Ad esempio, myhost.example.com.

  TTL Il tempo di vita per la voce DNS, di pochi secondi. Valori più alti saranno memorizzati nella cache più a lungo da altri server del nome, quindi i valori più bassi sono meglio per essere sicuri che gli aggiornamenti DNS vengano rilevati in modo tempestivo da altri server. Di solito un valore compreso tra 30 e 180 secondi è ragionevole, a seconda della frequenza con cui l'indirizzo IP cambia.

  Nome chiave Il nome della chiave come specificato nella configurazione del server DNS. Per le chiavi host, questo è in genere il FQDN, quindi sarebbe identico al valore nel campo nome dell'host. Per le chiavi di zona questo sarebbe il nome della zona DNS.

  Tipo di chiave Può essere uno di *zona*, un *host* o un *utente*. Il tipo di chiave è determinato dal server, quindi consultare la configurazione del server o l'amministratore del server DNS per determinare il **tipo di chiave**. In genere questo è impostato su *Host*.

  Chiave Contiene il testo effettivo della chiave, ad esempio /0/4bxF9A08n/zke/vANyQ"". Questo valore viene generato dal server DNS o dall'amministratore.

  Server L'indirizzo IP o l'hostname del server DNS a cui vengono inviati gli aggiornamenti.

  Protocollo Quando deselezionato, l'aggiornamento DNS viene inviato su UDP, quando selezionato utilizza invece TCP.

Utilizzare l'IP pubblico Per impostazione predefinita, l'indirizzo IP dell'interfaccia viene sempre inviato al server del nome per l'aggiornamento DNS. Se questa casella è selezionata, quando viene rilevato un indirizzo IP privato nell'**interfaccia** selezionata, viene eseguito un controllo per determinare l'indirizzo IP pubblico effettivo e quindi l'indirizzo IP viene utilizzato per l'aggiornamento DNS.

Tipo di record Determina quali record verranno aggiornati per questa voce. Per l'indirizzo IPv4, utilizzare *A*, per IPv6, utilizzare *AAAA*, o scegliere *entrambi*.

Descrizione Una descrizione a testo libero come riferimento.

Come per gli altri tipi di DNS dinamici, gli aggiornamenti RFC 2136 vengono eseguiti solo quando viene rilevata una modifica dell'indirizzo IP o una volta ogni 25 giorni.

23.7 SNMP

Il demone del protocollo di gestione della rete semplice (Simple Network Management Protocol, SNMP) consente il monitoraggio remoto di alcuni parametri di sistema Firew4LL. A seconda delle opzioni scelte, il monitoraggio può essere eseguito per il traffico di rete, i flussi di rete, le code pf e le informazioni generali di sistema come CPU, memoria e utilizzo del disco. L'implementazione SNMP utilizzata da Firew4LL è bsnmpd, che per impostazione predefinita ha solo le informazioni base di gestione (MIB) disponibili ed è estesa da moduli caricabili. Oltre a fungere da demone SNMP, può anche inviare trappole a un server SNMP per determinati eventi. Variano in base ai moduli caricati. Ad esempio, le modifiche allo stato del collegamento di rete genereranno un trap se viene caricato il modulo MIB II.

Il servizio SNMP può essere configurato navigando in **Servizi>SNMP**.

Il modo più semplice per vedere i dati disponibili è eseguire snmpwalk contro il firewall da un altro host con net-snmp o un pacchetto equivalente installato. I contenuti completi dei MIB disponibili sono al di là della portata di questo libro, ma ci sono un sacco di stampe e risorse online per SNMP, e alcuni degli alberi MIB sono coperti in RFC. Ad esempio, le risorse Host MIB sono definite da RFC 2790.

23.7.1 SNMP e IPv6

Il demone bsnmpd attualmente non supporta IPv6.

23.7.2 Demone di SNMP

Queste opzioni dettano se e come verrà eseguito il demone SNMP. Per attivare il demone SNMP, selezionare **Abilitare**. Una volta selezionata **Abilitare**, le altre opzioni possono essere modificate.

Porta del polling Le connessioni SNMP vengono effettuate utilizzando solo i client UDP e SNMP predefiniti per l'utilizzo della porta UDP 161. Questa impostazione controlla quale porta viene utilizzata per il demone SNMP e il client SNMP o l'agente di polling deve essere modificato in modo che corrispondano.

Posizione di sistema Questo campo di testo specifica una stringa da restituire quando la posizione del sistema viene interrogata tramite SNMP. Qualsiasi testo può essere utilizzato qui. Per alcuni dispositivi una città o uno Stato potrebbe essere abbastanza adatto, mentre altri potrebbero aver bisogno di dettagli più specifici come il rack e la posizione in cui risiede il sistema.

Contatto di sistema Una stringa che definisce le informazioni di contatto per il sistema. Può essere un nome, un indirizzo e-mail, un numero di telefono o qualsiasi altra cosa sia necessaria.

Leggere la stringa di comunità Con SNMP, la stringa comunità agisce come una sorta di nome utente e password in uno. I client SNMP dovranno utilizzare questa stringa di comunità durante il polling. Il

valore predefinito di public è comune, quindi consigliamo vivamente di utilizzare un valore diverso oltre a limitare l'accesso al servizio SNMP con le regole del firewall.

23.7.3 Trappola di SNMP

Per indicare al demone SNMP di inviare trap SNMP, selezionare **Abilitare**. Una volta che abilitare è stata selezionata, le altre opzioni possono essere modificate.

Server del trap Il server trap è l'hostname o l'indirizzo IP a cui vengono inoltrati i trap SNMP.

Porta server del trap Per impostazione predefinita, i trap SNMP sono impostati sulla porta UDP 162. Se il ricevitore dei trap SNMP è impostato per una porta diversa, regolare questa impostazione in modo che corrisponda.

Stringa di trap SNMP Questa stringa verrà inviata insieme a qualsiasi trap SNMP generato.

23.7.4 Moduli

I moduli caricabili consentono al demone SNMP di comprendere e rispondere alle query per ulteriori informazioni sul sistema. Ogni modulo caricato consumerà risorse aggiuntive. In quanto tale, assicurarsi che vengano caricati solo i moduli richiesti.

MibII Questo modulo fornisce informazioni specificate nell'albero MIB II standard, che copre le informazioni e le interfacce di rete. Avere questo modulo caricato, tra le altre cose, fornisce informazioni sull'interfaccia di rete tra cui lo stato, l'hardware e gli indirizzi IP, la quantità di dati trasmessi e ricevuti e molto altro.

Grafico di rete (Netgraph) Il modulo netgraph fornisce alcune informazioni relative a netgraph come i nomi e gli Stati dei nodi netgraph, i peer hook e gli errori.

PF Il modulo PF fornisce una vasta gamma di informazioni su pf. L'albero MIB copre aspetti del set di regole, Stati, interfacce, tabelle e code ALTQ.

Risorse host Questo modulo fornisce informazioni sull'host stesso, inclusi uptime, media di carico e processi, tipi di archiviazione e utilizzo, dispositivi di sistema collegati e persino software installato. Questo modulo richiede MIBII, quindi se MIBII è deselezionato quando questa opzione è selezionata, MIBII verrà selezionato automaticamente.

UCD Questo modulo fornisce varie informazioni sui sistemi conosciuti come ucdavis MIB, o UCD-SNMP-MIB. Fornisce informazioni sull'utilizzo della memoria, sull'utilizzo del disco, sui programmi in esecuzione e altro ancora.

Regex Il modulo Regex è riservato per un uso o un utilizzo futuro da parte degli utenti che personalizzano il codice in base alle loro esigenze. Consente di creare contatori SNMP da file di registro o altri file di testo.

23.7.5 Binding interfaccia

Questa opzione configura il demone SNMP per ascoltare solo l'interfaccia scelta o l'indirizzo IP virtuale. Tutte le interfacce con indirizzi IP, VIP del CARP e VIP Alias di IP vengono visualizzate nell'elenco a discesa.

L'associazione a un'interfaccia locale specifica può facilitare la comunicazione su tunnel VPN, in quanto elimina la necessità del percorso statico precedentemente menzionato e fornisce anche una maggiore sicurezza non esponendo il servizio ad altre interfacce. Può anche migliorare la comunicazione su più interfacce locali, poiché il demone SNMP risponderà dall'indirizzo "più vicino" a un indirizzo IP di sorgente e non all'indirizzo IP a cui è stata inviata la query.

23.8 UPnP e NAT-PMP

Universal Plug and Play (UPnP) e Protocollo di mappatura delle porte NAT (NAT Port Mapping Protocol, NAT-PMP) sono servizi di rete che consentono al software e ai dispositivi di configurarsi a vicenda quando si collegano a una rete. Ciò include la creazione automatica della propria porta forward del NAT dinamico e delle regole del firewall associate.

Il servizio UPNP e NAT-PMP su Firew4LL, trovato su **Servizi>UPnP e NAT-PMP**, consente ai PC client e ad altri dispositivi come console di gioco di consentire automaticamente il traffico in entrata richiesto. Ci sono molti programmi e sistemi popolari che supportano UPnP, come Skype, uTorrent, mIRC, client IM, Wii U, PlayStation 4 e Xbox One. NAT-PMP è supportato sui prodotti Apple.

UPnP utilizza il Protocollo di individuazione del servizio semplice (Simple Service Discovery Protocol, SSDP) per il rilevamento della rete, che utilizza la porta UDP 1900. Il demone UPnP utilizzato da Firew4LL, miniupnpd, utilizza anche la porta TCP 2189. Quando si utilizza un set di regole LAN rigoroso, aggiungere manualmente le regole del firewall per consentire l'accesso a questi servizi, specialmente se la regola predefinita LAN per chiunque (LAN-to-any) è stata rimossa o in configurazioni a ponte. NAT-PMP è gestito anche da miniupnpd e utilizza la porta UDP 5351.

23.8.1 UPnP & NAT-PMP e IPv6

Al momento della stesura di questo articolo, il servizio UPNP e NAT-PMP sulle versioni correnti di Firew4LL supporta IPv6, ma il supporto client è ancora spotty.

23.8.2 Problemi di sicurezza

UPnP e NAT-PMP sono un classico esempio del compromesso «sicurezza contro convenienza». Per loro stessa natura, questi servizi sono insicuri. Qualsiasi programma sulla rete può consentire l'ingresso e l'inoltro di qualsiasi traffico - un potenziale incubo di sicurezza. D'altra parte, inserire e mantenere le porte forward del NAT e le loro regole associate possono essere un'incombenza, soprattutto quando si tratta di console di gioco. Ci sono un sacco di congetture e di ricerca coinvolti per trovare le porte e le impostazioni corrette, ma UPnP *funziona* e richiede poco sforzo amministrativo. Le porte forward manuali per adattarsi a questi scenari tendono ad essere eccessivamente permissive, esponendo potenzialmente servizi che non dovrebbero essere aperti da Internet. Le porte forward sono sempre attive, dove UPnP può essere temporaneo.

I controlli di accesso esistono nella configurazione del servizio UPnP, che aiuta a bloccare quali dispositivi sono autorizzati ad apportare modifiche. Oltre ai controlli di accesso integrati, è possibile esercitare un ulteriore controllo con le regole del firewall. Se correttamente controllato, UPnP può anche essere un po' più sicuro consentendo ai programmi di raccogliere e ascoltare su porte casuali, invece di avere sempre la stessa porta aperta e inoltrata.

23.8.3 Configurazione

Per configurare UPnP e NAT-PMP:

- Passare a **Servizi>UPnP e NAT-PMP**
- Configurare le opzioni come segue:

Abilita UPnP e NAT-PMP Controllo principale per l'intero servizio. Se deselezionato, tutti i servizi di questa pagina sono disabilitati.

Consentire la mappatura delle porte UPnP quando selezionata, UPnP è consentito.

Consentire la mappatura delle porte NAT-PMP Quando è selezionata, NAT-PMP è consentito.

Interfaccia esterna L'interfaccia WAN per il traffico in uscita. Questo deve essere impostato sulla WAN contenente il gateway predefinito. È possibile selezionare una sola **interfaccia esterna**.

Interfacce Le interfacce locali in cui i client che hanno il permesso di utilizzare UPnP/NAT-PMP risiedono. Quando un bridge è in uso, selezionare solo l'interfaccia bridge con un indirizzo IP. È possibile selezionare più interfacce.

Velocità di download Velocità massima di download riferita ai client, in kilobit al secondo.

Velocità di upload Velocità massima di upload riferita ai client, in kilobit al secondo.

Indirizzo delle WAN di override Seleziona un indirizzo IP di interfaccia alternativo da utilizzare, ad esempio un indirizzo IP virtuale CARP o Alias dell'IP.

Coda dello shaping di traffico Il nome di una coda di shaping del traffico ALTQ (non limitatore) in cui verrà inserito il traffico consentito tramite l'utilizzo di UPnP.

Nota: prestare attenzione quando si seleziona questa coda. UPnP è utilizzato da traffico come console di gioco, che hanno bisogno di alta priorità, e anche da client di trasferimento di file che possono avere bisogno di bassa priorità.

Pacchetti di registro Una volta selezionata, le porte forward generate da UPnP/NAT-PMP saranno impostate sul registro, in modo che ogni connessione effettuata avrà una voce nei registri del firewall, che si trova in **Stato>Registri di sistema**, nella scheda **Firewall**.

Utilizzare l'uptime di sistema Per impostazione predefinita, il demone UPnP segnala l'uptime del servizio quando interrogato piuttosto che l'uptime di sistema. La selezione di questa opzione causerà invece la segnalazione del tempo di attività effettivo del sistema.

Negare l'accesso per impostazione predefinita Quando selezionata, UPnP consentirà solo l'accesso ai client corrispondenti alle regole di accesso. Questo è un metodo più sicuro per controllare il servizio, ma come discusso sopra, è anche meno conveniente.

Autorizzazioni specificate dall'utente Questi campi specificano regole di accesso definite dall'utente. Se viene scelta l'opzione di negazione predefinita, è necessario impostare regole per consentire l'accesso. Regole aggiuntive possono essere aggiunte facendo clic su  **Aggiungere** regole sono formulate utilizzando il seguente formato:

```
<[allow|deny]> <[external port|port range]> <[internal IP|IP/CIDR]>
↪<[internal port|port range]>
```

- Fare clic su **Salvare**

Il servizio UPNP e/o NAT-PMP verrà avviato automaticamente.

Esempi di autorizzazione utente UPnP

Negare l'accesso alla porta esterna 80 che inoltra ciò che arriva da ogni cosa sulla LAN, 192.168.1.1, con una Subnet /24, alla porta locale 80:

```
deny 80 192.168.1.1/24 80
```

Consentire a 192.168.1.10 di inoltrare qualsiasi porta non privilegiata:

```
allow 1024-65535 192.168.1.10 1024-65535
```

23.8.4 Stato

Lo stato del processo del daemon UPnP può essere visualizzato in **Stato>Servizi**. La pagina dello stato del servizio mostra se il demone è in esecuzione o arrestato e consente di arrestare, avviare o riavviare il servizio. In circostanze normali, la gestione manuale del demone non è necessaria.

Un elenco di porte e client attualmente inoltrati, simile alla figura *Schermata dello stato di UPnP & NAT-PMP che mostra PC Client con porte forward*, può essere visualizzato in **Stato>UPnP e NAT-PMP**.

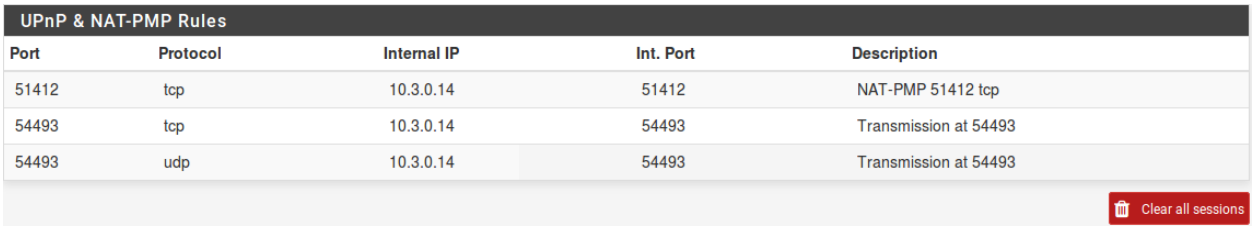


Fig. 2: Schermata dello stato di UPnP & NAT-PMP che mostra PC Client con porte forward

23.8.5 Risoluzione dei problemi

La maggior parte dei problemi con UPnP tendono a coinvolgere il bridging. In questo caso è importante avere regole del firewall che consentano UPnP sulla porta UDP 1900. Poiché si tratta di traffico multicast, la destinazione sarà l'indirizzo di trasmissione per la Subnet, o in alcuni casi renderlo *qualsiasi* è necessario. Consultare i registri del firewall in **Stato>Registri di sistema**, nella scheda **Firewall** per vedere se il traffico viene bloccato. Prestare particolare attenzione all'indirizzo di destinazione, in quanto potrebbe essere diverso dal previsto.

Ulteriori problemi con le console di gioco possono anche essere alleviati passando al NAT in uscita manuale e abilitando la porta statica. Vedi *Porta statica* per maggiori dettagli

23.9 NTPD

Il servizio NTP è un demone del Protocollo dell'ora di rete (Network Time Protocol, NTP) che ascolterà le richieste dei client e permetterà loro di sincronizzare il loro orologio con quello del firewall di Firew4LL. Eseguire un server NTP locale e utilizzarlo per i client locali, riduce il carico sui server di livello inferiore e può garantire che i sistemi locali possano sempre raggiungere un server dell'orario. Prima di delegare questa attività a un firewall che esegue Firew4LL, la migliore pratica è garantire che il firewall abbia un orologio accurato e mantenga l'orario ragionevolmente.

23.9.1 NTP e IPv6

Il demone del progetto NTP supporta pienamente IPv6 come client e server.

Configurazione del server NTP

Per configurare il server NTP:

- Passare a **Servizi>NTP**
- Configurare le impostazioni come segue:

  Interfaccia Selezionare le interfacce da utilizzare per NTP. Il demone NTP si lega a tutte le interfacce per impostazione predefinita per ricevere risposte correttamente. Questo può essere ridotto al minimo selezionando almeno un'interfaccia da associare, ma tale interfaccia verrà utilizzata anche

per generare le query NTP inviate ai server remoti, non solo per servire i client. Deselezionare tutte le interfacce è l'equivalente di selezionare tutte le interfacce.

Server dell'orario Un elenco di server da interrogare per mantenere sincronizzato l'orologio di questo firewall. Questo elenco viene inizialmente estratto dalle voci in **Sistema>Configurazione generale**. Per ottenere i migliori risultati, si consiglia di utilizzare almeno tre server, ma non più di cinque. Fare clic su  Aggiungere a server di tempo aggiuntivi configurati.

Preferenza Quando è selezionata, questa voce del server NTP è favorita dal demone NTP rispetto ad altri.

Nessuna selezione Se selezionato, questo server NTP non viene utilizzato per la sincronizzazione dell'ora, ma solo per visualizzare le statistiche.

Modalità orfana La modalità orfana utilizza l'orologio di sistema quando non sono disponibili altri orologi, altrimenti i client non riceveranno una risposta quando altri server non sono raggiungibili. Il valore immesso qui è lo strato utilizzato per la **modalità orfana** e in genere è impostato abbastanza in alto da preferire i server live. Il valore predefinito è 12.

Grafici NTP Selezionare per abilitare i grafici RRD per le statistiche del server NTP.

Registrazione Quando le opzioni di registrazione sono attive, i registri NTP vengono scritti utilizzando syslog e possono essere trovati in **Stato>Registri di sistema**, nella scheda **NTP**.

Registrare i messaggi del peer Una volta selezionato, NTP registrerà i messaggi relativi agli eventi peer, alle informazioni e allo stato.

Registrare i messaggi di sistema Una volta selezionato, NTP registrerà i messaggi sugli eventi, le informazioni e lo stato del sistema.

Registrazione delle statistiche Fare clic su  **Mostrare avanzate** per visualizzare queste opzioni. Quando abilitato, NTP creerà file di log giornalieri persistenti in /var/log/ntp per mantenere i dati delle statistiche. Il formato dei record delle statistiche nei file di registro può essere trovato in ntp.pagina man conf

Registrare le statistiche dell'orologio di riferimento Una volta selezionato, NTP registra le statistiche dei driver dell'orologio su ogni aggiornamento.

Registrare le statistiche dell'esercizio dell'orologio Una volta selezionato, NTP registra le statistiche del filtro loop su ogni aggiornamento dell'orologio locale.

Registrare le statistiche del peer di NTP Quando selezionato, NTP registra le statistiche per tutti i peer del demone NTP, insieme a segnali speciali.

Secondi da saltare (Leap seconds) Fare clic su  **Mostrare avanzate** per visualizzare queste opzioni. Definisce il contenuto del file Leap Second, utilizzato da NTP per annunciare i prossimi secondi da saltare ai client. Questo viene in genere utilizzato solo dai server dello strato 1. Il formato esatto del file può essere trovato nell'elenco dei secondi da saltare di IETF

- Fare clic su **Salvare**

Restrizioni di accesso

Le restrizioni di accesso (ACL) sono configurate nella scheda **ACL** in **Servizi>NTP**. Questi ACL controllano come NTP interagisce con i client.

Restrizioni di accesso predefinite Controllano il comportamento per tutti i client per impostazione predefinita.

Kiss-o'-Death Quando impostato, NTP invierà un pacchetto KoD quando si verifica una violazione di accesso. Tali pacchetti sono a tasso limitato e non più di uno al secondo sarà inviato.

Modifiche Quando impostato, le query ntpq e ntpdc che tentano di modificare la configurazione del server vengono negate, ma vengono restituite query informative.

Query Quando impostato, tutte le query da ntpq e ntpdc vengono negate.

> **Avvertimento:** L'impostazione di questo disabiliterà efficacemente la pagina di stato NTP, che si basa su ntpq.

Servizio Quando impostato, NTP negherà tutti i pacchetti tranne le query da ntpq e ntpdc.

Associazione di peer Quando impostato, NTP nega i pacchetti che si tradurrebbero in una nuova associazione peer, inclusi i pacchetti attivi broadcast e simmetrici per i peer senza un'associazione esistente.

Servizio trap Quando è impostato, NTP non fornirà un messaggio di controllo del servizio trap in modalità 6, utilizzato per la registrazione degli eventi da remoto.

Restrizioni di accesso personalizzate Definisce il comportamento per specifici indirizzi client o sottoreti.

Fare clic su  **Aggiungere** per aggiungere una nuova definizione di rete.

Rete/maschera La Subnet e la maschera per definire il client controllato dalle restrizioni in questa voce.

Restrizioni I nomi delle opzioni sono versioni abbreviate di quelle nell'elenco predefinito, nello stesso ordine.

Fare clic su **Salvare** per memorizzare gli ACL.

GPS seriale

Se questo firewall dispone di una porta seriale disponibile, è possibile utilizzare un GPS seriale per fornire un orologio di riferimento per il firewall. Se il GPS supporta anche un segnale di impulso al secondo (Pulse Per Second, PPS), che può essere utilizzato anche come un PPS dell'orologio di riferimento.

> **Avvertimento:** Le unità GPS USB possono unzionare, ma noi non consigliamo il loro uso a causa di problemi di temporizzazione. Il sovraccarico di USB le rende inaffidabile come orologio o fonte di temporizzazione.

Per ottenere i migliori risultati, si consiglia di configurare almeno due server NTP in **Sistema>Configurazione generale** o **Servizi>NTP** per evitare la perdita di sincronizzazione se i dati GPS non sono validi nel tempo. In caso contrario, il demone NTP può utilizzare solo i valori dell'orologio locale non sincronizzato quando fornisce il tempo ai client.

Per configurare un GPS per l'uso da parte di NTP:

- Passare a **Servizi>NTP**
- Fare clic sulla scheda **GPS seriale**
- Configurare le impostazioni come segue:

  Tipo di GPS Selezionare la marca e il modello dell'unità GPS. Se il modello è sconosciuto, utilizzare la scelta *Predefinito*. Se il modello è noto ma non elencato, utilizzare *Personalizzato*.

Porta seriale Sono elencate tutte le porte seriali rilevate sul firewall. Selezionare la porta con il GPS collegato. Le porte seriali dell'hardware di bordo iniziano con cuau, le porte seriali USB sono precedute da cuaU.

Tasso di baud Immettere la velocità seriale per il GPS, in genere un valore basso come 4800

Frasi NMEA Per impostazione predefinita, NTP ascolterà tutte le frasi NMEA supportate. Per limitare questo a tipi specifici, selezionarli dall'elenco.

Falsificare il tempo 1 Specifica una costante da aggiungere al segnale PPS di GPS come offset.

Falsificare il tempo 2 Specifica una costante da aggiungere al tempo GPS come offset.

Strato Utilizzato per configurare lo strato dell'orologio GPS. Il valore predefinito è 0, quindi il GPS è preferito a tutti gli altri. Se invece è necessario preferire un altro orologio, impostare il valore dello strato superiore allo strato dell'orologio preferito.

Flag Queste opzioni forniscono ulteriori modifiche per ottimizzare il comportamento GPS:

Preferire questo orologio Segna l'orologio di riferimento come preferito da NTP.

Non utilizzare questo orologio Impedisce che l'orologio venga utilizzato da NTP per la sincronizzazione del tempo, viene visualizzato solo per riferimento.

Elaborazione del segnale PPS Consente l'elaborazione del segnale di impulso al secondo (PPS) nel driver GPS. Abilitare questa opzione solo se il GPS è noto per emettere un segnale PPS utilizzabile.

Elaborazione del segnale PPS del bordo di caduta Quando è impostato, il bordo di caduta del segnale PPS viene utilizzato per la temporizzazione, piuttosto che il bordo di salita.

Disciplina dell'orologio PPS del Kernel Quando è impostato, il Kernel del sistema operativo utilizzerà PPS direttamente per i tempi.

Posizione oscura nel timestamp Oscura i dati GPS in modo che la posizione dell'orologio non possa essere determinata.

Registrare la frazione di secondi del timestamp ricevuto Una volta selezionato, questo può riempire rapidamente il registro, ma può essere utile per la messa a punto dell'opzione **Falsificare il tempo 2**.

ID orologio Un identificatore di 1-4 caratteri utilizzato per modificare l'ID dell'orologio GPS. Il valore predefinito è GPS.

Inizializzazione GPS Contiene la stringa di inizializzazione inviata al GPS all'avvio per configurare il comportamento. Quando si utilizza il tipo GPS personalizzato, è necessario immettere manualmente una stringa di inizializzazione corretta per il GPS.

Calcolatore della somma di controllo di NMEA Calcola un checksum da utilizzare quando si creano nuovi valori di inizializzazione GPS o si regolano i valori esistenti.

- Fare click su **Salvare**

Sorgente PPS (non GPS)

Una sorgente PPS non GPS, come una radio, può essere utilizzata anche per i tempi di clock. Non può essere utilizzato per la sincronizzazione poiché non ci sono dati temporali, ma può essere utilizzato per garantire un ticchettio accurato dell'orologio.

Per configurare una sorgente PPS non GPS:

- Passare a **Servizi>NTP**
- Fare clic sulla scheda **PPS**

- Configurare le impostazioni come segue:

  Porta seriale Sono elencate tutte le porte seriali rilevate sul firewall. Selezionare la porta con il GPS collegato. Le porte seriali dell'hardware di bordo iniziano con cuau, le porte seriali USB sono precedute da cuaU.

  Falsificare il tempo 1 Specifica una costante da aggiungere al segnale PPS come offset, per tenere conto del ritardo tra il trasmettitore e il ricevitore.

  Strato Utilizzato per configurare lo strato della sorgente PPS. Il valore predefinito è 0, quindi la sorgente del PPS è preferita su tutti gli altri. Se invece è necessario preferire un altro orologio, impostare il valore dello strato superiore allo strato dell'orologio preferito.

Flag

Elaborazione del segnale PPS del bordo di caduta Quando è impostata, il bordo di caduta del segnale PPS viene utilizzato per la temporizzazione, piuttosto che il bordo di salita.

Disciplina dell'orologio PPS del Kernel Quando è impostato, il Kernel del sistema operativo utilizzerà PPS direttamente per i tempi.

Registrare un timestamp Registra un timestamp una volta per ogni secondo, che è utile per costruire trame di deviazione Allan.

ID dell'orologio Un identificatore di carattere 1-4 utilizzato per modificare l'ID dell'orologio PPS. Il valore predefinito è PPS.

- Fare click su **Salvare**

Stato

La pagina di stato NTP mostra lo stato di ciascun server peer NTP. Questa pagina di stato può essere trovata in **Stato>NTP**. Un esempio dello stato è mostrato nella figura *Stato del demone NTP con l'uscita GPS*.

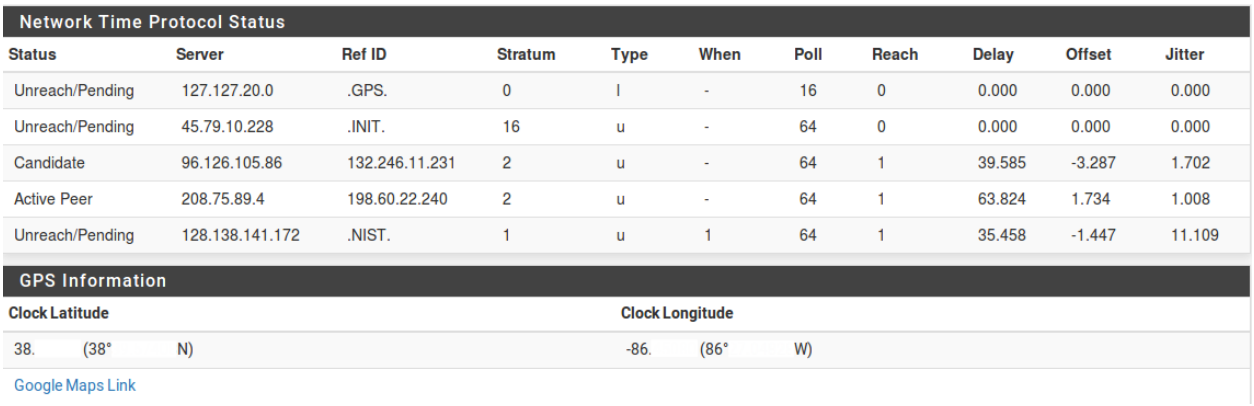
La schermata di stato contiene una riga per ogni peer ed elenca l'indirizzo IP del peer o l'ID server, l'ID del clock di riferimento per il peer e vari altri valori che indicano la qualità generale del server NTP dal punto di vista di questo firewall. La prima colonna è la più utile, in quanto indica quale peer è attualmente il peer attivo per la sincronizzazione dell'orario, quali server sono potenziali candidati per essere peer e quali server sono stati rifiutati e perché.

Se un GPS seriale è collegato e configurato, vengono elencate anche le coordinate riportate dal dispositivo GPS, insieme a un link alle coordinate su Google Maps.

Nota: La qualità dei dati GPS può variare ampiamente a seconda del

---

livello del segnale, del dispositivo GPS e del modo in cui viene collegato. Le porte seriali tradizionali sono di qualità superiore e più adatte all'utilizzo dell'orologio GPS. Le unità GPS seriale dell'USB può essere accettabile, ma a causa di come funzioni l'USB, il tempismo dei segnali non può essere garantito nel modo in cui può esserlo con una tradizionale porta seriale programmata.



Network Time Protocol Status

Status	Server	Ref ID	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
Unreach/Pending	127.127.20.0	.GPS.	0	l	-	16	0	0.000	0.000	0.000
Unreach/Pending	45.79.10.228	.INIT.	16	u	-	64	0	0.000	0.000	0.000
Candidate	96.126.105.86	132.246.11.231	2	u	-	64	1	39.585	-3.287	1.702
Active Peer	208.75.89.4	198.60.22.240	2	u	-	64	1	63.824	1.734	1.008
Unreach/Pending	128.138.141.172	.NIST.	1	u	1	64	1	35.458	-1.447	11.109

GPS Information

Clock Latitude			Clock Longitude		
38.	(38°	N)	-86.	(86°	W)

Google Maps Link

Fig. 3: Stato del demone NTP con l'uscita GPS

23.10 WOL (Wake on LAN)

La pagina WOL (Wake on LAN) su **Servizi>WOL** può riattivare i computer da uno stato spento inviando speciali "pacchetti magici".

La scheda di interfaccia di rete nel computer del client che deve essere attivato deve supportare WOL e deve essere configurata correttamente. In genere esiste un'impostazione del BIOS per abilitare WOL e gli adattatori non integrati richiedono spesso un cavo WOL collegato tra NIC e un'intestazione WOL sulla scheda madre.

WOL ha molti usi potenziali. In genere, le workstation e i server vengono mantenuti in esecuzione a causa dei servizi forniti, dei file o delle stampanti che condividono o per comodità. L'uso di WOL consentirebbe a questi di rimanere in uno stato di sonno per risparmiare energia. Quando è richiesto un servizio, il sistema può essere attivato quando necessario. Un altro esempio potrebbe essere se qualcuno ha bisogno di accesso remoto a un sistema, ma l'utente lo spegne prima di lasciare l'ufficio. Utilizzando WOL il sistema di destinazione può essere attivato, e può quindi essere accessibile una volta avviato.

Avvertimento: WOL non offre alcuna sicurezza intrinseca. Qualsiasi sistema sulla stessa rete di livello 2 può trasmettere un pacchetto WOL e il pacchetto sarà accettato e obbedito. È meglio configurare WOL solo nel BIOS per le macchine che ne hanno bisogno e disabilitarlo in tutti gli altri. Ci sono alcune estensioni WOL specifiche del fornitore che forniscono una maggiore sicurezza, ma nulla è supportato universalmente.

23.10.1 Attivare una singola macchina

Per attivare una singola macchina:

- Passare a **Servizi>Attivare la LAN**
- Selezionare l'**interfaccia** attraverso la quale è possibile raggiungere il sistema di destinazione
- Inserire l'**indirizzo MAC** del sistema di destinazione nel formato di xx:xx:xx:xx:xx:xx
- Fare clic su **Inviare**

  Firew4LL trasmetterà un pacchetto magico WOL fuori l'interfaccia scelta, e se tutto è andato come previsto, il sistema si accende e inizia ad avviarsi. Tenete a mente che i sistemi impiegheranno del tempo per l'avvio. Potrebbero essere diversi minuti prima che il sistema di destinazione sia disponibile.

23.10.2 Memorizzazione degli indirizzi MAC

Per memorizzare un indirizzo MAC per comodità:

- Passare a **Servizi>Attivare la LAN**
- Fare clic su  **Aggiungere** nell'elenco degli indirizzi MAC memorizzati per aggiungere una nuova voce
- Selezionare l'**interfaccia** attraverso la quale è possibile raggiungere il sistema di destinazione
- Inserire l'**indirizzo MAC** del sistema di destinazione nel formato di xx:xx:xx:xx:xx:xx
- Immettere una **descrizione** per la voce, ad esempio il nome, il proprietario o la posizione del sistema di destinazione. Ad esempio: «PC di Pat» o » Server di Sue"
- Fare clic su **Salvare**

Una volta salvato, la voce sarà disponibile nell'elenco **Servizi>Attivare la LAN**.

Mantenere le voci è simile ad altre attività in Firew4LL: Fare clic su  per modificare una voce esistente e fare clic su  per rimuovere una voce.

23.10.3 Riattivare una singola macchina memorizzata

Per inviare un pacchetto magico WOL a un sistema precedentemente memorizzato:

- Passare a **Servizi>Attivare la LAN**
- Individuare la voce desiderata nell'elenco
- Fare clic sul suo **indirizzo MAC** o fare clic su  l'icona nella colonna **Azioni**

La pagina WOL verrà ricaricata e verrà inviato il pacchetto magico. Verrà visualizzato anche lo stato tentativo WOL.

23.10.4 Accendere tutte le macchine memorizzate

Per inviare un pacchetto magico WOL a tutti i sistemi memorizzati contemporaneamente:

- Passare a **Servizi>Attivare la LAN**
- Fare clic su  **Attivare tutti i dispositivi** sotto l'elenco degli indirizzi memorizzati.

23.10.5 Attivazione dai lease del DHCP

Per inviare un pacchetto magico WOL dalla vista delle lease di DHCP:

- Passare a **Stato>lease di DHCP**
- Individuare il sistema desiderato nell'elenco
- Fare clic su  alla fine della riga di lease per inviare un pacchetto magico WOL

Nota: la funzione WOL è disponibile solo per i sistemi contrassegnati offline, il che significa che non sono nella tabella ARP sul firewall. Se un sistema è stato spento di recente, possono essere necessari alcuni minuti per la scadenza della voce ARP prima che venga contrassegnata offline.

Se un sistema è stato spento per un bel po " di tempo, fare clic su **Mostrare tutte le lease configurate** potrebbe essere necessario per visualizzare la lease precedente.

Quando si fa clic sul link, il browser tornerà alla pagina WOL e verrà inviato il pacchetto magico.

23.10.6 Salvare dalla lista dei lease del DHCP

Un indirizzo MAC e un hostname possono essere copiati in una nuova voce della mappatura WOL durante la visualizzazione delle lease di DHCP.

- Passare a **Stato>lease di DHCP**
- Individuare il sistema desiderato nell'elenco
- Fare clic su alla fine della voce di lease
- Confermare i valori nella pagina e inserire tutte le informazioni mancanti.
- Fare clic su **Salvare**

23.11 Server PPPoE

Firew4LL può fungere da server PPPoE, accettando e autenticando le connessioni dai client PPPoE su un'interfaccia locale, nel ruolo di un concentratore di accesso (LAC). Questa funzione può essere utilizzata per forzare gli utenti ad autenticarsi prima di accedere alla rete o controllare in altro modo il loro comportamento di accesso.

Il server PPPoE si trova in **Servizi>Server PPPoE**. La configurazione è molto simile al server VPN di L2TP (*VPN di L2TP*).

Più server PPPoE possono essere configurati su interfacce separate. Per iniziare a configurare un server PPPoE:

- Passare a **Servizi>Server PPPoE**
- Fare clic su **Aggiungere** per aggiungere una nuova voce server
- Configurare il server PPPoE come segue:

  Abilitare Se selezionata, questa istanza del server PPPoE sarà attiva.

  Interfaccia La singola interfaccia su cui sarà disponibile il servizio PPPoE.

  Conteggio degli utenti totali Determina quanti client in totale sono autorizzati a connettersi a questa istanza.

  Accessi massimi dell'utente Determina quante volte un singolo client può accedere contemporaneamente.

  Indirizzo del server L'indirizzo IP che il sistema Firew4LL invierà ai client PPPoE da utilizzare come gateway.

> **Avvertimento:** Questo indirizzo IP non deve essere un indirizzo IP attualmente in uso sul firewall.

Intervallo di indirizzi remoti L'indirizzo IP per l'inizio della Subnet client PPPoE. Insieme alla Subnet Maskt definisce la rete utilizzata dai client PPPoE.

Subnet Maskt Definisce la maschera CIDR assegnata ai client PPPoE.

Descrizione Testo esplicativo opzionale per questa istanza del server.

Server del DNS Campi opzionali utilizzati per inviare i server DNS specifici ai client PPPoE, altrimenti l'indirizzo IP del firewall verrà inviato al client attraverso il DNS se il forwarder del DNS o il risolutore del DNS sono abilitati. Se il forwarder del DNS e il risolutore del DNS sono entrambi disabilitati, verranno inviati invece i server DNS configurati sul firewall.

- Configurare RADIUS se questo verrà utilizzato per l'autenticazione dell'utente. È possibile utilizzare qualsiasi server RADIUS.

Vedi anche:

Vedere *autenticazione RADIUS con il server Windows* per informazioni sulla configurazione di RADIUS su un server Windows.

Usare l'autenticazione RADIUS Selezionare per configurare il server PPPoE per utilizzare almeno un server RADIUS per l'autenticazione anziché gli utenti locali.

Usare l'accounting del RADIUS Opzionale, invia i dati di accounting del RADIUS al server RADIUS per annotare elementi come i tempi di accesso e di logout e la larghezza di banda utilizzata.

Usare un server di autenticazione del RADIS di backup Un secondo server RADIUS da utilizzare se il server RADIUS primario non riesce.

Indirizzo IP del NAS Facoltativo, invia un indirizzo IP specifico al server RADIUS per l'attributo dell'indirizzo IP del NAS.

Aggiornamento dell'accounting del RADIUS L'intervallo in cui i dati di accounting vengono inviati al server RADIUS, in secondi.

Indirizzi IP emessi dal RADIUS Una volta selezionato, gli indirizzi IP possono essere assegnati agli utenti tramite gli attributi di risposta del RADIUS.

Server RADIUS primario Il server RADIUS preferito da utilizzare per l'autenticazione.

Indirizzo IP L'indirizzo IP del server RADIUS

Porta di autenticaazione La porta utilizzata per l'autenticazione (in genere 1812)

Porta per l'accounting La porta utilizzata per i dati di accounting (in genere 1813)

Segreto condiviso del server RADIUS primario Il segreto condiviso configurato per questo firewall sul server RADIUS. Lo stesso valore deve essere inserito nella casella di conferma.

Server RADIUS secondario Stesso tipo di impostazioni del primario, ma definisce il server RADIUS secondario.

- Aggiungere utenti al server per utilizzare l'autenticazione locale:
  - Fare clic su  Aggiungere utente

    Nome utente Il nome utente per l'account utente

    Password La password per l'account utente

    Indirizzo IP Un indirizzo IP statico opzionale per assegnare l'utente al login

- Ripetere se necessario
- Fare clic su **Salvare**

23.12 Proxy IGMP

Il proxy IGMP (Protocollo della gestione del gruppo di internet, Internet Group Management Protocol) fornisce un mezzo per il proxy del traffico multicast tra i segmenti di rete.

Il servizio proxy IGMP può essere trovato in **Servizi>Proxy IGMP**.

Per una configurazione del proxy IGMP funzionante, è necessario definire un'interfaccia upstream e almeno un'interfaccia downstream. Per configurare il proxy IGMP:

- Passare a **Servizi>Proxy IGMP**
- Fare clic su **Aggiungere** per creare una nuova istanza di interfaccia
- Configurare l'istanza come segue:

  Interfaccia L'interfaccia da utilizzare per questa istanza

  Descrizione Testo facoltativo per descrivere questa istanza

  Tipo Il tipo di interfaccia di rete definita da questa istanza

  Interfaccia di upstream L'interfaccia in uscita che è responsabile della comunicazione alle fonti di dati multicast disponibili. Ci può essere solo **un**'interfaccia upstream.

  Interfaccia di downstream Le interfacce di distribuzione alle reti di **destinazione**, in cui i **client** multicast possono unirsi a gruppi e ricevere dati multicast. È necessario configurare una o più interfacce downstream.

  Soglia La soglia TTL per i dati inoltrati su un'interfaccia, per evitare che il loop si verifichi. I pacchetti con un TTL inferiore al valore in questo campo verranno ignorati. Il TTL predefinito è 1 se il campo è lasciato vuoto.

  Reti Un elenco di voci di rete mascherate da CIDR per controllare quali sottoreti possono avere i loro dati multicast proxy. Fare clic su **Aggiungere rete** per accedere a reti aggiuntive.
- Fare click su **Salvare**

Una regola del firewall è richiesta anche sul lato **Downstream** (ad esempio *LAN*) per abbinare e superare il traffico multicast. Nelle *Opzioni avanzate* della regola firewall, **Consentire pacchetti con opzioni IP** deve essere abilitata. L'installazione di base del software Firew4LL include servizi che aggiungono funzionalità e flessibilità fondamentali al firewall. Gli argomenti di questo capitolo discutono i servizi nell'installazione di base che il firewall fornisce per altri host sulla rete. Questi servizi includono l'allease di indirizzi IPv4 e IPv6 tramite DHCP, la risoluzione DNS e il DNS dinamico, SNMP, UPnP e altro ancora. I servizi aggiuntivi possono anche essere aggiunti con pacchetti, che saranno coperti più avanti nel libro.

CAPITOLO 24

Log - Monitoraggio del sistema

24.1 Registri di sistema

Firew4LL registra molti dati per impostazione predefinita, ma lo fa in un modo che non traboccherà l'archiviazione sul firewall. I log possono essere visualizzati nella GUI in **Stato>Registri di sistema** e in /var/log/ sul file system.

Alcuni componenti come DHCP e IPsec generano abbastanza registri che hanno le proprie schede di registrazione per ridurre l'ingombro nel registro di sistema principale e per facilitare la risoluzione dei problemi per questi singoli servizi. Per visualizzare altri registri, fare clic sulla scheda per il sottosistema da visualizzare. Alcune aree, come il **Sistema** e la **VPN**, hanno sotto-schede con ulteriori opzioni correlate.

I registri Firew4LL sono contenuti in un formato di registro circolare binario chiamato **clog**. Questi file sono di dimensioni fisse e non crescono mai. Di conseguenza, il registro contiene solo una certa quantità di voci e le vecchie voci vengono continuamente espulse dal registro man mano che vengono aggiunte nuove voci. Se la conservazione dei log è un problema per un'organizzazione, i log possono essere copiati su un altro server con syslog dove possono essere mantenuti in modo permanente o ruotati con meno frequenza. Vedere Registrazione remota con Syslog più avanti in questo capitolo per informazioni su syslog.

Nelle normali installazioni complete in cui i registri sono tenuti su disco, vengono mantenuti attraverso i riavvii. Per le installazioni NanoBSD o quando /var si trova in un disco RAM, i registri vengono ripristinati al momento dell'avvio.

24.1.1 Visualizzare I registri di sistema

I registri di sistema possono essere trovati in **Stato>Registri di sistema**, nella scheda **Sistema**. Ciò includerà le voci di registro generate dall'host stesso oltre a quelle create da servizi e pacchetti che non hanno i loro registri reindirizzati ad altre schede/file di registro.

Come mostrato dalle voci di esempio nella figura *Esempio delle voci di registro di sistema*, ci sono voci di registro da diverse aree nel registro di sistema principale. Molti altri sottosistemi registreranno qui, ma la maggior parte non sovraccaricherà i registri in una sola volta. In genere, se un servizio ha molte voci di registro, verrà spostato nella propria scheda e nel file di registro.

Aug 5 18:15:57	avahi-daemon[38307]: Found user 'avahi' (UID 1003) and group 'avahi' (GID 1003).
Aug 5 18:15:41	avahi-daemon[44110]: Leaving mDNS multicast group on interface em0.IPv4 with address 192.168.10.1.
Aug 5 18:15:41	avahi-daemon[44110]: Leaving mDNS multicast group on interface tun0.IPv4 with address 192.168.100.2.
Aug 5 18:15:41	avahi-daemon[44110]: Got SIGTERM, quitting.
Aug 5 18:15:32	sshd[38258]: Accepted password for admin from 192.168.10.10 port 64864 ssh2
Aug 5 01:01:02	php: : phpDynDNS: No Change In My IP Address and/or 25 Days Has Not Past. Not Updating Dynamic DNS Entry.
Aug 5 01:01:02	php: : DynDns: Cached IP: 72.69.194.6
Aug 5 01:01:02	php: : DynDns: Current WAN IP: 72.69.194.6
Aug 5 01:01:02	php: : DynDns: _detectChange() starting.
Aug 5 01:01:02	php: : DynDns: updatedns() starting
Aug 5 01:01:02	php: : DynDns: Running updatedns()

Fig. 1: Esempio delle voci di registro di sistema

Filtraggio delle voci di registro

Ogni registro può essere cercato e filtrato per trovare le voci corrispondenti a un modello specificato. Questo è molto utile per rintracciare i messaggi di registro da un servizio specifico o voci di registro contenenti un nome utente specifico, indirizzo IP e così via.

Per cercare le voci di registro:

- Passare a **Stato>Registri di sistema** e quindi alla scheda per il registro da cercare
- Fare clic su  nella barra delle scorciatoie per aprire il pannello **Filtro di registro avanzato**
- Immettere i criteri di ricerca, ad esempio, inserire del testo o un'espressione regolare nel campo **Messaggio**
- Fare clic su  **Applicare filtro**

I campi di filtraggio variano a seconda della scheda di registro, ma possono includere:

I campi di filtraggio variano a seconda della scheda di registro, ma possono includere:

> **Messaggio** Il corpo del messaggio di registro stesso. Una parola o una frase possono essere inseriti per abbinare esattamente, o utilizzare espressioni regolari per abbinare modelli complessi. **Orario** Il timestamp del messaggio di registro. Utilizza nomi del mese abbreviati in tre lettere. **Processo** Il nome del processo o del demone che genera i messaggi di registro, ad esempio sshd o check_reload_status. **PID** Il numero ID del processo di un comando o daemon in esecuzione. Nei casi in cui sono presenti più copie di un demone in esecuzione, ad esempio openvpn, utilizzare questo campo per isolare i messaggi da una singola istanza. **Quantità** Il numero di corrispondenze da restituire nei risultati del filtro. L'impostazione di questo valore superiore al numero di voci di registro nel file di registro non avrà alcun effetto, ma l'impostazione superiore al valore di visualizzazione corrente mostrerà temporaneamente più messaggi di registro.

La scheda del registro di Firewall ha un diverso set di campi di filtraggio:

> **Indirizzo IP di sorgente** L'indirizzo IP di sorgente elencato nella voce di registro. **Indirizzo IP di destinazione** L'indirizzo IP di destinazione elencato nella voce di registro. **Pass** Seleziona questa opzione per abbinare solo le voci di registro che hanno superato il traffico. **Block** Selezionare questa opzione per abbinare solo le voci di registro che hanno bloccato il traffico. **Interfaccia** Il nome descrittivo facile da utilizzare dell'interfaccia per la corrispondenza (ad esempio WAN, LAN, OPT2, DMZ) **Porta sorgente** La porta sorgente della voce di registro da abbinare, se il protocollo utilizza le porte. **Porta di destinazione** La porta di destinazione della voce di registro da corrispondere, se il protocollo utilizza le porte

Protocollo Il protocollo da abbinare, come TCP, UDP o ICMP. **Flag di protocollo** Per TCP, questo campo corrisponde ai flag TCP nella voce di registro, ad esempio SA (SYN+ACK) o FA (FIN + ACK)

Il riquadro del filtro è nascosto per impostazione predefinita, ma può essere incluso nella pagina in ogni momento controllando il filtro di registro in Sistema>Configurazione generale.

24.1.2 Cambiare le impostazione di registro

Le impostazioni del registro possono essere regolate in due modi diversi. Innanzitutto, le opzioni possono essere impostate globalmente in **Stato>Registro di sistema** nella scheda **Impostazioni**. In secondo luogo, ogni scheda di registro può avere le proprie impostazioni univoche che sovrascrivono i valori predefiniti globali. Per modificare queste impostazioni, fare clic su  nella barra delle scorciatoie durante la visualizzazione di un registro. Ciascuno di questi metodi sarà spiegato in dettaglio in questa sezione.

L'area delle opzioni globali contiene più opzioni rispetto alle impostazioni per registro. Solo le differenze saranno trattate in dettaglio per le impostazioni per registro.

Impostazioni globali del registro

Le opzioni di registro globali in **Stato>Registro di sistema** nella scheda **Impostazioni** includono:

Visualizzazione avanti/indietro per impostazione predefinita i registri vengono visualizzati nel loro ordine naturale con le voci più vecchie in alto e le voci più recenti in basso. Alcuni amministratori preferiscono vedere le voci più recenti in alto, l'ordine può essere invertito selezionando questa casella.

Voci di registro della GUI Il numero di voci di registro da visualizzare nelle schede di registro della GUI per impostazione predefinita. Questo non limita il numero di voci nel file, solo ciò che viene mostrato sulla pagina al momento. Il valore predefinito è 50. I file di registro effettivi possono contenere molto più del numero di righe da visualizzare, a seconda delle dimensioni del file di registro.

Dimensione del file di registro (byte) La dimensione del file clog. La dimensione del file controlla direttamente quante voci può contenere. La dimensione predefinita del registro è di circa 500.000 byte (500KB). Ci sono circa 20 file di log, quindi qualsiasi aumento delle dimensioni del file si tradurrà in un utilizzo totale del disco dai registri 20 volte maggiore. La dimensione totale del registro corrente e lo spazio su disco rimanente vengono visualizzati per riferimento. Alla dimensione predefinita, i registri conterranno in media circa 2500 voci, ma potrebbero essere significativamente più o meno a seconda delle dimensioni delle singole voci di registro.

> **Avvertimento:** la nuova dimensione del registro non avrà effetto fino a quando un registro non viene eliminato o reinizializzato. Questo può essere fatto individualmente da ogni scheda di registro o può essere fatto per tutti i registri utilizzando il  Reset

Registrare i pacchetti dalle regole di blocco predefinite Selezionata per impostazione predefinita. Quando abilitata, la regola di negazione predefinita, che blocca il traffico non corrispondente ad altre regole, registrerà le voci nel registro del firewall. In genere queste voci di registro sono utili, ma in alcuni casi d'uso rari possono produrre voci di registro indesiderate rese ridondanti da regole di blocco personalizzate con registrazione abilitata.

Registrare i pacchetti dalle regole di passaggio predefinite Deselezionata per impostazione predefinita. Quando impostata, la registrazione si verificherà per i pacchetti che corrispondono alle regole di svalutazione predefinite sulle interfacce in Firew4LL. L'impostazione di questa opzione genererà una grande

quantità di dati di registro per le connessioni in uscita dal firewall. Si consiglia di abilitarla solo per brevi periodi di tempo durante l'esecuzione della risoluzione dei problemi o della diagnostica.

Registrare i pacchetti dalle regole delle reti bogon bloccate Selezionata per impostazione predefinita. Una volta selezionata, se un'interfaccia è attiva nelle **reti bogon bloccate**, verranno registrati i pacchetti corrispondenti a tale regola. Deselezionare per disabilitare la registrazione.

Registrare i pacchetti dalle regole delle reti private bloccate Selezionata per impostazione predefinita. Una volta selezionata, se un'interfaccia è attiva per le **reti private bloccate**, verranno registrati i pacchetti corrispondenti a tale regola. Deselezionare per disabilitare la registrazione.

Registro del server Web Una volta selezionato, i messaggi di log dal processo della Gui del Web, nginx, verranno inseriti nel registro di sistema principale. A volte, specialmente con il portale captive attivo, questi messaggi possono essere frequenti ma irrilevanti e ingombrare il contenuto del registro.

Registri grezzi Quando selezionata, questa impostazione disabilita l'analisi dei log, visualizzando il contenuto grezzo dei log. I registri grezzi contengono più dettagli, ma sono molto più difficili da leggere. Per molti registri, impedisce anche alla GUI di mostrare colonne separate per il processo e il PID, lasciando tutte quelle informazioni contenute nella colonna del **messaggio**.

Proxy IGMP Alterna la verbosità dei log del proxy IGMP. Per impostazione predefinita, i registri non contengono molte informazioni. L'attivazione di questa opzione fa sì che il proxy IGMP registri più dettagli.

Mostrare le descrizioni delle regole Controlla se e dove la visualizzazione del registro firewall mostrerà le descrizioni delle regole che hanno attivato le voci. La visualizzazione delle descrizioni delle regole causa un sovraccarico di elaborazione aggiuntivo che può rallentare la visualizzazione del registro, specialmente nei casi in cui la vista è impostata per mostrare un numero elevato di voci.

Non caricare le descrizioni Di default corrente. Quando selezionata questa scelta non visualizzerà alcuna descrizione delle regole. La descrizione può ancora essere visualizzata facendo clic sull'icona della colonna delle azioni nella vista del registro firewall.

Mostrare come colonna Aggiunge la descrizione della regola in una colonna separata. Questo funziona meglio se le descrizioni sono brevi o il display è ampio.

Mostrare come seconda riga Aggiunge una seconda riga a ciascuna voce del registro firewall contenente la descrizione della regola. Questa scelta è migliore per le descrizioni delle regole lunghe o per i display stretti.

Suggerimento: Se i registri del firewall vengono visualizzati lentamente con le descrizioni delle regole abilitate, selezionare *Non caricare le descrizioni* per prestazioni più rapide.

Registrazione locale Quando selezionata, i registri locali non vengono mantenuti. Non sono scritti su disco né sono conservati in memoria. Mentre questo sia salva sia scrive su disco e richiede l'uso della registrazione remota in modo che le informazioni non vengano perse. Non è consigliabile utilizzare questa opzione poiché avere registri locali è vitale per la stragrande maggioranza dei casi d'uso.

Resettare i file di registro Questo pulsante cancellerà i dati da tutti i file di log e li reinizializzerà come nuovi, svuotando i registri. Questo deve essere fatto dopo aver modificato le dimensioni del file di registro e può anche essere utilizzato per cancellare informazioni irrilevanti/vecchie dai registri, se necessario.

> **Avvertimento:** Reimpostare i file di registro non salverà le altre opzioni sulla pagina. Se le opzioni di questa pagina sono state modificate, fare clic su Salvare prima di tentare di reimpostare i file di registro.

Fare clic su **Salvare** per memorizzare le nuove impostazioni. Le restanti opzioni in questa schermata sono discusse nella *Registrazione remota con Syslog*.

Impostazioni per registro

Per modificare le impostazioni per registro, visitare la scheda log per modificare e quindi fare clic su  nella barra delle scorciatoie per espandere il pannello Impostazioni.

Su questo pannello vengono visualizzate diverse opzioni. La maggior parte delle opzioni mostrerà il valore predefinito globale o avrà una scelta di **impostazioni generali delle opzioni di registrazione** che utilizzerà il valore globale e non il valore per registro.

Il pannello Impostazioni per registro per ogni scheda Visualizza solo le opzioni relative a tale registro. Ad esempio, le opzioni per registrare le regole di blocco o passaggio predefinite vengono visualizzate solo quando si visualizza la scheda Registro Firewall.

Ogni pannello Impostazioni per registro ha almeno le seguenti opzioni: **Visualizzazione avanti/indietro**, **Voci di log GUI**, **Dimensione file di log (byte)** e **visualizzazione formattata/grezza**. Per ognuno di questi, può essere impostato un valore che si applicherà solo a questo registro. Per ulteriori informazioni su come funzionano queste opzioni, vedere *Impostazioni globali del registro* sopra.

Fare clic su Salva per memorizzare le nuove impostazioni di registro.

Nota: Se la dimensione del file di registro è stata modificata, dopo il salvataggio, aprire nuovamente il pannello Impostazioni e fare clic sul pulsante  **Cancellare il registro** per ripristinare il registro utilizzando la nuova dimensione.

24.2 Registrazione remota con Syslog

Le opzioni di **registrazione remota** in **Stato>Registri di sistema** nella scheda **Impostazioni** consentono a syslog di copiare le voci di registro su un server remoto.

I registri tenuti da Firew4LL sul firewall stesso sono di dimensioni finite e vengono cancellati al riavvio su NanoBSD. La copia di queste voci su un server syslog può aiutare la risoluzione dei problemi e abilitare il monitoraggio a lungo termine. Avere una copia remota può anche aiutare a diagnosticare gli eventi che si verificano prima che un firewall si riavvii o dopo che sarebbero stati altrimenti persi a causa della cancellazione dei registri o quando le voci più vecchie vengono ripetute fuori dal registro e nei casi in cui la memoria locale è fallita ma la rete rimane attiva.

Avvertimento: Le politiche legislative aziendali o locali possono dettare la lunghezza dei registri di tempo perché devono essere conservati da firewall e dispositivi simili. Se un'organizzazione richiede una conservazione del registro a lungo termine per scopi propri o governativi, è necessario un server syslog remoto per ricevere e conservare questi registri

Per avviare la registrazione in remoto:

- Passare a **Stato>Registri di sistema** nella scheda **Impostazioni**
- Selezionare **Inviare messaggi di log al server syslog remoto**
- Selezionare le opzioni come segue:

Indirizzo sorgente Controlla dove il demone syslog si lega per l'invio di messaggi. Nella maggior parte dei casi, l'opzione predefinita (*qualsiasi*) è l'opzione migliore, quindi il firewall utilizzerà l'indirizzo più vicino alla destinazione. Se il server di destinazione si trova in una VPN di IPsec, tuttavia, la scelta di un'interfaccia o di un indirizzo IP virtuale all'interno della rete locale di Fase 2 consentirà ai messaggi di log di fluire correttamente su un tunnel.

Protocollo IP Quando si sceglie un'interfaccia per l'**indirizzo di sorgente**, questa opzione dà al demone syslog una preferenza per l'utilizzo di IPv4 o IPv6, a seconda di quale sia disponibile. Se non esiste un indirizzo corrispondente per il tipo selezionato, viene utilizzato invece l'altro tipo.

Server di log remoti Inserire fino a tre server remoti utilizzando le caselle contenute in questa sezione. Ogni server remoto può utilizzare un indirizzo IP o un hostname e un numero di porta opzionale. Se la porta non è specificata, si assume la porta di syslogd predefinita, 514.

Un server syslog è in genere un server direttamente raggiungibile dal firewall Firew4LL su un'interfaccia locale. La registrazione può anche essere inviata a un server attraverso una VPN.

> **Avvertimento:** Non inviare i dati di registro direttamente attraverso qualsiasi connessione WAN o link sito-a-sito non crittografato, in quanto è testo semplice e potrebbe contenere informazioni sensibili.

Contenuti di syslog da remoto Le opzioni in questa sezione controllano quali messaggi di log verranno inviati al server di log remoto.

Tutto Quando impostato, tutti i messaggi di registro di tutte le aree vengono inviati al server.

Eventi di sistema I principali messaggi di registro di sistema che non rientrano in altre categorie.

Eventi del DNS Messaggi del registro del firewall in formato raw. Il formato del registro raw è riportato nell'articolo wiki della documentazione sul formato del log del filtro

Eventi DNS Messaggi dal risolutore del DNS (unbound), dal forwarder del DNS (dnsmasq), e dal demone filterdns che risolve periodicamente i nomi host in alias.

Eventi DHCP Messaggi dai demoni DHCP con IPv4 e IPv6, agenti del relay e client.

Eventi PPP Messaggi dal client della WAN di PPP (PPPoE, L2TP, PPTP)

Eventi del captive portal Messaggi dal sistema del portale captive, in genere messaggi di autenticazione ed errori.

Eventi VPN Messaggi da demoni VPN come IPsec e OpenVPN, così come il server L2TP e server PPPoE.

Eventi dei gateway da monitorare Messaggi dal daemon, dpinger, del gateway da monitorare

Eventi del demone del routing Messaggi relativi al routing come annunci del routing IPv6, UPnP/NAT-PMP, da pacchetti come OSPF, BGP e RIP.

Eventi del bilanciamento del carico del server Messaggi da relayd che gestisce il bilanciamento del carico del server.

Eventi del protocollo dell'orario di rete Messaggi dal demone NTP e client.

Eventi wireless Messaggi dal demone AP del Wireless, hostapd.

- Fare clic su Salvare per memorizzare le modifiche.

Se un server syslog non è già disponibile, è abbastanza facile configurarne uno. Vedere *Server di syslog su Windows con Kiwi Syslog* per informazioni sulla configurazione di Kiwi Syslog su Windows. Quasi tutti i sistemi Unix o simili a UNIX possono essere utilizzati come server syslog. FreeBSD è descritto nella seguente sezione, ma altri potrebbero essere simili.

24.2.1 Configurazione di un server Syslog su FreeBSD

L'impostazione di un server syslog su un server FreeBSD richiede solo un paio di passaggi. In questo esempio, sostituire 192.168.1.1 con l'indirizzo IP del firewall, sostituire exco-rtr con l'hostname del firewall e sostituire exco-rtr.example.com con l'hostname completo e il dominio del firewall. Questo esempio utilizza 192.168.1.1 perché la migliore pratica è quella di inviare messaggi syslog utilizzando l'indirizzo interno di un firewall, non un'interfaccia WAN.

Nota: Queste modifiche devono essere apportate sul server di syslog, non sul firewall.

Innanzitutto, il firewall avrà probabilmente bisogno di una voce /etc/hosts contenente l'indirizzo e il nome del firewall:

192.168.1.1 exco-rtr exco-rtr.example.com

Quindi regolare i flag di avvio per syslogd per accettare i messaggi di syslog dal firewall. Modificare /etc/rc.conf e aggiungere questa riga se non esiste, o aggiungere questa opzione alla riga esistente per l'impostazione:

syslogd_flags=» -a 192.168.1.1»

Infine, aggiungere le linee a /etc/syslog.conf per catturare le voci di registro da questo host. Sotto qualsiasi altra voce esistente, aggiungere le seguenti righe:

```
!*
```

+* +exco-rtr . /var/log/exco-rtr.log

Queste righe ripristineranno i filtri del programma e dell'host, quindi imposteranno un filtro host per questo firewall utilizzando il nome breve inserito in /etc/hosts.

Suggerimento: Guardare /etc/syslog.conf f sul firewall Firew4LL per idee sul filtraggio dei log per vari servizi in file di log separati sul server syslog.

Dopo queste modifiche, syslogd deve essere riavviato. Su FreeBSD questo è un semplice comando:

```
# service syslogd restart
```

Ora guardare il file di registro sul server syslog e se la configurazione è corretta, popolerà i registri con voci sull'attività sul firewall.

24.3 Dashboard

La pagina principale del firewall è la **dashboard**. La pagina dashboard fornisce una vasta gamma di informazioni che possono essere viste a colpo d'occhio, contenute nei widget configurabili. Questi widget possono essere aggiunti o rimossi e trascinati in posizioni diverse.

24.3.1 Gestione dei widget

Ogni widget segue alcune convenzioni di base per il controllo della sua posizione, dimensione, impostazioni e così via, i cui meccanismi sono coperti qui in questa sezione.

Aggiunta e rimozione di widget

Per iniziare ad aggiungere widget, fare clic sul pulsante nell'area controlli della dashboard della barra delle scorciatoie per visualizzare l'elenco dei widget disponibili. Vedere *Controlli della dashboard nella barra delle scorciatoie*.

All'interno del pannello **Widget disponibili**, Fare clic sul nome di un widget per aggiungerlo alla Dashboard (vedere *Elenco dei widget disponibili*). La dashboard ricaricherà con il nuovo widget visualizzato in una delle sue colonne.

Per chiudere e rimuovere un widget dalla dashboard, fare clic sul pulsante nella sua barra del titolo, come si vede nella figura Barra del titolo del widget, quindi fare clic su nei controlli dashboard.

Fig. 2: Controlli della dashboard nella barra delle scorciatoie

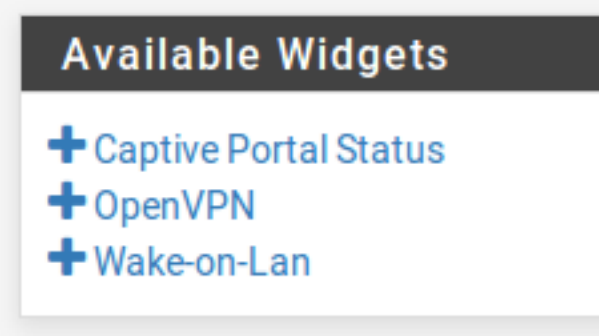


Fig. 3: Elenco dei widget disponibili

Riorganizzare i widget

I widget possono essere riorganizzati e spostati tra le colonne. Per spostare un widget, fare clic e trascinare la barra del titolo (figura *Barra del titolo dei widget*), Spostare il mouse nella posizione desiderata, e quindi rilasciare. Quando il widget viene spostato «scatterà» nella sua nuova posizione, in modo che la nuova posizione possa essere visualizzata in anteprima prima di rilasciare il pulsante del mouse. Dopo aver posizionato un widget, fare clic su nei controlli della dashboard (*Controlli del dashboard nella barra delle scorciatoie*).

Fig. 4: Barra del titolo dei widget

Ridurre al minimo i widget

Per ridurre al minimo un widget in modo che nasconde il suo contenuto e si presenta solo come la sua barra del titolo, fare clic sul pulsante nella sua barra del titolo, come si vede nella figura *Barra del titolo dei widget*. Per

ripristinare il widget al suo normale display, fare clic sul pulsante  . Dopo aver modificato lo stato del widget, fare clic su  nei controlli della dashboard (*Controlli della dashboard nella barra delle scorciatoie*).

Modifica delle impostazioni del widget

Alcuni widget hanno impostazioni personalizzabili che controllano come il loro contenuto viene visualizzato o aggiornato. Se un widget ha impostazioni, il pulsante  apparirà nella sua barra del titolo come si vede nella figura *Barra del titolo dei widget*. Fare clic su quel pulsante e appariranno le impostazioni per il widget. Una volta che le impostazioni sono state regolate, fare clic sul pulsante **Salvare** all'interno del pannello delle impostazioni widget.

24.3.2 Widget disponibili

Ogni widget contiene un insieme specifico di dati, tipo di informazioni, grafico, ecc. Ciascuno dei widget attualmente disponibili sarà coperto in questa sezione, insieme con le loro impostazioni (se presenti). Questi sono elencati in ordine alfabetico.

Stato del captive portal

Questo widget mostra l'elenco corrente degli utenti del captive portal online, inclusi il loro indirizzo IP, indirizzo MAC e nome utente.

Stato del CARP

Il widget dello stato del CARP visualizza un elenco di tutti gli indirizzi IP virtuali di tipo CARP, insieme al loro stato come MASTER o BACKUP.

DNS dinamico

Il widget del DNS dinamico visualizza un elenco di tutti i nomi host del DNS dinamico configurati, il loro indirizzo corrente e lo stato.

Gateway

Il widget del gateway elenca tutti i gateway di sistema insieme al loro stato attuale. Le informazioni di stato sono costituite dall'indirizzo IP del gateway, dal tempo di andata e ritorno (Round Trip Time, RTT) noto anche come ritardo o latenza, dalla quantità di perdita di pacchetti e dallo stato (online, avviso, down o raccolta di dati). I widget vengono aggiornati ogni pochi secondi tramite AJAX.

Stato di Gmirror

Questo widget mostrerà lo stato di un array del RAID del gmirror sul sistema, se uno è configurato. Il widget mostrerà se l'array è online/OK (completo), in ricostruzione o degradato.

Pacchetti installati

Il widget dei pacchetti installati elenca tutti i pacchetti installati sul sistema, insieme ad alcune informazioni di base su di essi, come la versione installata e se è disponibile o meno un aggiornamento.

Quando un pacchetto ha un aggiornamento disponibile,  viene visualizzato accanto al numero di versione. I pacchetti possono essere aggiornati da questo widget facendo clic sul pulsante  alla fine della riga di un pacchetto.

I pacchetti possono anche essere reinstallati facendo clic su  o rimossi facendo clic su  .

Statistiche dell'interfaccia

Questo widget mostra una griglia, con ogni interfaccia sul sistema mostrato nella propria colonna. Varie statistiche di interfaccia sono mostrati in ogni riga, tra cui pacchettio, byte, e conteggi di errore.

Interfacce

Il widget **interfacce** differisce dal widget delle **statistiche di interfaccia** in quanto visualizza informazioni generali sull'interfaccia piuttosto che contatori. Il widget delle **interfacce** mostra il tipo e il nome di ciascuna interfaccia, l'indirizzo IPv4, l'indirizzo IPv6, lo stato del collegamento dell'interfaccia (up o down), nonché la velocità del collegamento quando disponibile.

IPsec

Il widget IPsec ha tre schede: la prima scheda, **Panoramica**, è un conteggio di tunnel attivi e inattivi. la seconda scheda, **Stato del tunnel**, elenca ogni tunnel IPsec configurato e se quel tunnel è up o down. L'ultima scheda, **Mobile**, mostra gli utenti della VPN IPsec di accesso remoto online, come quelli che utilizzano IKEv2 o Xauth.

Stato del bilanciamento del carico

Questo widget visualizza una vista compatta della configurazione di bilanciamento del carico del server. Ogni riga mostra lo stato di un server virtuale. La colonna **Server** mostra il nome del server virtuale, lo stato e l'indirizzo IP con la porta in cui il server virtuale accetta le connessioni. La colonna **Pool** mostra i singoli server pool e il loro stato, con una percentuale di uptime. La colonna **Descrizione** mostra la descrizione del testo dal server virtuale.

Log del firewall

Il widget dei **registri del firewall** fornisce una vista dell'aggiornamento di AJAX del registro firewall. Il numero di righe mostrate dal widget è configurabile. Come per la normale vista del registro firewall, facendo clic sull'icona azione accanto alla voce di registro verrà visualizzata una finestra che mostra quale regola ha causato la voce di registro. Facendo clic sull'indirizzo IP di sorgente o di destinazione, tale valore verrà copiato in **Diagnostica>DNS** in cui è possibile risolvere l'indirizzo.

Stato NTP

Il widget dello **stato di NTP** mostra la sorgente di sincronizzazione NTP corrente e l'ora del server da tale fonte.

OpenVPN

Il widget di **OpenVPN** visualizza lo stato di ogni istanza OpenVPN configurata, sia per i server che per i client. Viene mostrato lo stato di ogni istanza, ma lo stile e il tipo di informazioni mostrate variano a seconda del tipo di connessione OpenVPN. Ad esempio, i server basati su SSL/TLS mostrano un elenco di tutti i client connessi. Per i client e i server delle chiavi statiche, viene visualizzato uno stato up/down. In ogni caso viene visualizzato l'indirizzo IP del client di connessione con il nome e l'ora della connessione.

Immagine

Il widget immagine, come suggerisce il nome, visualizza un'immagine scelta dall'utente. Questo può essere utilizzato funzionalmente, per un diagramma di rete o simile, oppure può essere per lo stile, la visualizzazione di un logo aziendale o altra immagine.

Per aggiungere un'immagine:

- Fare clic su  sulla barra del titolo del widget immagine
- Fare clic su **Sfogliare** per individuare l'immagine da caricare
- Fare clic su **Caricare** per caricare l'immagine

La dimensione dell'immagine si adatterà all'area del widget, che può variare a seconda delle dimensioni del browser e della piattaforma.

RSS

Il widget RSS (Rdfsite Summary, o come viene spesso chiamato, sindacazione davvero semplice) visualizzerà un feed RSS arbitrario. Per impostazione predefinita, mostra il feed RSS del blog Firew4LL. Alcune persone scelgono di mostrare i feed RSS aziendali interni o i feed RSS del sito di sicurezza, ma possono caricare qualsiasi feed RSS.

Oltre a definire i feed RSS da visualizzare, il numero di storie e le dimensioni del contenuto visualizzato sono anche configurabili.

Stato dei servizi

Questo widget fornisce la stessa vista e il controllo dei servizi che appare in **Stato>Servizi**. Ogni servizio è elencato insieme alla sua descrizione, stato (esecuzione, arresto) e controlli avvio/riavvio/arresto.

Stato intelligente

Se S.M.A.R.T. è abilitato su un'unità nel firewall, questo widget mostrerà un breve stato dell'integrità dell'unità come riportato da S.M.A.R.T.

Informazioni di sistema

Questo widget è il widget principale, la visualizzazione di una vasta gamma di informazioni sul sistema in esecuzione. Le informazioni visualizzate includono:

- **Nome** L'hostname completamente qualificato configurato del firewall.
- **Versione** La versione corrente in esecuzione di Firew4LL sul firewall. La versione, l'architettura e il tempo di compilazione vengono visualizzati in alto. Sotto il tempo di compilazione, viene mostrata la versione sottostante di FreeBSD.

Sotto questi elementi è il risultato di un controllo di aggiornamento automatico per una versione più recente di Firew4LL (solo installazioni complete). Questo controllo di aggiornamento automatico può essere disabilitato nelle impostazioni di aggiornamento.

- **Piattaforma** La piattaforma indica quale variazione di Firew4LL è in esecuzione. Un'installazione completa mostrerà Firew4LL, un'installazione incorporata mostra NanoBSD.
- **Porzione di avvio di NanoBSD** Se si tratta di un'installazione incorporata, viene visualizzata anche la porzione in esecuzione (|*firew4ll|0* o |*firew4ll|1*), insieme alla porzione che verrà utilizzata per il prossimo avvio.
- **Tipo di CPU** Il tipo di CPU visualizzato è la stringa di versione per il processore, ad esempio "Intel(R) Atom(TM) CPU C2758 @ 2.40 GHz". Viene visualizzato anche il conteggio della CPU e il layout pacchetto/core.

  Se **powerd** è attivo e la frequenza della CPU è stata abbassata, la frequenza corrente viene mostrata lungo la dimensione della frequenza massima.
- **Crittografia dell'hardware** Se è stato rilevato un acceleratore crittografico hardware noto, verrà visualizzato qui.
- **Uptime** Questo è il momento in cui il firewall è stato riavviato l'ultima volta.
- **Data/ora corrente** La data e l'ora correnti del firewall, compreso il fuso orario. Questo è utile per confrontare le voci di registro, specialmente quando il fuso orario sul firewall è diverso da dove risiede l'utente.
- **Server DNS** Elenca tutti i server DNS configurati sul firewall.
- **Ultima modifica di configurazione** La data dell'ultima modifica di configurazione sul firewall.
- **Dimensione della tabella di stato** Mostra una rappresentazione grafica e numerica degli stati attivi e degli Stati possibili massimi configurati sul firewall. Sotto i conteggi di stato c'è un collegamento per visualizzare il contenuto della tabella di stato.
- **Utilizzo di MBUF** Mostra il numero di cluster del buffer di memoria di rete in uso e il massimo che il sistema ha a disposizione. Questi buffer di memoria di rete vengono utilizzati per le operazioni di rete, tra le altre attività. Se il numero è vicino al massimo o al massimo, aumentare il numero di Mbuf disponibili come descritto nella *sintonizzazione Hardware e risoluzione dei problemi*.
- **Carico medio** Un conteggio di quanti processi attivi sono in esecuzione sul firewall durante gli ultimi 5, 10 e 15 minuti. Questo è in genere 0,00 su un sistema inattivo o leggermente caricato.
- **Utilizzo della CPU** Un grafico a barre e la percentuale di tempo della CPU in uso dal firewall. Si noti che la visualizzazione della dashboard aumenterà un po" l'utilizzo della CPU, a seconda della piattaforma. Su piattaforme più lente come ALIX è probabile che questo sia significativamente più alto di quanto sarebbe altrimenti.
- **Utilizzo della memoria** La quantità corrente di RAM in uso dal sistema. Si noti che la RAM inutilizzata viene spesso allocata per la cache e altre attività, quindi non viene sprecata o è inattiva, quindi questo numero potrebbe essere più alto del previsto anche se funziona normalmente.
- **Utilizzo di swap** La quantità di spazio di swap in uso da parte del sistema. Se il sistema esaurisce la RAM fisica e c'è spazio di swap disponibile, le pagine di memoria meno utilizzate verranno salvate nel file di swap sul disco rigido. Questo indicatore mostra solo quando il sistema ha configurato lo spazio di swap, che sarà solo su installazioni complete.
- **Utilizzo del disco** La quantità di spazio utilizzato sul disco di avvio o sul supporto di archiviazione. Vengono visualizzati il tipo e la posizione dei filesystem montati, inclusi i dischi di memoria quando presenti.

Sensori termici

Il widget dei sensori termici visualizza la temperatura dai sensori supportati quando presente. Per molti popolari chip basati su Intel e AMD, I sensori possono essere attivati scegliendo il tipo di sensore appropriato in **Sistema>Avanzate** nella scheda **Varie** sotto **sensori termici**

Viene visualizzata una barra per ciascun sensore, che in genere corrisponde a ciascun core della CPU. Le soglie di avviso e critiche possono essere configurate nelle impostazioni del widget.

Grafici del traffico

Il widget dei grafici del traffico contiene un grafico SVG dal vivo per il traffico su ogni interfaccia. Le interfacce visualizzate sono configurabili nelle impostazioni del widget. La frequenza di aggiornamento predefinita dei grafici è una volta ogni 10 secondi, ma può anche essere regolata nelle impostazioni per questo widget. I grafici sono disegnati allo stesso modo di quelli trovati nel grafico del traffico di stato.

Attivare la LAN

Il widget dell'attivazione della LAN mostra tutte le voci WOL configurate in servizi Attivare la LAN e offre un mezzo rapido per inviare il pacchetto magico a ciascun sistema per riattivarlo. Viene anche mostrato lo stato corrente di un sistema. Per riattivare un sistema, fare clic su  accanto alla sua voce.

24.4 Stato dell'interfaccia

Lo stato delle interfacce di rete può essere visualizzato in **Stato>Interfacce**. Nella prima parte della figura *Stato dell'interfaccia*, è stata effettuata una connessione WAN di DHCP e l'indirizzo IPv4 e IPv6, DNS, ecc. L'indirizzo MAC, il tipo di supporto, i pacchetti in/out, gli errori e le collisioni per l'interfaccia di rete sono tutti visibili. I tipi di connessione dinamica come PPPoE e PPTP hanno un pulsante **Disconnettere** quando è collegato e un pulsante **Connettere** quando è offline. Le interfacce che ottengono un indirizzo IP da DHCP hanno un pulsante **Rilasciare** quando c'è un lease attivo e un pulsante **Rinnovare** quando non c'è.

Nella parte inferiore dell'immagine, la connessione LAN è visibile. Poiché si tratta di un'interfaccia normale con un indirizzo IP statico, viene mostrato solo il solito set di elementi.

Se uno stato dell'interfaccia indica «nessun vettore», significa in genere che il cavo non è collegato o che il dispositivo sull'altra estremità non funziona correttamente in qualche modo. Se vengono visualizzati errori, in genere sono di natura fisica: errori di cablaggio o di porta. Il sospetto più comune sono i cavi che sono facili ed economici da sostituire. In alcune circostanze possono comparire errori e collisioni a causa di una velocità di collegamento o di una mancata corrispondenza duplex. Vedere *Velocità e duplex* per ulteriori informazioni su come impostare la velocità e il duplex di un'interfaccia.

24.5 Stato servizio

Molti servizi di sistema e pacchetti mostrano lo stato dei loro demoni in **Stato>Servizi**.

Ogni servizio viene visualizzato con un nome, una descrizione e lo stato, come si vede nella figura Stato dei servizi. Lo stato è elencato come **in esecuzione** o **arrestato**.

Normalmente, non è necessario controllare i servizi in questo modo, ma occasionalmente ci sono motivi di manutenzione o risoluzione dei problemi per farlo.

Da questo punto di vista, i servizi possono essere controllati in vari modi:

- Fare clic su  per riavviare un servizio in esecuzione
- Fare clic su  per interrompere un servizio in esecuzione
- Fare clic su  per avviare un servizio interrotto

Se disponibile, vengono visualizzate altre scorciatoie che passano a una configurazione del servizio (), a una pagina di stato dettagliata () o ai registri (). Vedere *Navigare rapidamente nella GUI con le scorciatoie* per saperne di più sulle icone di scelta rapida.

24.6 Grafici di monitoraggio

Il firewall raccoglie e mantiene i dati su come il sistema funziona, e quindi memorizza questi dati nei file di database Round-Robin (Rrd) file. I grafici creati da questi dati sono disponibili in **Stato>Monitoraggio**.

Il grafico in quella pagina può essere configurato per mostrare elementi di diverse categorie e una categoria e un grafico possono essere scelti sia per l'asse sinistro che per l'asse destro per un facile confronto.

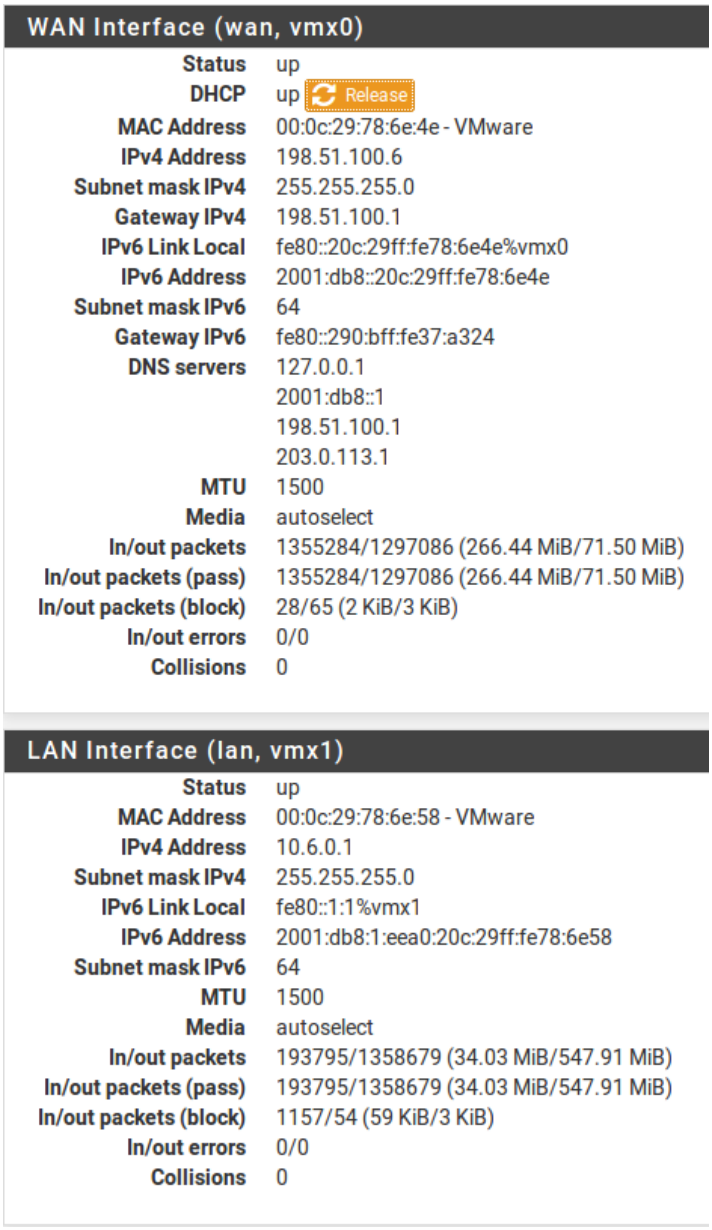


Fig. 5: Stato dell'interfaccia

Services

Service	Description	Status	Actions
bsnmpd	SNMP Service	Running	
dhcpd	DHCP Service	Running	
dnsmasq	DNS Forwarder	Running	
dpinger	Gateway Monitoring Daemon	Running	
ipsec	IPsec VPN	Running	
miniupnpd	UPnP Service	Running	
ntpd	NTP clock sync	Running	
openvpn	OpenVPN server: Vendor Remote Access Server	Running	
openvpn	OpenVPN server: Satellite Offices	Running	
openvpn	OpenVPN server: New York Office Site-to-Site	Running	
openvpn	OpenVPN server: Employee Remote Access Server	Running	
radvd	Router Advertisement Daemon	Running	
relayd	Server load balancing daemon	Running	
sshd	Secure Shell Daemon	Running	

Fig. 6: Stato dei servizi

24.6.1 Lavorare con i grafici

Il firewall visualizza un grafico che mostra il suo utilizzo della CPU per impostazione predefinita. Per visualizzare altri grafici o aggiungere una seconda categoria su un altro asse, le impostazioni del grafico devono essere modificate come descritto nella sezione successiva, *Impostazioni del grafico*.

All'interno del grafico, le etichette nell'angolo in alto a sinistra annotano le fonti per i dati nell'asse sinistro e nell'asse destro.

Il grafico contiene una legenda in alto a destra con ciascuna delle fonti di dati tracciate sul grafico. Fare clic su una fonte dei dati nella legenda la nasconderà dalla vista.

Suggerimento: Se una fonte dei dati ha un picco grande, fare clic sul suo nome nella legenda per rimuoverlo dal grafico. Con l'origine dei dati più grande rimossa, saranno visibili maggiori dettagli dalle altre fonti rimanenti.

L'hostname del firewall, il periodo di tempo del grafico e la risoluzione del grafico vengono stampati lungo la parte inferiore del grafico, insieme al tempo in cui è stato generato il grafico.

Il firewall stampa una tabella sotto il grafico stesso con un riepilogo dei dati. Questa tabella contiene minimi, medie, massimi, valori correnti, in alcuni casi il 95° percentile. Nei casi in cui vengono fornite unità, il puntatore del mouse sopra l'unità visualizzerà una descrizione più dettagliata dell'unità.

Nota: I totali non vengono visualizzati perché per il modo in cui i dati vengono memorizzati nei file RRD, i totali accurati non sono possibili. Per visualizzare l'utilizzo totale del traffico sulle interfacce di rete, installare il pacchetto dei **totali del traffico dello stato**.

La figura *Grafico del traffico della WAN* mostra un esempio di un grafico di traffico di 8 ore su un'interfaccia firewall denominata *CABLE* con inverso abilitato. L'interfaccia ha un utilizzo massimo di 9,96 Mbit/s durante un periodo di 1 minuto.

24.6.2 Impostazioni dei grafici

Per modificare il grafico, fare clic su  sulla barra delle scorciatoie per visualizzare il pannello delle impostazioni del grafico.

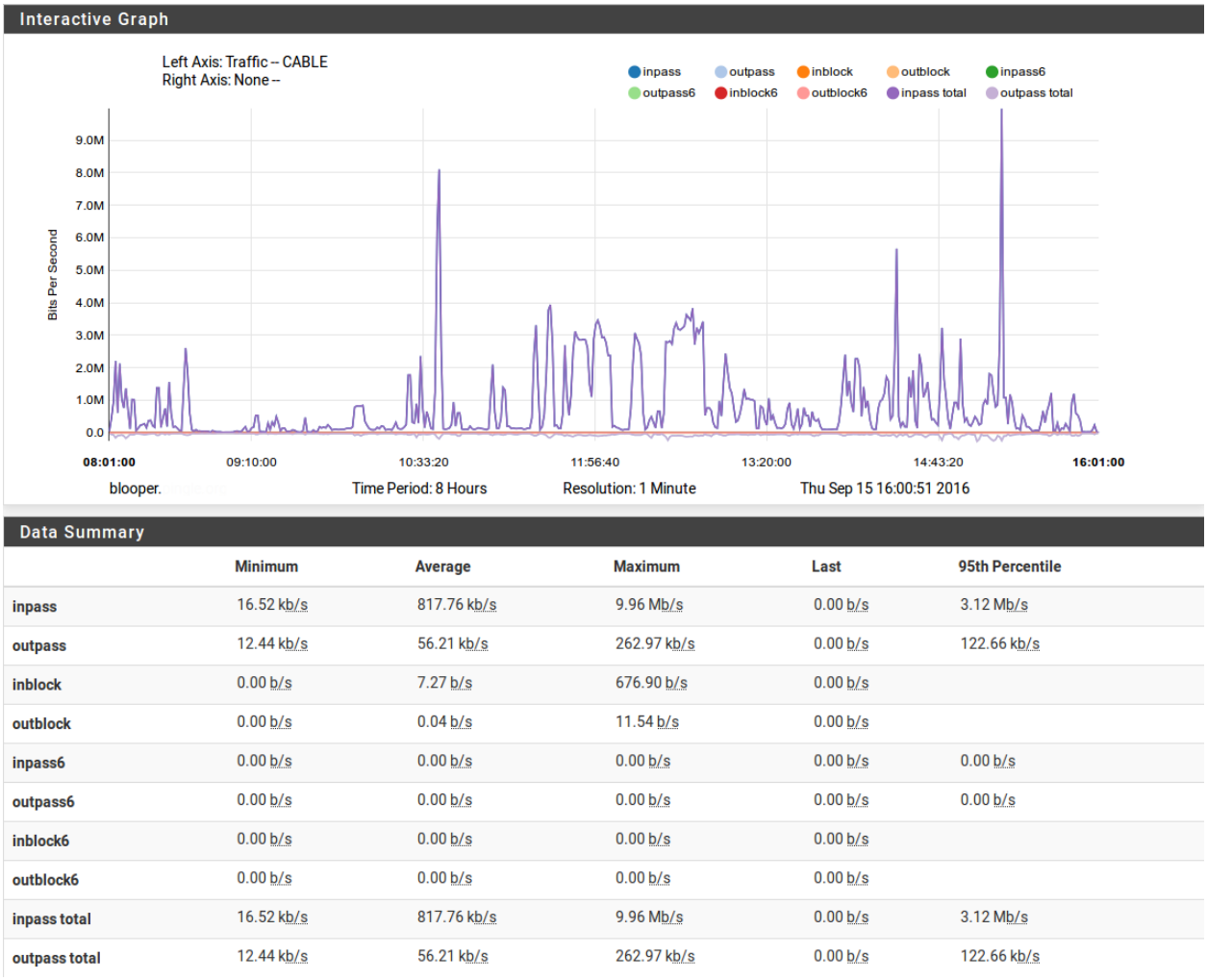
Suggerimento: Il pannello delle impostazioni del grafico è nascosto per impostazione predefinita, ma questo comportamento può essere modificato. Passare a **Sistema>Configurazione generale** e controllare le impostazioni di monitoraggio per visualizzare sempre il pannello delle impostazioni di default.

Le opzioni del pannello impostazioni sono:

Asse sinistro/asse destro Le opzioni qui controllano i dati disponibili su ciascun asse. Per impostazione predefinita, solo **l'asse sinistro** viene popolato con un valore, ma entrambi possono essere utilizzati per confrontare le aree. Prima scegliere una **categoria** (o *nessuna*), quindi scegliere un **grafico** all'interno di quella categoria. L'elenco delle categorie e dei grafici disponibili varia a seconda della configurazione del firewall.

Categoria L'area generale del grafico desiderato: sistema, traffico, pacchetti, qualità, portale captice, NTP, Code, QueueDrops, DHCP, cellulare, wireless e utenti VPN. Questi sono trattati in modo più dettagliato più avanti in questa sezione.

Grafico Il grafico specifico da visualizzare dalla categoria scelta.



Data Summary

	Minimum	Average	Maximum	Last	95th Percentile
inpass	16.52 kb/s	817.76 kb/s	9.96 Mb/s	0.00 b/s	3.12 Mb/s
outpass	12.44 kb/s	56.21 kb/s	262.97 kb/s	0.00 b/s	122.66 kb/s
inblock	0.00 b/s	7.27 b/s	676.90 b/s	0.00 b/s	
outblock	0.00 b/s	0.04 b/s	11.54 b/s	0.00 b/s	
inpass6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s
outpass6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s
inblock6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	
outblock6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	
inpass total	16.52 kb/s	817.76 kb/s	9.96 Mb/s	0.00 b/s	3.12 Mb/s
outpass total	12.44 kb/s	56.21 kb/s	262.97 kb/s	0.00 b/s	122.66 kb/s

Fig. 7: Grafico del traffico della WAN

Opzioni Questa sezione del pannello delle impostazioni controlla l'aspetto del grafico stesso, inclusi l'intervallo di tempo e lo stile.

Periodo di tempo Il periodo di tempo da mostrare sul grafico. Gli intervalli predefiniti coprono da 1 ora fino a 4 anni o può essere scelto un periodo *personalizzato*. Selezionando *personalizzato* vengono visualizzati i controlli del **periodo personalizzato**. Tutti i periodi vengono visualizzati anche se non ci sono dati in un database grafico che risale a quel punto. Il grafico sarà vuoto per le volte in cui il grafico non era attivo.

Risoluzione La più piccola porzione di tempo per la quale i dati sono disponibili su questo grafico. Nel corso del tempo, i dati sono consolodati su periodi più lunghi in modo che la risoluzione venga persa. Ad esempio, su un grafico di 1 ora è possibile vedere i dati da intervalli di un minuto, ma su un grafico di un'ora che include dati più vecchi, non è possibile mostrare i dati con precisione poiché è stata calcolata la media. A seconda del periodo di tempo del grafico può contenere *1 minuto*, *5 minuti*, *1 ora* o *1 giorno* medi per i dati. Le risoluzioni che non sono possibili per un determinato periodo di tempo non possono essere selezionate.

Inverso Utilizzato su grafici come il grafico del traffico, per separare i dati in entrata e in uscita. Ad esempio, con **inverso** impostato su *On*, I dati in uscita sono rappresentati come un valore negativo per differenziarlo più facilmente dai dati in entrata.

Periodo personalizzato Quando il **periodo di tempo** è impostato su *personalizzato*, la GUI visualizza questa sezione per configurare il periodo di tempo personalizzato per il grafico.

Data di inizio La data di inizio del grafico. Facendo clic nel campo verrà visualizzato un controllo di raccolta della data del calendario. Solo oggi, o i giorni in passato, possono essere selezionati.

Ora d'inizia L'ora del giorno per iniziare il grafico usando lo stile di 24 ore (0-23)

Data di fine La data di fine per il grafico.

Ora di fine L'ora di fine per il grafico, esclusivo. L'ora scelta non è inclusa nel grafico. Ad esempio, su un grafico a partire dalle ore 10 alle ore 12, il grafico copre dalle 10:00 am alle 12:00 pm.

Impostazioni Fare clic su  **Mostrare avanzate** per visualizzare ulteriori controlli avanzati non in genere necessari per l'uso medio.

Esporta come CSV Fare clic su questo pulsante per scaricare i dati dal grafico come un file di foglio di calcolo .csv (Valori separati da virgole, Comma Separated Values), che può quindi essere importato in un altro programma per l'analisi.

Salvare come predefinito Fare clic su questo pulsante per memorizzare le impostazioni del grafico corrente come configurazione predefinita, in modo che questo grafico specifico venga visualizzato di default nelle visite future a questa pagina.

Disabilitare/Abilitare la rappresentazione grafica Questo interruttore disabiliterà o abiliterà la raccolta dei dati del grafico. La grafica è abilitata per impostazione predefinita. Normalmente questo sarebbe disabilitato solo per scopi diagnostici o se tutta la grafica richiesta viene gestita esternamente.

Resettare i dati della rappresentazione grafica Fare clic su questo pulsante cancellerà tutti i file di database del grafico e creerà nuovi file vuoti.

Fare clic su  **Aggiornare grafici** per modificare il grafico nella vista selezionata.

24.6.3 Elenco delle categorie dei grafici

Esistono diverse categorie di dati del grafico che il firewall può tracciare. Ogni categoria è coperta qui, ma non tutte le categorie saranno visibili su ogni firewall. Alcuni grafici devono essere abilitati separatamente o saranno presenti solo se è abilitata una caratteristica specifica o un pezzo di hardware.

Grafici di sistema

I grafici della categoria *Sistema* mostrano una panoramica generale dell'utilizzo del sistema, incluso l'utilizzo della CPU, l'utilizzo della memoria e gli stati del firewall.

Cluster di Mbuf

Il grafico dei **cluster di Mbuf** traccia l'utilizzo del cluster del buffer di memoria di rete del firewall. I firewall con molte interfacce, o molti core e NIC della CPU che utilizzano una coda di interfaccia per core, possono consumare un gran numero di buffer di memoria di rete. Nella maggior parte dei casi, questo utilizzo sarà abbastanza piatto, ma a seconda delle varie circostanze, come un carico elevato inutilizzato, i valori potrebbero aumentare. Se l'utilizzo si avvicina al massimo configurato, aumentare il numero di buffer.

Vedi anche:

Fare riferimento a *Sintonizzazione dell'hardware e risoluzione dei problemi* per informazioni su come aumentare la quantità di mbuf disponibili per il sistema operativo.

Il grafico del **cluster Mbuf** contiene le seguenti fonti di dati:

Corrente Il numero corrente di cluster Mbuf consumati

Cache Il numero di cluster Mbuf memorizzati nella cache

Totale Il totale di Corrente e Cache

Massimo Il numero massimo consentito di cluster mbuf

Grafico Della Memoria

Il grafico della **memoria** mostra l'utilizzo della RAM di sistema suddiviso utilizzando le seguenti fonti di dati:

Attiva La quantità di memoria attiva (in uso)

Inattiva La quantità di memoria inattiva, che era in uso, ma potrebbe essere riassegnata.

Libera La quantità di memoria libera, che non viene utilizzata affatto.

Cache La quantità di memoria utilizzata per la memorizzazione nella cache dal sistema operativo.

Cablata La quantità di memoria cablata, in genere la memoria del kernel

---

Nota: Il sistema operativo tenterà di utilizzare la RAM quanto possibile per la cache piuttosto che permettergli di rimanere inattivo, quindi la quantità di RAM libera apparirà spesso inferiore al previsto. Se la domanda di memoria aumenta, la memoria memorizzata nella cache sarà resa disponibile per l'uso.

Grafico del processore

Il grafico del processore mostra l'utilizzo della CPU per il firewall utilizzando le seguenti fonti di dati:

Utilizzo dell'utente La quantità di tempo del processore consumata dai processi utente.

Utilizzo buono La quantità di tempo del processore consumato dai processi con un'alta priorità.

Utilizzo del sistema La quantità di tempo del processore consumata dal sistema operativo e dal kernel.

Interruzioni La quantità di tempo del processore consumata dalla gestione degli interrupt, che sta elaborando input e output dell'hardware, comprese le interfacce di rete.

Processi Il numero di processi in esecuzione.

Grafico degli stati

Il grafico degli stati mostra il numero di stati di sistema, ma suddivide anche il valore in diversi modi.

Cambiamenti di stato Il numero di cambiamenti di stato al secondo, o «churn». Un valore elevato da questa fonte indicherebbe un rapido numero di connessioni nuove o in scadenza.

Stati del filtro Il numero totale di voci di stato nella tabella stati.

Indirizzi di sorgente Il numero di indirizzi IP sorgente univoci attivi.

Indirizzi di destinazione Il numero di indirizzi IP di destinazione univoci attivi.

Grafici del traffico

I grafici del traffico mostrano la quantità di larghezza di banda utilizzata su ogni interfaccia disponibile in bit al secondo. L'elenco dei grafici contiene le voci per ogni interfaccia assegnata, così come IPsec e singoli client e server OpenVPN.

Il grafico del traffico è suddiviso in diverse fonti di dati. A parte il totale, ognuno ha un equivalente IPv4 e IPv6. Le origini dati IPv6 hanno 6 aggiunto al nome.

inpass Il tasso di traffico che entra in questa interfaccia che è *passato* nel firewall.

outpass Il tasso di traffico in partenza da questa interfaccia che è *passato* fuori dal firewall.

inblock Il tasso di traffico che tenta di raggiungere questa interfaccia che è stato *bloccato* dall'accesso al firewall.

outblock Il tasso di traffico che tenta di lasciare questa interfaccia che è stato *bloccato* dal lasciare il fiewall.

inpass totale Il tasso totale di traffico (IPv4 e IPv6) passato in entrata.

outpass totale Il tasso totale di traffico (IPv4 e IPv6) passato in uscita.

Nota: I termini «inbound» e" outbound » su questi grafici sono dal punto di vista del firewall stesso. Su un'interfaccia esterna come una WAN, il traffico "in entrata" è il traffico che arriva al firewall da Internet e il traffico "in uscita" è il traffico che lascia il firewall verso una destinazione su Internet. Per un'interfaccia interna, come LAN, il traffico"in entrata" è il traffico che arriva al firewall da un host sulla LAN, probabilmente destinato a una posizione su Internet e il traffico "in uscita" è il traffico che lascia il firewall andando a un host sulla LAN.

Grafici dei pacchetti

I grafici del pacchetto funzionano molto come i grafici del traffico e hanno gli stessi nomi per le fonti dei dati, tranne che invece di segnalare in base alla larghezza di banda utilizzata, riporta il numero di *pacchetti al secondo* (pps) passati. L'elenco dei **grafici** contiene le voci per ogni interfaccia assegnata, così come IPsec e i singoli client e server OpenVPN.

Pacchetti al secondo (pps) è una metrica migliore per giudicare le prestazioni hardware rispetto al throguhput del traffico in quanto riflette più accuratamente quanto bene l'hardware gestisce i pacchetti di qualsiasi dimensione. Un circuito può essere venduto su un certo livello di larghezza di banda, ma è più probabile che l'hardware sia strozzato dall'incapacità di gestire un grande volume di piccoli pacchetti. In situazioni in cui l'hardware è il fattore limitante, il grafico dei **pacchetti** può mostrare un altopiano alto o picchi mentre il grafico del traffico mostra l'utilizzo sotto la velocità nominale della linea.

Grafici della qualità

La categoria **Qualità** contiene le voci del **grafico** che tracciano la qualità delle interfacce WAN o simile alle WAN, come le interfacce con un gateway specificato o quelle che utilizzano DHCP o PPPoE. Il firewall contiene una voce di **grafico** per gateway, compresi i gateway configurati in precedenza, ma non esistono più. I file di dati del grafico per i vecchi gateway non vengono rimossi automaticamente in modo che i dati storici siano disponibili per riferimento futuro.

Le seguenti orfonti di dati vengono utilizzate per monitorare l'affidabilità del gateway:

Perdita di pacchetti La percentuale di tentati ping all'indirizzo IP da monitorare che sono stati persi. La perdita sul grafico indica problemi di connettività o tempi di utilizzo eccessivo della larghezza di banda in cui i ping sono stati eliminati.

Ritardo medio Il ritardo medio (Tempo di andata e ritorno, RTT) sui ping inviati all'indirizzo IP da monitorare. Un alto RTT significa che il traffico sta prendendo molto tempo per fare il viaggio di andata e ritorno dal firewall per l'indirizzo IP da monitorare e ritorno. Un RTT alto potrebbe provenire da un problema sul circuito o da un elevato utilizzo.

Ritardo di deviazione standard La deviazione standard sui valori RTT. La deviazione standard dà un'impressione della variabilità della RTT durante un determinato periodo di calcolo. Una bassa deviazione standard indica che la connessione è relativamente stabile. Una deviazione standard elevata significa che il RTT sta fluttuando su e giù su una vasta gamma di valori, il che potrebbe significare che la connessione è instabile o molto occupata.

Captive Portal

La categoria **captive portal** contiene le voci del **grafico** per ogni zona del captive portal, passato e presente. I file di dati del grafico per le vecchie zone non vengono rimossi automaticamente.

Simultanea La scelta del grafico *simultaneo* mostra quanti utenti sono registrati in un determinato punto nel tempo. Quando gli utenti si disconnettono o le loro sessioni scadono, questo conteggio andrà giù. Un gran numero di utenti simultanei non causerà necessariamente uno sforzo sul portale, ma può essere utile per giudicare le esigenze generali di capacità e la larghezza di banda.

Accesso Il grafico degli *accessi* mostra il numero di eventi di accesso che si verificano durante ogni intervallo di polling. Questo è utile per giudicare quanto sia occupato il demone del captive portal in un dato momento. Un gran numero di utenti che accedono allo stesso tempo metterà più stress sul demone del portale rispetto agli accessi che sono sparsi nel corso di una giornata.

NTP

Il grafico **NTP** visualizza le statistiche relative al servizio NTP e alla qualità dell'orologio. Questo grafico è disabilitato per impostazione predefinita perché non è rilevante per la maggior parte dei casi d'uso. Il grafico può essere abilitato in **Servizi>NTP**. In quella pagina, controllare **Abilitare grafici RRD di statistiche NTP**.

Vedi anche:

Per ulteriori informazioni su questi valori, consultare il manuale di configurazione di NTP, il manuale delle query di NTP e le specifiche di NTPv4.

Offset Differenza di clock combinata tra dal server rispetto a questo host.

Jitter di sistema (sjit) Jitter di sistema combinato, che è una stima dell'errore nel determinare l'offset.

Jitter del clock (cjit) Jitter calcolato dal modulo di disciplina dell'orologio.

Giro del clock (wander) Stabilità della frequenza di clock espressa in parti per milione (PPM)

Offset di frequenza (freq) Offset relativo all'orologio dell'hardware (in PPM)

Dispersione della root (disp) differenza totale tra l'orologio locale e l'orologio di riferimento primario in tutta la rete.

Grafici di coda/Codadue della coda (Queuedrops)

I grafici della coda sono un composito di ogni coda di shaper del traffico. Viene mostrata ogni singola coda, rappresentata da un colore unico.

La categoria **Code** mostra l'utilizzo individuale della coda in byte.

La categoria **QueueDrops** mostra un conteggio di cadute di pacchetti da ogni coda.

DHCP

La categoria **DHCP** contiene un grafico per ogni interfaccia con un server DHCP abilitato. Le fonti dei dati mostrate per DHCP sono:

Locazioni Il numero di leasing in uso fuori dall'intervallo DHCP configurato per l'interfaccia.

Locazioni statiche Il numero di lease di mappatura statica configurati per l'interfaccia.

Intervallo DHCP La dimensione totale del pool DHCP disponibile per l'uso sull'interfaccia.

Se il conteggio delle **locazioni** si avvicina al valore dell'**intervallo**, potrebbe essere necessario un pool più grande per l'interfaccia. Le mappature statiche esistono al di fuori dell'intervallo, quindi non tengono conto della quantità di locazioni consumate nel pool.

Cellulare

Su alcuni dispositivi 3G/4G, il firewall è in grado di raccogliere dati di potenza del segnale per il grafico cellulare. La potenza del segnale è l'unico valore tracciato sul grafico.

Wireless

La categoria **Wireless** è presente su sistemi contenenti un dispositivo di rete wireless 802.11 abilitato e in uso come client (infrastruttura, modalità BSS). Le seguenti fonti di dati vengono raccolte e visualizzate quando si agisce come client wireless:

SNR Il rapporto segnale-rumore per l'AP a cui è collegato il client.

Canale Il numero di canale wireless utilizzato per raggiungere l'AP.

Tasso La velocità dei dati wireless per l'AP.

Utenti di VPN

La categoria degli **utenti VPN** mostra il numero di utenti OpenVPN registrati contemporaneamente per ogni singolo server OpenVPN.

24.7 Stati firewall

Firew4LL è un *firewall stateful* e utilizza uno stato per monitorare ogni connessione da e verso il firewall. Questi stati possono essere visualizzati in diversi modi nella WebGUI e dalla console.

24.7.1 Visualizzazione nella WebGUI

Un elenco dei contenuti della tabella dello stato del firewall è disponibile nella WebGUI navigando in **Diagnostica>Stati**. La figura *Esempio di stati* mostra un esempio dell'output visualizzato dalla GUI.

WAN	tcp	198.51.100.6:37246 -> 162.208.119.39:443	TIME_WAIT:TIME_WAIT	91 / 89	6 KiB / 120 KiB	
LAN	tcp	10.6.0.114:49266 -> 52.88.223.32:443	ESTABLISHED:ESTABLISHED	248 / 244	18 KiB / 20 KiB	
WAN	tcp	198.51.100.6:55087 (10.6.0.114:49266) -> 52.88.223.32:443	ESTABLISHED:ESTABLISHED	248 / 244	18 KiB / 20 KiB	
WAN2	icmp	203.0.113.106:36339 -> 203.0.113.1:36339	0:0	832.827 K / 921	22.26 MiB / 25 KiB	

Fig. 8: Esempio di stati

Il firewall visualizza diverse colonne in questa pagina, ognuna con informazioni importanti:

Interfaccia L'interfaccia a cui è associato lo stato. Questa è l'interfaccia attraverso la quale il pacchetto inizialmente è entrato o è uscito dal firewall.

Protocollo Il protocollo del traffico che ha creato lo stato, come TCP, UDP, ICMP o ESP.

Sorgente e destinazione Questa colonna è in due parti, prima la sorgente, poi una freccia che indica la direzione, e quindi la destinazione. La sorgente e la destinazione possono anche avere un numero di porta elencato se il protocollo in questione utilizza le porte. Nei casi in cui viene applicato il NAT (NAT in uscita, porta forward o NAT 1: 1), l'indirizzo viene mostrato sia prima che dopo l'applicazione di NAT.

Per il NAT, come il NAT in uscita, che traduce la sorgente, la sezione sorgente visualizza la sorgente modificata e la sorgente originale tra parentesi. Per i tipi NAT che traducono la destinazione, come la porta forward, la sezione destinazione mostra la destinazione tradotta e la destinazione originale tra parentesi.

Stato Lo stato corrente della connessione monitorata da questa voce di stato. I valori specifici variano a seconda del protocollo. Ad esempio, TCP ha molti più tipi di stato rispetto a UDP o altri protocolli senza connessione. La voce in questa colonna contiene due parti separate da due punti. La prima parte è lo stato per il lato sorgente e la seconda parte è lo stato per il lato di destinazione. Vedere *interpretazione degli stati* per maggiori dettagli.

Pacchetti Il numero di pacchetti osservati corrispondenti allo stato dai lati di sorgente e destinazione.

Byte La dimensione totale dei pacchetti osservati corrispondenti allo stato dai lati di sorgente e destinazione.

I singoli stati possono essere rimossi facendo clic su alla fine della loro riga.

Stati di filtraggio

Il pannello **filtro di stato** consente una rapida ricerca del contenuto della tabella di stato per trovare elementi di interesse. Per cercare uno stato:

- Selezionare un'**interfaccia** specifica nel pannello **filtro di stato** o lasciarla su *tutto* per abbinare tutte le interfacce.
- Immettere un'**espressione di filtro** che è una semplice stringa di testo da abbinare esattamente nella voce. Le espressioni regolari non sono supportate in questo campo.
- Fare clic su **Filtro** per individuare i risultati.

Tutte le colonne vengono ricercate per il testo corrispondente e vengono visualizzate solo le voci corrispondenti al testo.

Suggerimento: La ricerca di un indirizzo IP o di una sottorete presenterà anche un pulsante  **Eliminare gli stati** che, una volta cliccato, rimuoverà tutti gli stati originati o che andranno all'indirizzo IP o alla sottorete inseriti.

Interpretazione degli stati

La colonna di **Stato** per ogni voce Della tabella di stato fornisce le informazioni necessarie per determinare esattamente ciò che sta accadendo con la connessione. Ogni voce di stato contiene due valori con due punti tra di loro, che segnano quale valore rappresenta lo stato della sorgente (a sinistra) e la destinazione (a destra).

Alcuni dei tipi di stato più comuni sono:

SYN_INVIATO Per le connessioni TCP, questo indica che il lato che mostra questo stato ha inviato un pacchetto SYN di TCP tentando di avviare un handshake di connessione.

CHIUSO Per le connessioni TCP, il lato con questo stato considera la connessione chiusa o non è stato ricevuto alcun traffico.

STABILITO Una connessione TCP è considerata pienamente stabilita da questo lato.

TEMPO DI ATTESA/ATTESA DI FINE Una connessione TCP è in fase di chiusura e finitura.

NESSUN TRAFFICO Non sono stati ricevuti pacchetti che corrispondono allo stato da questo lato.

SINGOLO Un singolo pacchetto è stato osservato su questo stato da questo lato.

MULTIPLI Più pacchetti sono stati osservati su questo stato da questo lato.

Abbinamenti comuni trovati spesso nella tabella di stato includono:

STABILITO:STABILITO Una connessione TCP bidirezionale completamente stabilita.

SYN_INVIATO:CHIUSO Il lato che mostra *SYN_INVIATO* ha inviato un pacchetto SYN di TCP ma nessuna risposta è stata ricevuta dal lato lontano. Spesso ciò è dovuto al fatto che il pacchetto non raggiunge la sua destinazione o viene bloccato lungo la strada.

SINGOLO:NESSUN TRAFFICO Simile a quanto sopra, ma per UDP e altri protocolli senza connessione. Nessuna risposta è stata ricevuta dal lato di destinazione.

SINGOLO:MULTIPLO Per UDP e altri protocolli senza connessione, comunemente osservati con DNS in cui il client invia un pacchetto ma riceve una grande risposta in più pacchetti.

MULTIPLO:MULTIPLO Per UDP e altri protocolli senza connessione, ci sono più pacchetti in entrambe le direzioni, il che è normale per una connessione UDP completamente operativa.

0:0 Indica che non ci sono dati a livello di stato. In genere si trova solo negli stati ICMP, poiché ICMP non ha livelli di stato come altri protocolli.

24.7.2 Riepilogo degli stati

Il **riepilogo della tabella di stato**, accessibile da **Diagnostica>Riepilogo degli stati**, fornisce statistiche generate da un'analisi approfondita della tabella di stato e delle connessioni in essa contenute.

Il report include l'indirizzo IP, un conteggio totale dello stato e guasti per protocollo e porte di sorgente/destinazione. Il passaggio del mouse sopra le porte mostra una visualizzazione tooltip dell'elenco completo delle porte anziché il numero totale di porte. A seconda dell'ambiente firewall, i valori elevati di qualsiasi metrica possono essere normali.

Il rapporto comprende le seguenti categorie:

Per indirizzo IP di sorgente Stati riassunti dall'indirizzo IP di sorgente. Questo è utile per trovare una potenziale fonte di attacco, o una scansione porta o tipo simile a sonda/attacco.

Per indirizzo IP di destinazione Stati riassunti dall'indirizzo IP di destinazione della connessione. Utile per trovare l'obiettivo di un attacco o identificare i server.

Totale per indirizzo IP Stati riassunti da tutte le connessioni da o verso un indirizzo IP. Utile per trovare host attivi utilizzando molte porte, come i client BitTorrent.

Per coppia di indirizzi IP Riassume gli stati tra due indirizzi IP coinvolti nelle connessioni attive. Utile per trovare coppie client/server specifiche che hanno un numero insolitamente elevato di connessioni.

> **Avvertimento:** Il riepilogo degli stati può richiedere molto tempo per elaborare e visualizzare, specialmente se il firewall ha una tabella di stato eccezionalmente grande o un processore lento. Nei casi in cui la tabella di stato è estremamente grande, la pagina potrebbe non essere visualizzata correttamente o la pagina potrebbe non riuscire con un errore di memoria. In questi casi, la pagina di riepilogo non può essere utilizzata.

24.7.3 Visualizzazione degli stati con pfTop

pfTop è disponibile dal menu GUI e console di sistema e offre viste live del set di regole del firewall, informazioni sulla tabella di stato e statistiche correlate.

pfTop nella GUI

Nella GUI, pfTop può essere trovato in **Diagnostica>pfTop**. La GUI offre diverse opzioni per controllare l'output:

Vista Controlla il tipo di output visualizzato da pfTop. Non tutte le viste conterranno informazioni significative per ogni configurazione del firewall.

Default Mostra una quantità equilibrata di informazioni, in base alla sorgente e alla destinazione del traffico.

Etichetta Incentrata sulle descrizioni delle regole del firewall.

Lungo Simile alla vista predefinita, ma su misura per i display più ampi con righe più lunghe per più colonne di informazioni. Mostra il gateway dopo la destinazione.

Coda Mostra le code di shapinga del traffico ALTQ e il loro utilizzo.

Regole Mostra le regole del firewall e il loro utilizzo.

Dimensione Mostra gli stati che hanno superato il maggior numero di dati.

Velocità Mostra gli stati che hanno traffico ad alto tasso.

Stato Mostra lo stato degli stati.

Tempo Mostra stati di lunga durata.

Ordina per Alcune viste possono essere ordinate. Quando l'ordinamento è possibile, sono disponibili i seguenti metodi di ordinamento. Quando è selezionata, la vista viene ordinata per la colonna scelta in ordine decrescente:

Nessuno Nessun ordinamento, l'ordine naturale mostrato dalla vista scelta.

Età L'età degli Stati.

Byte La quantità di stati corrispondenti ai dati inviati.

Indirizzo di destinazione L'indirizzo IP di destinazione dello stato.

Porta di destinazione Il numero di porta di destinazione dello stato.

Scadenza Il tempo di scadenza dello stato. Questo è il conto alla rovescia fino a quando lo stato verrà rimosso se non ci sono più dati corrispondenti allo stato.

Picco Il picco di traffico corrispondente a uno stato in pacchetti al secondo.

Pacchetto Il numero di pacchetti trasferiti corrispondenti a uno stato.

Tasso La velocità corrente di traffico corrispondente a uno stato in pacchetti al secondo.

Dimensione La quantità totale di traffico che ha trovato corrispondenza con uno stato.

Porta di sorgente Il numero di porta di sorgente dello stato.

Indirizzo di sorgente L'indirizzo IP di sorgente dello stato.

Numero massimo di stati Nelle viste che supportano l'ordinamento, questa opzione limita il numero di voci di stato mostrate nella pagina.

pfTop sulla console

Per accedere a pfTop dalla console o tramite ssh, utilizzare l'opzione 9 dal menu o eseguire pftop da un prompt della shell.

Durante la visualizzazione di pfTop in questo modo, ci sono diversi metodi per modificare la vista mentre si guarda il suo output. Premere h per visualizzare una schermata di aiuto che spiega le scelte disponibili. Gli usi più comuni sono l'utilizzo da 8 per selezionare viste diverse, lo spazio per un aggiornamento immediato e q per uscire. Vedere la sezione precedente per i dettagli sul significato delle viste disponibili e gli ordinamenti.

L'uscita è dimensionata dinamicamente alla larghezza del terminale, con terminali più larghi che mostrano molte più informazioni in colonne aggiuntive.

24.7.4 Stati di tracciamento della sorgente

Quando si utilizzano **connessioni sticky**, il firewall mantiene una tabella di tracciamento dei sorgenti che registra le mappature degli indirizzi IP interni a gateway esterni specifici per le connessioni passate da una regola che utilizza un gruppo di gateway di bilanciamento del carico (Gateway multipli sullo stesso livello). Per impostazione predefinita, queste associazioni esistono solo finché ci sono stati attivi dall'indirizzo IP interno. C'è un timeout configurabile per queste voci di tracciamento di sorgente per consentire loro di esistere più a lungo, se necessario.

Vedi anche:

Per ulteriori informazioni sulle connessioni sticky e sulle relative opzioni, vedere *Connessioni sticky*.

Le associazioni di tracciamento delle sorgenti sono visualizzate su **Diagnostica>Stati** nella scheda **Tracciamento delle sorgenti**, che è visibile solo se le connessioni sticky sono abilitate.

La pagina di tracciamento di origine elenca le seguenti informazioni:

Sorgente-a-detistinazione La mappatura di un indirizzo IP locale a un gateway con carico bilanciato specifico.

Numero di stati Indica il numero di stati che corrispondono a questo indirizzo IP di sorgente a qualsiasi destinazione, incluso il traffico che non è bilanciato dal carico.

Numero di connessioni Il numero di stati corrispondenti a questo indirizzo IP di sorgente che utilizzano il gateway. Ad esempio, le connessioni che partono da questa fonte a un host Internet.

Tassi Il tasso di pacchetti corrispondenti a questa voce di tracciamento sorgente.

Queste associazioni possono essere rimosse singolarmente facendo clic sul pulsante Rimuovere alla fine di ogni riga.

24.7.5 Reimpostare tabella di stato/tabella di tracciamento sorgente

Alcune situazioni richiedono il ripristino della tabella di stato per forzare la chiusura e il ripristino di tutte le connessioni esistenti. Gli esempi più importanti stanno apportando modifiche alle regole NAT, alle regole del blocco firewall o allo shaping del traffico. Quando vengono effettuati questi tipi di modifiche, il ripristino della tabella di stato è l'unico modo per assicurarsi che tutte le connessioni rispettino il nuovo set di regole o le code dello shaping del traffico.

Sia la tabella di stato che la tabella di tracciamento sorgente possono essere reimpostate da **Diagnostica>Stati** nella scheda **Ripristinare gli stati**. Per reimpostare le tabelle, selezionare **tabella di stato**, **tracciamento sorgente** o entrambi, quindi fare clic su **Ripristinare**.

Avvertimento: Il browser sembra perdere la connessione con il firewall quando si ripristina la tabella di stato. Una volta che il browser si rende conto che la vecchia connessione non è valida, si riconnetterà. Chiudere e riaprire il browser per riconnettersi più velocemente.

24.8 Grafici del traffico

Sono disponibili grafici del traffico in tempo reale disegnati con JavaScript utilizzando NVD3 che si aggiornano continuamente. Questi grafici possono essere visualizzati in **Stato>Grafico del traffico**, e un esempio del grafico può essere trovato in figura *Esempio del grafico della LAN*.

Questi grafici di traffico mostrano il traffico dell'interfaccia in tempo reale e danno una visione chiara di ciò che sta accadendo «ora» piuttosto che basarsi su dati medi dei grafici RRD che sono migliori per le viste a lungo termine.

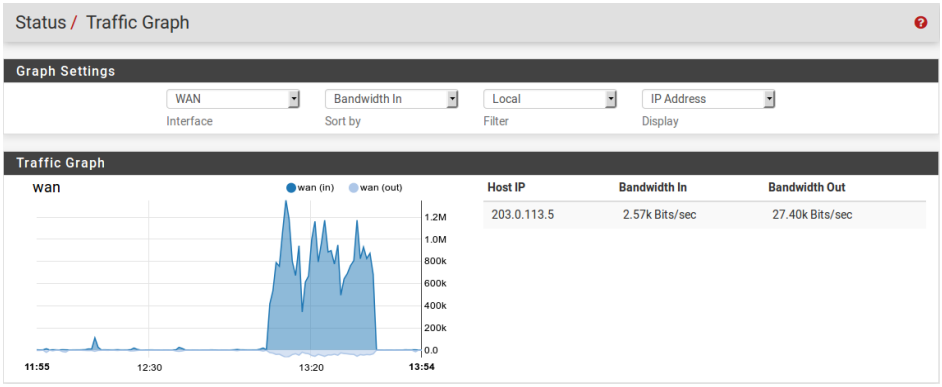


Fig. 9: Esempio del grafico della LAN

Solo un'interfaccia alla volta è visibile e questa interfaccia può essere modificata utilizzando l'elenco a discesa dell'**Interfaccia**. Una volta scelta un'interfaccia, la pagina si aggiorna automaticamente e inizia a visualizzare il nuovo grafico.

Grafici di traffico di stile simile possono anche essere visualizzati sulla dashboard aggiungendo il widget dei **grafici di traffico**. Utilizzando il widget, più grafici di traffico possono essere visualizzati contemporaneamente.

Vedi anche:

Per ulteriori informazioni sulla dashboard, vedere *Dashboard*.

Accanto al grafico del traffico viene visualizzata anche una tabella contenente scorci momentanei di dati che vengono trasferiti da indirizzi IP specifici. Questi sono limitati a essere visualizzati solo brevemente, quindi i trasferimenti in corso hanno maggiori probabilità di apparire rispetto alle connessioni rapide. Inoltre, verrà mostrata solo la connessione dalla sottorete primaria di quell'interfaccia.

La visualizzazione del grafico e della tabella può essere controllata utilizzando le seguenti opzioni:

Interfaccia L'interfaccia firewall da utilizzare come fonte di traffico per il grafico e la tabella.

Ordinamento Seleziona l'ordinamento del grafico, sia *Larghezza di banda In* o *Larghezza di banda Out*.

Filtro Seleziona il tipo di host da visualizzare nella tabella

Locale Mostra solo gli indirizzi IP all'interno della rete di interfaccia

Remoto Mostra solo gli indirizzi IP che non sono all'interno della rete di interfaccia

Tutti Mostra tutti gli indirizzi IP, all'interno e all'esterno della rete di interfaccia

Visualizzare Controlla la visualizzazione della colonna IP dell'host utilizzando una delle seguenti opzioni:

Indirizzo IP L'indirizzo IP dell'host.

Hostname L'hostname breve che corrisponde all'indirizzo IP, come elencato nelle mappature statiche DHCP, nelle sostituzioni host del risolutore del DNS o nelle sostituzioni host del forwarder del DNS.

Descrizione La descrizione che corrisponde all'indirizzo IP, come elencato nelle mappature statiche DHCP, nelle sostituzioni host del risolutore del DNS o nelle sostituzioni host del forwarder del DNS.

FQDN Il nome di dominio completo che corrisponde all'indirizzo IP, come elencato nelle mappature statiche DHCP, nelle sostituzioni host del risolutore del DNS o nelle sostituzioni host del forwarder del DNS.

24.9 Attività sistema (Top)

La pagina **Diagnostica>Attività di sistema** visualizza l'elenco dei principali processi attivi in esecuzione sul firewall. Questo equivale a eseguire il comando Top-aSH in un prompt della shell, tranne che la versione GUI non ha il riepilogo dell'utilizzo della CPU.

Utilizzando questa vista, è facile vedere i processi che consumano la maggior parte della potenza della CPU durante un periodo di carico elevato. Ad esempio, se la voce più alta è una coda di elaborazione di interrupt per una delle schede di rete e il sistema non sta spingendo abbastanza traffico, potrebbe essere un segno che il firewall sta cercando di spingere più di quanto l'hardware possa gestire nella configurazione corrente. Se il processo superiore è un processo PHP, potrebbe essere che un browser abbia richiesto una pagina GUI che sta elaborando una grande quantità di dati

24.10 pfInfo

La pagina **Diagnostica>pfInfo** visualizza statistiche e contatori per il filtro dei pacchetti firewall che servono come metriche per giudicare come si comporta e elabora i dati. Le informazioni mostrate nella pagina contengono elementi quali:

Byte in/out Byte trasferiti dentro e fuori dal firewall.

Pacchetti in/out Pacchetti trasferiti in o out e contatori passati o bloccati per ogni direzione.

Tabella stati/Tabella di tracciamento della sorgente Statistiche sulla tabella di stato e tabella di tracciamento di stato (*Stati del firewall*).

Voci correnti Il numero di voci nella tabella

Ricerche Quante volte la tabella è stata cercata e il tasso corrente di ricerche, che corrisponde approssimativamente al numero di pacchetti passati dal firewall sulle connessioni aperte correnti.

Inserti Il numero di nuovi stati aggiunti alla tabella e la velocità con cui vengono aggiunti gli Stati. Un alto tasso indica che ci sono un sacco di nuove connessioni da effettuare verso o attraverso il firewall.

Rimossi Il numero di vecchi stati rimossi dal firewall.

Contatori Statistiche sui conteggi per vari tipi di pacchetti speciali, insoliti o mal formattati.

Contatori di limiti Contatori relativi a pacchetti che hanno raggiunto o superato i limiti configurati sulle regole del firewall, ad esempio stati massimi per indirizzo IP.

Limiti di dimensione della tabella Dimensione massima della tabella di stato, dimensione della tabella del nodo di origine, dimensione della tabella frag, numero di tabelle consentite e numero massimo di voci della tabella.

Timer di stato I valori di timeout configurati correnti per vari stati di connessione per TCP, UDP e altri protocolli.

Statistiche di interfaccia Contatori di pacchetti per interfaccia.

24.11 Stato del disco rigido S. M. A. R. T.

Il firewall può monitorare lo stato dei dischi rigidi che supportano l'autocontrollo, l'analisi e la tecnologia di resoconto (S.M.A.R.T.). Questo meccanismo ha lo scopo di consentire alle unità di testare e monitorare le proprie prestazioni e affidabilità, con l'obiettivo finale di identificare un'unità in errore prima che subisca la perdita di dati o causi un'interruzione.

Il supporto per S.M.A.R.T. varia in base all'unità e al BIOS, ma è abbastanza ben supportato nei moderni dischi rigidi ATA e SSD.Potrebbe essere necessario abilitare S. M. A. R. T. nel BIOS e sull'unità.

Nota: S.M.A.R.T. non è una metrica perfetta per localizzare un'unità fallita; molte unità che hanno fallito passano ancora un test S.M.A.R.T., ma in generale Se S.M.A.R.T. individua un problema, uno esiste, quindi è utile identificare i guasti del disco.

La pagina **Diagnostica>Stato SMART** ottiene e visualizza informazioni da unità, esegue o interrompe i test di unità e visualizza i registri delle unità.

In ogni sezione della pagina, è necessario selezionare un **dispositivo** prima di scegliere un'opzione. Questo **dispositivo** è il disco da testare da S.M.A.R.T..

Avvertimento: Se un'unità non è elencata tra i dispositivi, non supporta S.M.A.R.T. o è collegata a un controller che non è supportato per questo scopo. Nel caso dei controller RAID, il controller stesso può offrire funzionalità o report simili tramite utilità specifiche del controller nella shell.

24.11.1 Visualizzazione delle informazioni sull'unità

Per visualizzare le informazioni su un'unità:

- Passare a **Diagnostica>Stato SMART**
- Individuare il pannello **Informazioni** sulla pagina

- Selezionare il **dispositivo** da visualizzare
- Selezionare il **tipo di informazioni**
- Fare clic su **Visualizzare**

Dopo aver esaminato l'output, fare clic su **Indietro** per tornare all'elenco delle opzioni.

I tipi di informazioni sono spiegati nelle prossime sottosezioni.

Informazione

L'opzione **Informazioni** mostra informazioni sull'unità stessa, tra cui marca, modello, numero di serie e altre informazioni tecniche sulle funzionalità, la connessione e il funzionamento dell'unità:

Model Family: Hitachi Travelstar 5K500.B Device Model: Hitachi HTS545050B9A300 Serial Number: 090630PB4400XXXXXXXX LU WWN Device Id: 5 000cca 597XXXXXX Firmware Version: PB4OC64G User Capacity: 500,107,862,016 bytes [500 GB] Sector Size: 512 bytes logical/physical Rotation Rate: 5400 rpm Form Factor: 2.5 inches Device is: In smartctl database [for details use: -P show] ATA Version is: ATA8-ACS T13/1699-D revision 6 SATA Version is: SATA 2.6, 3.0 Gb/s Local Time is: Fri Oct 7 16:31:20 2016 EDT SMART support is: Available - device has SMART capability. SMART support is: Enabled

Salute

L'opzione Salute fornisce un breve stato di passato/fallito dell'unità:

SMART overall-health self-assessment test result: PASSED

Funzionalità SMART

La scelta delle **funzionalità SMART** fornisce un report sulle funzionalità e verifica i supporti dell'unità, come in questo output:

General SMART Values: Offline data collection status: (0x00) Offline data collection activity

was never started. Auto Offline Data Collection: Disabled.

Self-test execution status: (0) The previous self-test routine completed without error or no self-test has ever been run.

Total time to complete Offline data collection: (645) seconds. Offline data collection capabilities: (0x5b) SMART execute Offline immediate.

Auto Offline data collection on/off support. Suspend Offline collection upon new command. Offline surface scan supported. Self-test supported. No Conveyance Self-test supported. Selective Self-test supported.

SMART capabilities: (0x0003)Saves SMART data before entering power-saving mode. Supports SMART auto save timer.

Error logging capability: (0x01) Error logging supported. General Purpose Logging supported.

Short self-test routine recommended polling time: (2) minutes. Extended self-test routine recommended polling time: (158) minutes. SCT capabilities: (0x003d)SCT Status supported.

SCT Error Recovery Control supported. SCT Feature Control supported. SCT Data Table supported.

Attributi

La vista **attributi** è la schermata più utile nella maggior parte dei casi, ma può anche essere una delle più difficili da interpretare. Ci sono diversi valori visualizzati, ma il numero e i valori variano ampiamente per marca e modello.

C'è un articolo completo su Wikipedia per S.M.A.R.T. che include una guida per interpretare i valori. Alcuni valori sono più evidenti di altri, ad esempio i conteggi per i settori riallocati dovrebbero essere pari a zero o vicini a zero. Altri possono essere più difficili come il tasso di errore di lettura grezzo, che sulla maggior parte delle unità dovrebbe essere basso, ma ci sono unità Seagate e simili che emettono senza senso o un numero elevato casuale in quel campo che lo rende inutile su quei dischi.

Alcuni dei valori sono informativi, come il conteggio Avvio/Arresto, il conteggio del ciclo di potenza e le ore di accensione che danno un senso dell'età complessiva e dell'utilizzo per l'unità. Un valore elevato non è necessariamente un male per quelli, ma se l'unità è straordinariamente vecchia, o c'è stato un gran numero di cicli di potenza, quindi avere un piano pronto per sostituire il disco in un prossimo futuro. La temperatura dell'unità può dare un'indicazione del suo ambiente e, se la temperatura è troppo alta, può portare a problemi di stabilità.

Il conteggio del ciclo di carico è un valore speciale per i dischi rotanti, poiché indica il numero di volte in cui le teste sono state parcheggiate. Alcune unità portatili parcheggeranno automaticamente le teste dopo un breve periodo di tempo, ma un sistema operativo come Firew4LL vorrà scrivere periodicamente, ciò porta le teste di nuovo fuori. Il parcheggio della testa ha senso solo in un dispositivo mobile che si muove molto in modo che le teste abbiano meno possibilità di influire sul piatto; in una situazione Server/firewall, è completamente inutile. Le unità sono in grado solo di supportare 100.000-300.000 cicli di carico nella loro vita, il che significa che il conteggio viene eseguito rapidamente se le teste sono continuamente parcheggiate e no. Firew4LL tenta di disabilitare le funzionalità di gestione dell'alimentazione dei dischi rigidi al momento dell'avvio perché altrimenti l'unità potrebbe fallire prematuramente dopo aver eseguito questo conteggio in alto. Questo movimento ciclico in atto è in genere udibile su unità come un rumore di clic morbido.

Le metriche mostrate per un SSD possono essere significativamente diverse, come visto sopra. In particolare, gli SSD possono fornire una stima della loro vita residua, scrivere di varie dimensioni, tassi di errore, errori di scrittura e altri valori specifici SSD al posto degli altri valori che non si applicano a un SSD.

Tutto

La selezione di **tutti**, come suggerisce il nome, mostrerà tutte le informazioni di cui sopra e include anche i registri delle unità e i risultati dell'autotest.

24.11.2 Auto-test

Per eseguire un test su un'unità:

- Passare a **Diagnostica>Stato SMART**
- Individuare il pannello **Eseguire autotest** sulla pagina
- Selezionare il **dispositivo** da testare
- Selezionare il **tipo di prova**
- Fare clic su  Testare

I tipi di test sono descritti nelle seguenti sottosezioni.

Offline

Un test **Offline** è chiamato così perché è fatto mentre il disco è inattivo. Questo test può rendere l'accesso all'unità lento mentre sta accadendo, ma se c'è molta attività del disco, l'unità potrebbe ritardare il test fino a quando il disco diventa inattivo di nuovo. A causa di questa variabilità, l'ora esatta del test è difficile da prevedere. Una stima del tempo per completare un test offline per un determinato disco è mostrata nelle **Capacità S.M.A.R.T**. Un test offline farà sì che l'unità aggiorni molti degli attributi S.M.A.R.T. per indicare i risultati. Dopo aver eseguito un test e controllato i risultati, rivedere gli **attributi S.M.A.R.T**. di nuovo così come il registro degli **errori**.

Breve

Il **breve** test dura circa dieci minuti e controlla la meccanica del disco e le prestazioni di lettura. Una stima più accurata della lunghezza che il test assumerà su un disco può essere visto nelle **capacità S.M.A.R.T**.. Per vedere i risultati di questo test, visualizzare i registri di **auto-test**. Può essere eseguito in qualsiasi momento e in genere non influisce sulle prestazioni.

Lungo

Il test **lungo** è simile al test breve ma è più approfondito. Il tempo impiegato dal test dipende dalla dimensione del disco, ma è molto più lungo del test breve da solo. Una stima più accurata della lunghezza che il test assumerà su un disco può essere visto nelle **capacità S.M.A.R.T**.. Come con il test breve, i risultati finiscono nei registri di **auto-test**.

Trasporto

Questo test non è supportato da tutte le unità. Il suo scopo primario è quello di testare l'unità dopo che è stato fisicamente trasferito per determinare se eventuali componenti sono stati danneggiati dal movimento. Nella maggior parte dei casi ci vogliono solo pochi minuti per completare. Per determinare se un'unità supporta un test di trasporto, fare riferimento all'output delle **capacità S.M.A.R.T**.

Annullamento dei test attivi

Per annullare un test attivo su un'unità:

- Passare a **Diagnostica>Stato SMART**
- Individuare il pannello **Interrompere** nella pagina
- Selezionare il **dispositivo** su cui è attualmente in esecuzione un test che deve essere annullato
- Fare clic su  Interrompere

Eventuali test attivi sull'unità verranno interrotti.

1. ### Registri delle unità

   I registri delle unità contengono informazioni ed errori, solitamente correlati agli autotest e potenzialmente ad altri errori riscontrati. Per visualizzare i registri delle unità:

- Passare a **Diagnostica>Stato SMART**
- Individuare il pannello **Visualizzare registri** sulla pagina
- Selezionare il **dispositivo** da visualizzare

- Selezionare il **tipo di registro**
- Fare clic su  Visualizzare

Registro errori Unità

Il registro degli **errori** di un'unità contiene una registrazione degli errori riscontrati durante il funzionamento dell'unità, ad esempio errori di lettura, errori non correggibili, errori CRC e così via. L'esecuzione di un test offline farà anche stampare più errori qui se vengono trovati durante il test.

Registri di autotest

I registri di **autotest** contengono un record di diversi recenti autotest eseguiti sull'unità. Mostra il tipo di test, i risultati del test e, nel caso di test che sono stati fermati prematuramente, mostra la percentuale del test rimanente.

Se si verifica un errore durante un test, viene stampato il primo indirizzo di blocco logico (LBA) per determinare dove si trova il problema nel disco.

24.12 Notifiche SMTP e Growl

Lo stato del sistema può essere segnalato passivamente utilizzando le notifiche SMTP o Growl. Queste notifiche consentono ai client di ricevere avvisi sugli eventi di sistema senza essere connessi al firewall. La configurazione e l'uso di questi meccanismi sono coperti in *notifiche*.

24.13 Visualizzazione del contenuto delle tabelle

Gli alias e altri elenchi simili di indirizzi sono memorizzati in una struttura PF chiamata **Tabella**. Queste tabelle possono essere relativamente statiche, come con l'elenco o gli alias di bogon, o dinamiche per cose come snort o indirizzi IP che superano i limiti di connessione. Un alias diventa una «tabella» una volta caricato nel set di regole del firewall. Le tabelle possono contenere sia indirizzi IPv4 che IPv6 e gli indirizzi appropriati vengono utilizzati in base alle regole in cui si fa riferimento alle tabelle.

Il contenuto di queste tabelle può essere visualizzato in **Diagnostica>Tabelle**, che visualizza le tabelle di sistema e definite dall'utente. In quella pagina, selezionare la **tabella** desiderata dal menu a discesa di tabella e il firewall visualizzerà il suo contenuto. Se un alias contiene un hostname, il contenuto dell'alias viene popolato da DNS. La visualizzazione della tabella risultante qui conferma quali indirizzi IP sono nella tabella in quel momento.

Le singole voci possono essere rimosse facendo clic su  alla fine della riga. Le tabelle definite manualmente o da un file verranno aggiornate quando il sistema esegue una ricarica del filtro, quindi è meglio modificare un alias e rimuovere una voce piuttosto che rimuoverla da questa pagina. La rimozione delle voci è meglio utilizzata per le tabelle dinamiche per rimuovere una voce prima che scada automaticamente.

24.13.1 Tabelle predefinite

Il firewall include diverse tabelle per impostazione predefinita, a seconda delle funzionalità abilitate:

- **bogon/bogonv6** Se un'interfaccia è configurata con *Reti bogon bloccate* attivo, queste tabelle saranno presenti sul firewall. Viene anche presentato un pulsante di aggiornamento  per le tabelle bogon che recupereranno immediatamente i dati bogon anziché attendere il solito aggiornamento mensile.

- **Sottoreti al NAT (tonatsubnets)** Quando si utilizza il NAT automatico in uscita, questa tabella mostra l'elenco delle reti per le quali viene eseguito il NAT automatico in uscita. Ispezionare la tabella può aiutare a diagnosticare problemi NAT difficili per confermare se una sottorete avrà NAT automatico in uscita applicato al suo traffico.
- **snort2c** Una tabella dinamica contenente i trasgressori bloccati da pacchetti IDS/IPS, Snort e Suricata.
- **virusprot** Una tabella dinamica contenente indirizzi che hanno superato i limiti definiti sulle regole del firewall.
- **Blocco del configuratore Web (webConfiguratorlockout)** Una tabella dinamica contenente client per cui hanno ripetutamente fallito i tentativi di accesso alla GUI.
- **Blocco di DDH (Sshlockout)** Simile a webConfiguratorlockout ma utilizzato per il monitoraggio di client a cui non riescono ripetuti tentativi di accesso SSH.

24.14 Testare il DNS

Diagnostica>Ricerca DNS esegue semplici query al DNS forward e inverso per ottenere informazioni su un indirizzo IP o un hostname e anche per testare i server DNS utilizzati dal firewall.

Per eseguire una ricerca DNS:

- Passare a **Diagnostica>Ricerca DNS**
- Immettere un **hostname** o un indirizzo IP da interrogare
- Fare clic su **Ricerca**

I risultati della query DNS vengono visualizzati sulla pagina, insieme a informazioni e opzioni di supporto. Gli indirizzi restituiti dalla query DNS vengono stampati nel pannello **Risultati**, insieme al tipo di record.

Accanto al pulsante **Ricerca** c'è un nuovo pulsante con l'etichetta **Aggiungere alias**, che fa esattamente questo: crea un alias sotto **Firewall>Alias** contenente i risultati della query come voci nell'alias.

Sotto i risultati c'è una tabella che mostra i tempi di risoluzione per server. Ciò mostra quanto velocemente ciascuno dei server DNS configurati ha risposto alla query specificata o se non ha mai risposto.

Il pannello **ulteriori informazioni** contiene collegamenti alle funzioni ping e traceroute sul firewall per questo host e collegamenti a strumenti esterni per cercare informazioni su chi possiede l'host o l'indirizzo IP.

24.15 Testare una porta TCP

La pagina **Diagnostica>Porta di prova** esegue un semplice test di connessione alla porta TCP per verificare se il firewall è in grado di comunicare con un altro host. Questo verifica se un host è attivo e accetta connessioni su una determinata porta, almeno dal punto di vista del firewall. Nessun dato viene trasmesso all'host remoto durante questo test, tenterà solo di aprire una connessione e, facoltativamente, di visualizzare i dati inviati dal server.

Nota: Questo test non funziona per UDP poiché non è possibile determinare in modo affidabile se una porta UDP accetta le connessioni in questo modo.

Per eseguire un test:

- Passare a **Diagnostica>Porta di prova**
- Compilare i campi della pagina. I campi **Hostname e Porta** sono obbligatori, il resto è facoltativo.

- Fare clic su  **Testare**.

In questa pagina sono disponibili le seguenti opzioni:

Hostname Questo è l'indirizzo IP o l'hostname del sistema di destinazione. Questo è un campo richiesto.

Porta Questa è la porta TCP sull'host di destinazione da testare. Questo è un campo obbligatorio e deve essere un numero di porta valido, ovvero un numero intero compreso tra 1 e 65.535.

Porta sorgente Se necessario, una porta sorgente specificata manualmente per la query. Questo non è richiesto nella maggior parte dei casi.

Testo remoto Se selezionata, questa opzione mostra il testo dato dal server durante la connessione alla porta. Il server dispone di 10 secondi per rispondere, e questa pagina visualizzerà tutto il testo inviato dal server in quei 10 secondi. Come tale, il test verrà eseguito per un minimo di 10 secondi durante l'esecuzione di questo controllo.

Indirizzo sorgente Un indirizzo IP di sorgente specifico o IP Alias/IP virtuale CARP da cui verrà inviata la query. Il servizio in fase di test può richiedere un indirizzo IP di sorgente specifico, rete, ecc, al fine di effettuare una connessione.

Protocollo IP Questa opzione seleziona *IPv4* o *IPv6* per controllare quale tipo di indirizzo IP viene utilizzato quando viene assegnato un hostname. Se la connessione è forzata a IPv4 o IPv6 e l'hostname non contiene un risultato utilizzando tale protocollo, si verificherà un errore. Ad esempio, se costretto a IPv4 e dato un hostname che restituisce solo un indirizzo IPv6 (AAAA record), non funzionerà.

I dati e le informazioni che Firew4LL raccoglie e visualizza è ogni bit importante quanto i servizi che fornisce. A volte sembra che i router commerciali vadano fuori del loro motodo di nascondere quante più informazioni possibili dagli utenti, ma Firew4LL può fornire quasi tutte le informazioni che chiunque possa mai desiderare (e poi alcune).

Questo capitolo contiene una varietà di metodi per trovare informazioni sullo stato del firewall, log, traffico, hardware e così via.

CAPITOLO 25

Gestione pacchetti

25.1 Installazione dei pacchetti

I pacchetti sono gestiti in **Sistema>Pacchetti**. Gli elenchi lì, esemplificati dalla figura *Elenco dei pacchetti*, mostra tutte le informazioni su un pacchetto: nome, categoria, versione e stato, un collegamento di informazioni sul pacchetto e una breve descrizione. Mantenere i pacchetti installati al minimo indispensabile per una distribuzione con una maggiore sicurezza. L'elenco dei pacchetti è presentato in ordine alfabetico.

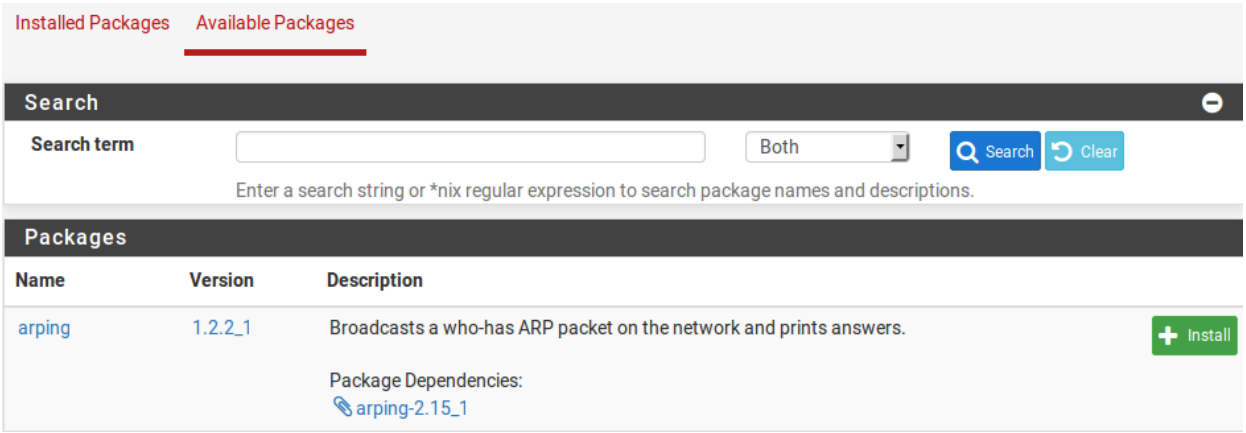


Fig. 1: Elenco dei pacchetti

I pacchetti sono installati come segue:

- Passare a **Sistema>Pacchetti**
- Fareclic sulla scheda **Pacchetti disponibili**
- Individuare il pacchetto da installare nell'elenco

  - Facoltativamente, cercare un pacchetto immettendo un valore nella casella **Termine di ricerca** e fare clic su **Ricerca**

- Cliccare sul pulsante **Installare** a destra della voce del pacchetto.
- Clicare su **Confermare** per procedere con l'installazione del pacchetto

Una volta confermata l'installazione, viene visualizzata la schermata di installazione del pacchetto in cui viene visualizzato l'avanzamento dell'installazione (Figura *Schermata pacchetto post-installazione*).

25.2 Reinstallazione e aggiornamento dei pacchetti

I pacchetti vengono reinstallati e aggiornati nello stesso modo in cui sono installati:

- Passare a **Sistema>Pacchetti**
- Fare clic sulla scheda **Pacchetti installati**, l'elenco apparirà come nella figura *Elenco dei pacchetti installati*
- Individuare il pacchetto da reinstallare o aggiornare nell'elenco. Se è disponibile una versione più recente di quella installata, la clonna **Versione del pacchetto** verrà evidenziata indicando la vecchia e la nuova versione.
- Cliccare su **Aggiornare** o **Reinstallare** il pacchetto.
- Cliccare su **Confermare** per procedere con la reinstallazione del pacchetto

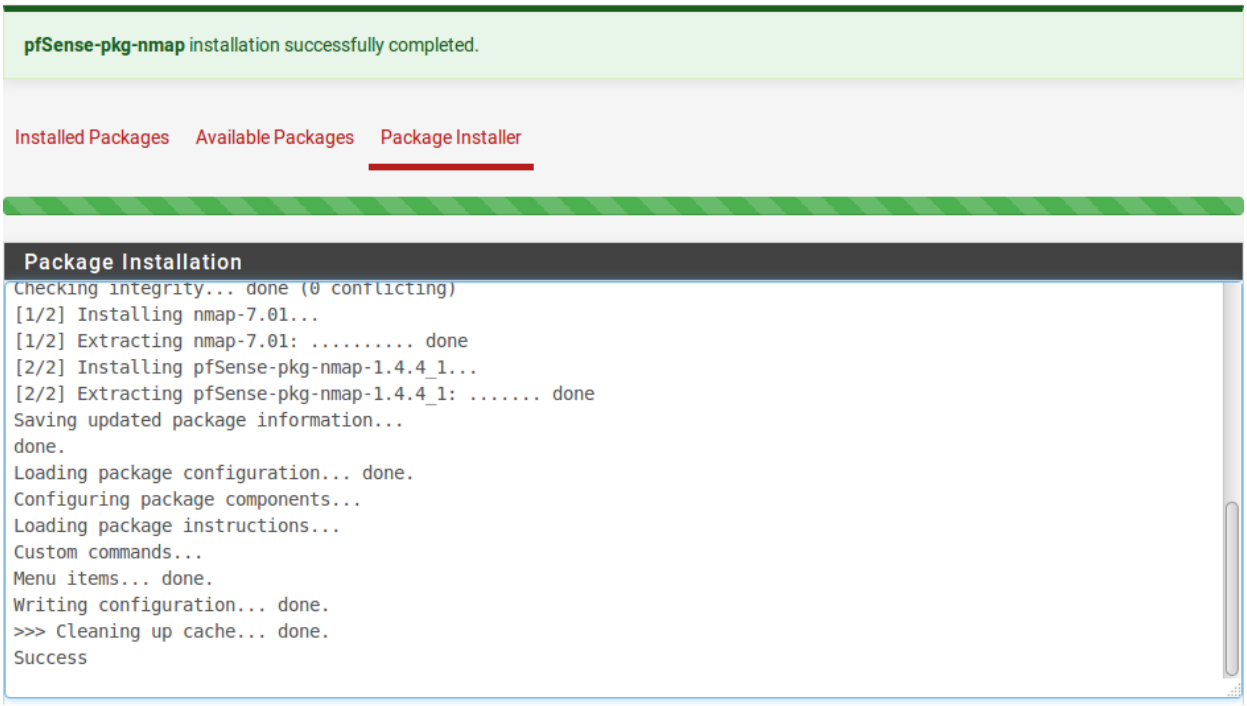


Fig. 2: Schermata pacchetto post-installazione

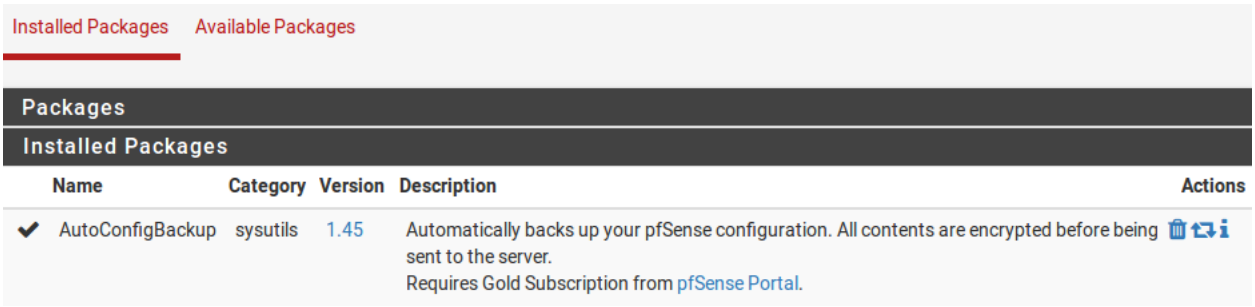


Fig. 3: Elenco dei pacchetti installati

25.3 Disinstallazione dei pacchetti

Per disinstallare un pacchetto:

- Passare a **Sistema>Pacchetti**
- Fare clic sulla scheda **Pacchetti installati**
- Individua il pacchetto da disinstallare nell'elenco
- Cliccare su per rimuovere il pacchetto
- Cliccare su **Confermare** per procedere con la rimozione del pacchetto

25.4 Sviluppo dei pacchetti

Per gli sviluppatori che hanno familiarità con FreeBSD, pkgng e PHP, i pacchetti non sono difficili da creare. Gli utenti finali e le organizzazioni possono trarre vantaggio dallo sviluppo di un pacchetto che non esiste. Per coloro che sono interessati alla creazione di pacchetti, le risorse sono disponibili nel Wiki della documentazione di Firew4LL, a partire dall' articolo sullo sviluppo di pacchetti.

Per inviare un nuovo pacchetto, creare una richiesta pull su Github per il repository di Firew4LL con porte freebsd in modo che il lavoro possa essere valutato per l'inclusione nel sistema dei pacchetti affinché tutti possano vederlo.

25.5 Una breve introduzione ai proxy Web e al resoconto: Squid, SquidGuard e Lightsquid

Questa sezione non intende essere una procedura formale, dettagliata e completa per l'utilizzo di Squid e altri software proxy Web correlati, ma una guida rapida per metterli in funzione e coprire le domande più frequenti sulle loro capacità . Questa sezione tratta Squid per la memorizzazione nella cache di pagine Web e attività correlate, SquidGuard per il filtro e il controllo dell'accesso al contenuto Web e Lightsquid per la segnalazione delle attività degli utenti in base ai registri di accesso a Squid.

Questa discussione presuppone che il firewall abbia una semplice LAN singola e una singola configurazione WAN. Se si verificano problemi durante questa configurazione, visitare la Wiki della documentazione di Firew4LL e il Forum di Firew4LL per ulteriore guida e assistenza.

Vedi anche:

Per ulteriori informazioni, è possibile accedere all'archivio di Hangout per visualizzare l'hangout di marzo 2014 su Squid, Squid-Guard e Lightsquid.

Avvertimento: Il traffico HTTPS non può essere intercettato in modo trasparente in quasi tutti i casi, questa sezione copre solo l'acquisizione trasparente del traffico HTTP. Vedere Proxy trasparenti e HTTP/HTTPS per dettagli.

25.5.1 Cache Proxy Web Squid

Squid è il fondamento di molte altre attività che iniziano con un proxy: può fungere da cache per migliorare le prestazioni Web, può agganciarsi a SquidGuard per il filtraggio dei contenuti e i suoi registri forniscono la base per i rapporti su dove stanno andando gli utenti nella rete.

Prima di ogni altra cosa, è necessario installare il pacchetto Squid. Una volta installato, il pacchetto deve essere configurato. La configurazione di Squid è suddivisa in diverse schede. Prima di lasciare una scheda, fai clic su **Salvare**.

Per avviare la configurazione, accedere a **Servizi>Server proxy di Squid**.

Configurare le impostazioni di Squid come segue, a partire dalla scheda Generale:

> **Abilitare il proxy Squid** *Selezionato* **Mantenere le impostazioni** *Selezionato* **Interfacce proxy** *LAN*, *loopback* **Consentire gli utenti sull'interfaccia** Selezionato, in modo che gli utenti LAN possano utilizzare il proxy. **Proxy HTTP trasparente** Selezionato, quindi il traffico HTTP client verrà intercettato. **Ignorare il proxy per la destinazione dell'indirizzo privato** Selezionato, in modo che il traffico locale e la VPN ignorino il proxy. **Bypassare il proxy per questi IP di sorgente** Se alcuni indirizzi IP dei client locali devono bypassare il proxy, inserirli in questa casella. Più indirizzi, reti o nomi di alias possono essere inseriti separati da un punto e virgola. **Bypass il proxy per questi IP di destinazione** Se alcuni server remoti devono bypassare il proxy, inserirli in questa casella. Più indirizzi, reti o nomi di alias possono essere inseriti separati da un punto e virgola. **Abilitare la registrazione degli accessi** Se Firew4LL è in esecuzione su un'installazione completa (NON incorporata/NanoBSD) e si desidera creare report di accesso Web, selezionare questa casella. **Hostname visibile** Immettere l'hostname del firewall come presentato ai client nei messaggi di errore del proxy. **E-mail dell'amministratore** Inserire un indirizzo di contatto utilizzabile. Se un utente rileva un errore proxy, questo verrà mostrato all'utente in modo che possano contattare l'indirizzo per il supporto.

Salvare le impostazioni, quindi passare alla scheda **Cache locale** e configurarla come segue:

> **Dimensione della cache del disco rigido** Impostare questo su un valore ragionevole per lo spazio disponibile sull'unità e la RAM. Se si esegue NanoBSD, immettere 0 qui.
>
> **Sistema di cache del disco rigido** Se si esegue NanoBSD, impostarlo su null

Altri parametri in questa scheda possono essere modificati in base alle esigenze per controllare la dimensione degli oggetti da memorizzare nella cache, la quantità di memoria utilizzabile per la memorizzazione nella cache e altre impostazioni correlate. Salvare le impostazioni prima di uscire dalla pagina.

Se ci sono più sottoreti locali dietro un percorso statico sulla LAN, visitare la scheda **Controllo accessi** e aggiungerle all'elenco **Sottoreti consentite**.

Dopo aver completato questi passaggi di configurazione, il proxy sarà attivo e funzionante. Se è in uso la modalità trasparente, caricare un sito di prova proxy come http://www.lagado.com/proxy-test ora rivelerà che la richiesta è stata instradata attraverso un proxy.

25.5.2 SquidGuard Controllo e filtro dell'accesso Web

Il pacchetto SquidGuard consente filtri URL molto potenti e controllo degli accessi. Può utilizzare liste nere o elenchi personalizzati di siti Web e può consentire o negare selettivamente l'accesso a tali siti. SquidGuard può funzionare su installazioni complete e NanoBSD, ma le liste nere possono essere utilizzate solo su installazioni complete. SquidGuard è in grado di fare molto di più di quanto sarà trattato in questa sezione. Visitare la Wiki della documentazione di Firew4LL e il Forum di Firew4LL per ulteriori informazioni e tutorial correlati.

Per usare SquidGuard:

- Installare e configurare Squid come descritto nella sezione precedente
- Installare il pacchetto SquidGuard
- Passare a **Servizi>Filtro proxy** per configurare SquidGuard

Impostazioni generali

- Passare a **Servizi>Filtro proxy di SquidGuard**, scheda **Impostazioni generali**
- Selezionare **Abilitare** per abilitare SquidGuard
- Fare clic su **Salvare**
- Selezionare le caselle per abilitare facoltativamente altre funzionalità desiderate, come la registrazione degli eventi di blocchi e la registrazione degli eventi della GUI

Nota: Dopo aver salvato le impostazioni su qualsiasi scheda di SquidGuard, tornare sempre alla scheda **Impostazioni generali** e fare clic sul pulsante  **Applicare**. Fino a quando non sarà stata intrapresa tale azione, le nuove impostazioni di SquidGuard non verranno utilizzate.

Blacklist

Le blacklist o liste nere sono elenchi predefiniti di siti in categorie specifiche, come **siti social**, **siti per adulti**, **siti di musica** e **siti sportivi**. Per utilizzare le blacklist, selezionare **Blacklist** e compilare un **URL di blacklist**. Le due liste più comuni sono elenco MESD e elenco di Shalla.

> **Avvertimento:** Le blacklist non funzionano correttamente su NanoBSD. Non tentare di usarli su quella piattaforma.

Prima che la lista nera possa essere utilizzata, deve essere scaricata e decompressa. Per fare ciò, dopo aver salvato le impostazioni in questa scheda, visitare la scheda **Blacklist** e fare clic su  **Scaricare**.

> **Avvertimento:** Se vengono utilizzate solo liste nere, SquidGuard potrebbe non funzionare. Definire almeno una categoria target come indicato in Categorie target.

Categorie target

Le **categorie target** sono elenchi personalizzati di siti o altre espressioni che definiscono un gruppo di elementi che possono essere utilizzati per consentire o negare l'accesso. Sono mantenuti nella scheda **Categorie target**.

Quando si aggiunge una nuova categoria target, sono necessarie alcune opzioni:

Nome Il nome per la categoria, come apparirà per la selezione su ACL. Il nome deve contenere da 2 a 15 caratteri alfanumerici e il primo carattere deve essere una lettera.

Elenco dei domini Questo è l'elenco dei nomi di dominio da bloccare, come ad esempio www.facebook.com, google.com, microsoft.com, ecc. È possibile inserire più domini, separati da uno spazio.

Modalità di reindirizzamento Questa opzione controlla cosa succede quando un utente viene bloccato da un sito in questo elenco. Il valore predefinito *nessuno* non reindirizzerà l'utente. L'impostazione più comune è la *pagina di errore interna*.

Reindirizzare Se l'utente viene reindirizzato utilizzando la *pagina di errore interna*, immettere qui il messaggio di errore che verrà presentato all'utente. Se viene utilizzato un tipo di reindirizzamento esterno, immettere l'URL completo per il sito di destinazione desiderato, incluso il protocollo appropriato come http:// o https://.

Elenchi di accesso (ACL)

Esistono due tipi di voci ACL in SquidGuard:

1. ACL comune, che è l'ACL predefinito applicato a tutti gli utenti
2. ACL di gruppo, voci che vengono applicate a specifici indirizzi IP, gruppi di indirizzi IP o reti.

Innanzitutto, visitare la scheda **ACL comune**. Scegliere le azioni predefinite per tutte le categorie disponibili dalle liste nere o quelle definite localmente. Per fare ciò, fare clic su **Elenco regole di destinazione**  e selezionare le azioni desiderate dall'elenco a discesa alla fine della riga per ciascuna categoria. La scelta **Accesso predefinito [tutto]** controlla cosa succede quando non è stata trovata alcuna corrispondenza in nessuna delle categorie disponibili.

Dopo aver salvato le impostazioni, passare alla scheda **ACL di gruppo** per creare una voce per un utente o un gruppo di utenti specifici. Utilizzando un ACL di gruppo, è possibile creare un'eccezione alle regole ACL comuni, sia per bloccare l'accesso a un sito che altri possono raggiungere, sia per consentire l'accesso a un sito che altri non possono visualizzare.

Per creare un **ACL di gruppo**:

- Passare alla scheda ACL di gruppo
- Cliccare su  **Aggiungere** per iniziare una nuova voce e configurarla come segue:

  Nome Il nome dell'ACL

  Cliente (sorgente) Immettere l'indirizzo IP dell'utente, la sottorete, ecc. È possibile inserire più valori, separati da spazi.

  Elenco delle regole target Definisce l'elenco delle azioni per questo specifico set di utenti
- Fare clic su **Salvare**
- Tornare alla scheda **Impostazioni generali**
- Fare clic su **Applicare**

25.5.3 Report degli accesso Web con Lightsquid

Lightsquid viene utilizzato per creare report che descrivono in dettaglio la cronologia Web dei computer che hanno avuto accesso ai siti tramite il proxy. Dopo aver installato il pacchetto Lightsquid, le impostazioni del rapporto sono disponibili in **Stato>Rapporti del proxy squid**.

Avvertimento: Questa funzione non è compatibile con le installazioni incorporate/NanoBSD senza modifiche manuali che vanno oltre ciò che la maggior parte degli utenti è in grado di eseguire.

L'aspetto dei report può essere personalizzato scegliendo la lingua, il colore della barra e lo schema dei report. L'opzione **Aggiornare il pianificatore** controlla la frequenza con cui il report verrà aggiornato automaticamente, ad esempio ogni 30 minuti.

Fare clic su **Salvare** per memorizzare le impostazioni, quindi fare clic su **Aggiornare completamente** per compilare il rapporto iniziale. Attendere qualche minuto, quindi fare clic su **Aprire Lightsquid** per visualizzare il rapporto.

Se nel report non sono presenti dati, verificare che **Abilitare la registrazione** sia impostato su Squid e che il traffico degli utenti stia attraversando il proxy come previsto.

25.5.4 Proxy trasparenti e HTTP/HTTPS

Quando si utilizza un proxy, è possibile intercettare il traffico **HTTP** in modo trasparente. Cioè, solo il traffico HTTP può essere acquisito automaticamente e forzato attraverso un proxy senza l'intervento dell'utente o delle sue conoscenze. Questo è conveniente, poiché non richiede la configurazione di alcuna impostazione sul PC dell'utente. Il rovescio della medaglia è che **solo questo traffico HTTP** può essere catturato usando questo metodo; non è possibile intercettare HTTPS allo stesso modo.

Il tentativo di intercettare in modo trasparente HTTPS interromperebbe la catena di fiducia creata da SSL, facendo sì che l'utente venisse accolto con un avviso di certificato spaventoso quando tentava di accedere a un sito sicuro. Questo avviso sarebbe valido in quel caso, poiché il proxy sta essenzialmente eseguendo un attacco man-in-the-middle al fine di ispezionare il traffico dell'utente.

Il pacchetto proxy Squid è in grado di intercettare HTTPS, ma non può essere fatto completamente senza la conoscenza dell'utente o alterazioni del proprio computer. Come minimo, l'intercettazione di HTTPS richiede l'installazione di una CA di root attendibile creata a tale scopo, in modo che possa sembrare che il proxy utilizzi certificati validi.

Il metodo migliore consiste nel posizionare le impostazioni proxy nel computer dell'utente e/o nel software del browser. Questa attività può essere eseguita manualmente, tramite GPO su un dominio Windows, tramite DHCP o automaticamente tramite WPAD. I dettagli di questi vanno oltre lo scopo di questo libro, ma ci sono informazioni su molte di quelle tattiche sulla Wiki della documentazione di Firew4LL e sul Forum di Firew4LL.

Il sistema di pacchetti Firew4LL offre la possibilità di estendere Firew4LL senza aggiungere rigonfiamento e potenziali vulnerabilità della sicurezza alla distribuzione di base. I pacchetti sono supportati su installazioni complete e un set ridotto di pacchetti è disponibile su installazioni integrate basate su NanoBSD.

Nota: le installazioni di NanoBSD hanno la capacità di eseguire

alcuni pacchetti, ma a causa della natura della piattaforma e delle sue restrizioni di scrittura su disco, alcuni pacchetti non funzioneranno e quindi non sono disponibili per l'installazione su quella piattaforma.

Per vedere i pacchetti disponibili per l'attuale piattaforma firewall utilizzata, selezionare **Sistema>Pacchetti**, sulla scheda **Pacchetti disponibili**.

25.6 Introduzione ai pacchetti

Molti dei pacchetti sono stati scritti dalla comunità Firew4LL e non dal team di sviluppo Firew4LL. I pacchetti disponibili variano abbastanza ampiamente e alcuni sono più maturi e ben mantenuti di altri. Esistono pacchetti che installano e forniscono un'interfaccia GUI per software di terze parti, come Squid, e altri che estendono le funzionalità di Firew4LL stesso, come il pacchetto Utilità di esportazione del client di OpenVPN (OpenVPN Client Export Utility) che crea automaticamente file di configurazione VPN.

Di gran lunga il pacchetto più popolare disponibile per Firew4LL è il server proxy di Squid (Squid Proxy Server). Viene installato più del doppio delle volte rispetto al prossimo pacchetto più popolare: Squidguard, che è un filtro per i contenuti che funziona con Squid per controllare l'accesso alle risorse Web da parte degli utenti. Non sorprende che il terzo pacchetto più popolare sia Lightsquid, che è un pacchetto di analisi del registro di Squid che riporta i siti Web visitati dagli utenti dietro il proxy.

Alcuni altri esempi di pacchetti disponibili (che non sono correlati a Squid) sono:

- Monitoraggi della larghezza di banda che mostra il traffico per indirizzo IP come ntopng e Darkstat.
- Servizi extra come FreeRADIUS.
- Proxy per altri servizi come SIP e FTP e proxy inversi per HTTP o HTTPS come HAProxy.
- Utilità di sistema come NUT per il monitoraggio di un UPS.
- Utilità di terze parti popolari come nmap, iperf e arping.
- BGP Routing, routing OSPF, cron editing, agente Zabbix e molti, molti altri.
- Alcuni elementi che in precedenza erano nel sistema di base ma venivano spostati in pacchetti, come RIP (instradato)

Al momento della stesura di questo articolo ci sono più di 40 diversi pacchetti disponibili; troppi per coprirli tutti in questo libro! L'elenco completo dei pacchetti che possono essere installati su un determinato sistema è disponibile all'interno di qualsiasi sistema Firew4LL passando a **Sistema>Pacchetti**.

Il caricamento della schermata dei pacchetti potrebbe richiedere un po' più di tempo rispetto ad altre pagine nell'interfaccia web. Questo perché il firewall recupera le informazioni sul pacchetto dai server dei pacchetti Firew4LL prima che la pagina venga visualizzata per fornire le informazioni sul pacchetto più aggiornate. Se il firewall non dispone di una connessione Internet funzionale inclusa la risoluzione DNS, il processo non riuscirà e attiverà una notifica. Se le informazioni sul pacchetto sono state recuperate in precedenza, verranno visualizzate dalla cache, ma le informazioni saranno obsolete. Questo di solito è causato da una configurazione del server DNS mancante o errata. Per le connessioni IP statiche, verificare che i server DNS funzionanti siano immessi nella pagina **Sistema>Impostazione generale**. Per quelli con connessioni assegnate dinamicamente, assicurarsi che i server DNS assegnati dall'ISP funzionino.

CAPITOLO 26

Firew4ll e il software di terze parti

26.1 Autenticazione RADIUS con Windows Server

Windows 2008 e versioni successive possono essere configurati come server RADIUS utilizzando il server della politica di rete (Network Policy Server, NPS) di Microsoft. Ciò consente l'autenticazione per OpenVPN, il captive portal, il server PPPoE o persino la stessa GUI di Firew4LL utilizzando gli account dell'utente locali del server o la directory attiva di Windows.

26.1.1 Scelta di un server per NPS

NPS richiede una quantità minima di risorse ed è adatto per l'aggiunta a un server Windows esistente nella maggior parte degli ambienti. Microsoft consiglia di installarlo su un controller di dominio di Active Directory per migliorare le prestazioni in ambienti in cui NPS esegue l'autenticazione con Active Directory. Può anche essere installato su un server membro, il che può essere desiderabile in alcuni ambienti per ridurre l'impronta di attacco dei controller di dominio. Ogni servizio accessibile in rete offre un'altra potenziale strada per compromettere un server. NPS ha un solido record di sicurezza, soprattutto rispetto ad altri servizi che devono essere in esecuzione su controller di dominio affinché Active Directory funzioni, quindi questo non è un grosso problema nella maggior parte degli ambienti di rete. La maggior parte degli ambienti installa NPS su uno dei controller di dominio.

26.1.2 Installazione di NPS

Su Windows Server 2008:

- Passare a **Gestione dei server**
- Fare clic su **Ruoli** a sinistra ed espanderlo
- Fare clic su **Aggiungere ruoli** a destra
- Fare clic su **Avanti** per saltare la schermata di introduzione

Su Server 2012:

- Aprire **Gestione dei server della dashboard**

- Fare clic su **Aggiungere ruoli e funzionalità**
- Fare clic su Installazione basata su ruoli o basata su funzioni
- Fare clic su **Avant**i ancora una volta
- Selezionare il server dall'elenco
- Fare di nuovo clic su **Avanti**

Su entrambe le versioni del server, i passaggi rimanenti sono simili:

- Controllare **Politica di rete** e i **servizi di accesso** nell'elenco dei ruoli
- Fare clic su **Aggiungere funzionalità** se appare
- Fare clic su **Avanti** su ciascuna schermata fino alla fine della procedura guidata
- Fare clic su **Finire** o **Installare**, a seconda della versione del server di Windows

1. ### Configurazione di NPS

Per configurare NPS, visualizzare Gestione del server e dovrebbero essere presenti o Politica di rete e Servizi di accesso (2008) o NAP (2012).

Per prima cosa verrà aggiunto un client RADIUS per Firew4LL, quindi verranno configurati i criteri di accesso remoto.

Aggiunta di un client RADIUS

Aprire la configurazione NPS:

Sul server 2008:

- Aprire l'albero della **Gestione del server**
- Espandere la vista sotto di essa fino a quando **client e server RADIUS** sono visibili
- Fare clic su **Client RADIUS**

Sul server 2012:

- Apri la dashboard di **gestione del server**
- Fare clic su **NAP**
- Fare clic con il tasto destro sul server nell'elenco dei server
- Fare clic su **Politica del server di rete**
- Espandere **Client e server RADIUS**
- Fare clic su **client RADIUS**

Aggiungere il nuovo client RADIUS:

- Fare clic con il tasto destro su **client RADIUS**

Fare clic su **Nuovo**, come mostrato in figura *Aggiungere un nuovo client RADIUS*

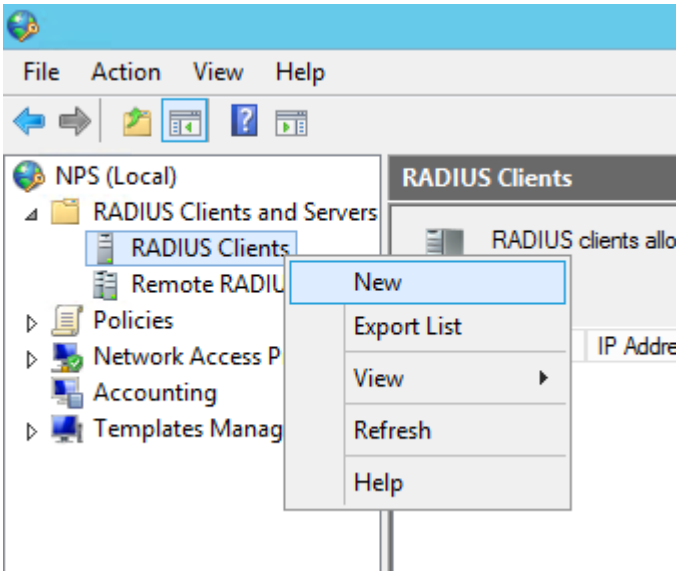


Fig. 1: Aggiungere un nuovo client RADIUS

- Immettere un nome descrittivo per il firewall, come mostrato nella figura *Aggiungere nuovo indirizzo client RADIUS*. Questo può essere l'hostname o FQDN.
- Immettere l'indirizzo (IP o DNS) per il firewall, che deve essere l'indirizzo IP da cui Firew4LL avvierà le richieste RADIUS o un nome di dominio completo che si risolverà in quell'indirizzo IP.

Nota: Questo è l'indirizzo IP dell'interfaccia del firewall più vicino al server RADIUS. Se il server RADIUS è raggiungibile tramite l'interfaccia LAN del firewall, questo sarà l'indirizzo IP della LAN. Nelle distribuzioni in cui Firew4LL non è il firewall perimetrale e l'interfaccia WAN risiede sulla rete interna in cui risiede il server RADIUS, l'indirizzo IP della WAN è ciò che deve essere inserito.

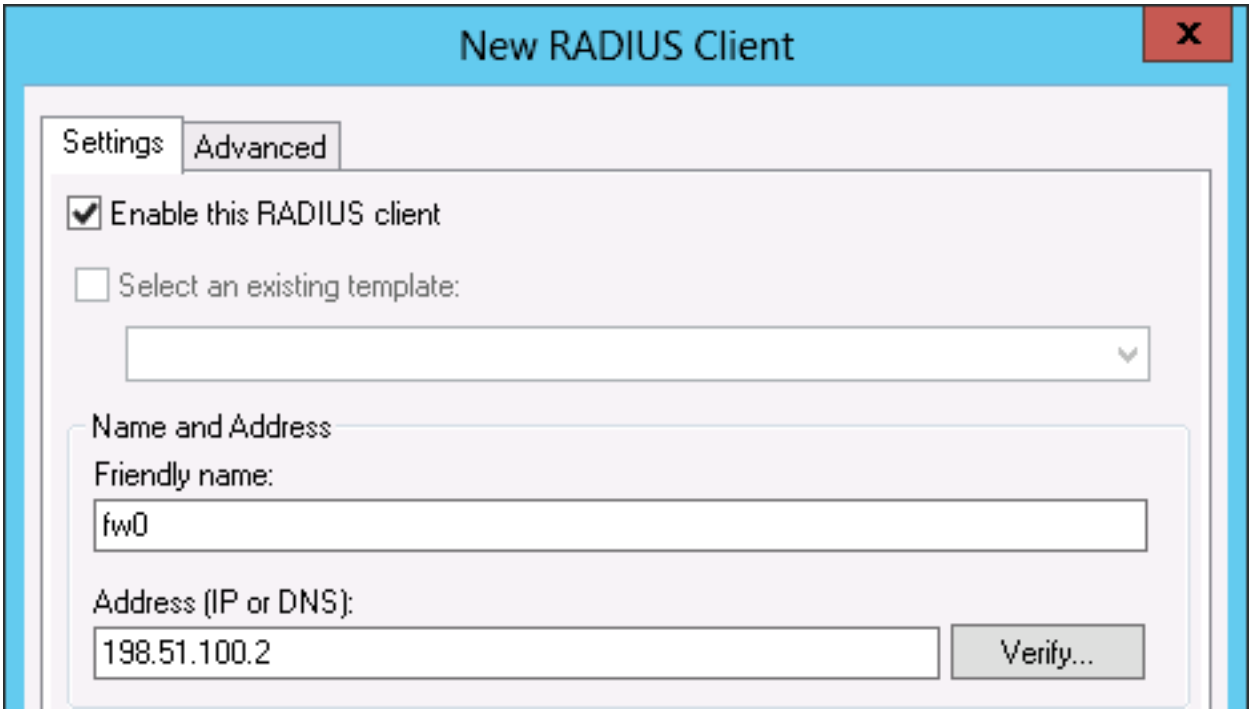


Fig. 2: Aggiungere nuovo indirizzo client RADIUS

- Immettere un **segreto condiviso**, come mostrato nella figura *Aggiungere un nuovo segreto condiviso del client RADIUS*. Questo segreto condiviso viene utilizzato da Firew4LL per autenticarsi quando si effettuano richieste di accesso RADIUS. Windows può crearne uno automaticamente facendo clic su **Generare**.
- Cliccare OK.

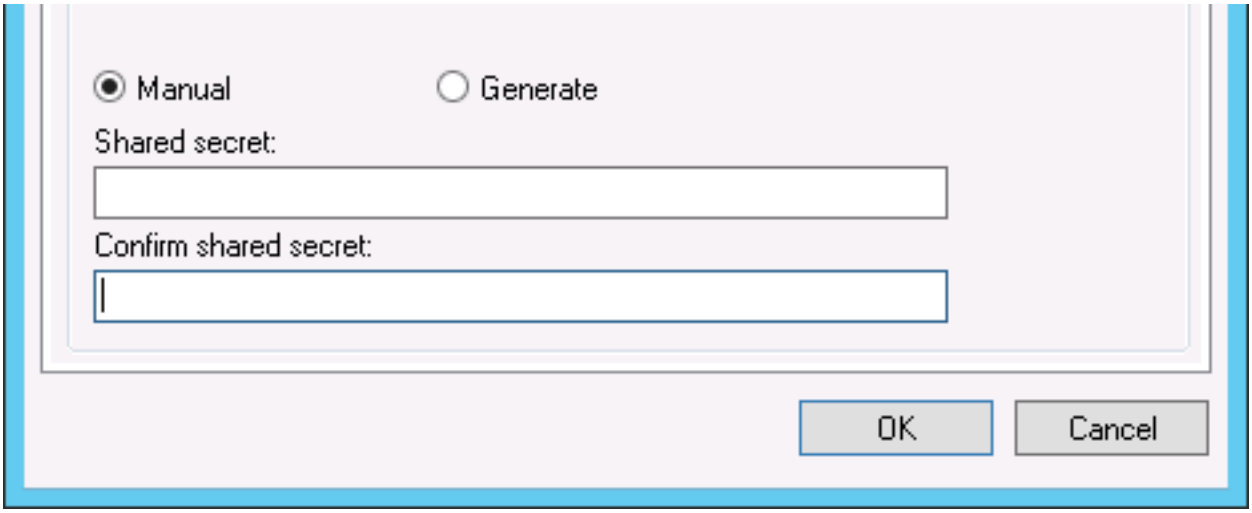


Fig. 3: un nuovo segreto condiviso del client RADIUS

La configurazione di NPS è ora completa. Il client RADIUS è visibile come nella figura *Elenco del client RADIUS*.

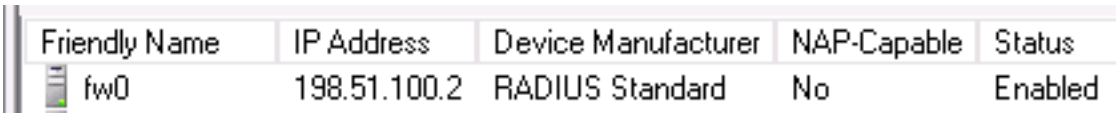


Fig. 4: Elenco del client RADIUS

Fare riferimento alle sezioni precedenti di questa guida che descrivono il servizio da utilizzare con RADIUS per ulteriori indicazioni su come utilizzare il servizio. RADIUS può essere utilizzato in Gestione utenti (*Gestione e autenticazione dell'utente*) che abilita anche RADIUS per IPsec e OpenVPN, per il captive portal (*Configurazione del portale mediante l'autenticazione RADIUS*) e il server PPPoE (*Server PPPoE*), tra l'altro.

Configurazione di utenti e politica di rete

Se un utente può eseguire l'autenticazione tramite RADIUS è controllato tramite la **politica di rete**. Utilizzando la politica di rete, un amministratore può collocare un utente in uno specifico gruppo di Active Directory per consentire l'accesso VPN e offrire anche funzionalità più avanzate come le restrizioni dell'ora del giorno.

Ulteriori informazioni sui criteri di accesso remoto sono disponibili nella documentazione di Microsoft all'indirizzo http://technet.microsoft.com/it-it/library/cc785236% 28WS.10% 29.aspx.

Aggiunta di una politica di rete

- Aprire la finestra di configurazione di NPS
- Espandere **NPS (locale)**, **Politica**, quindi **Politica di rete**
- Fare clic con il tasto destro su **Politica di rete**
- Fare clic su **Nuovo**

- Immettere Consentire da Firew4LL nel **nome della politica**
- Lasciare il **Tipo di server di accesso alla rete** impostato su *Non specificato*
- Fare clic su **Avanti**
- Fare clic su **Aggiungere** nella finestra Specificare condizioni
- Selezionare **gruppi di Windows**
- Cliccare **Aggiungere**
- Immettere o selezionare il nome del gruppo utenti che contiene utenti VPN, ad esempio UtenteVPN
- Cliccare
- Fare clic su **Avanti**
- Scegliere **Accesso concesso**
- Fare clic su **Avanti**
- Selezionare **metodi di autenticazione** aggiuntivi in base alle necessità per le funzionalità su Firew4LL:
  - Lasciare selezionati i metodi di autenticazione esistenti
    - Selezionare **Microsoft: Password protetta (EAP-MSCHAP v2)** se questo criterio verrà utilizzato per l'autenticazione IPsec IKEv2 EAP-RADIUS
    - Selezionare **Autenticazione crittografata (CHAP)**
    - Selezionare **Autenticazione non crittografata (PAP, SPAP)**

  lasciando tutti gli altri metodi selezionati che erano già abilitati.
- Fare clic su **Avanti**
- Fare clic su Rifiutare se la procedura guidata presenta un prompt per visualizzare un argomento della guida
- Configurare eventuali restrizioni di accesso aggiuntive, se necessario
- Fare clic su **Avanti** sulle schermate rimanenti fino a raggiungere la schermata finale
- Fare clic su **Finire**

Modifica di una politica di rete esistente

Le politiche esistenti possono essere modificate per modificarne i vincoli o altre proprietà. Ad esempio, per modificare una politica precedente per abilitarla per l'uso da IPsec per IKEv2 EAP-RADIUS:

- Aprire la finestra di configurazione di NPS
- Espandere **NPS (locale)**, **Politica**, quindi **Politica di rete**
- Modificare la politica attualmente in uso
- Fare clic sulla scheda **Vincoli**
- Fare clic su **Metodi di autenticazione**
- Cliccare **Aggiungere**
- Selezionare **Microsoft: password protetta (EAP-MSCHAP v2)**
- Cliccare **OK**
- Fare clic su **Applicare** per riavviare NPS
- Cliccare **OK**

Risoluzione dei problemi di NPS

Se l'autenticazione fallisce, questa sezione descrive i problemi più comuni che gli utenti incontrano con NPS.

Verificare la porta

Innanzitutto assicurarsi che la porta predefinita **1812** sia utilizzata da NPS. Se il server NPS era stato precedentemente installato, potrebbe essere stato configurato con porte non standard.

- Aprire la finestra di configurazione di NPS
- Fare clic con il tasto destro su **NPS (Locale)** nella parte superiore sinistra della console
- Fare clic su **Proprietà**
- Fare clic sulla scheda **Porte**
- Verificare la configurazione della porta di **autenticazione**. Specificare più porte separandole con una virgola. (come mostrato in figura *Porte NPS*). La porta 1812 **deve** essere una delle porte configurate per l'autenticazione.
- Verificare le porte di **Accounting**, se necessario. Se è richiesta l'accounting RADIUS, la porta 1813 deve essere una delle porte specificate in questa casella.

Controllare il visualizzatore degli eventi

Quando il server risponde a un tentativo di autenticazione RADIUS, NPS accede al registro di sistema nel visualizzatore degli eventi con il risultato della richiesta di autenticazione. Se l'accesso viene negato, viene registrato il motivo per cui è stato negato.

Nel campo Descrizione delle proprietà dell'evento, la riga Motivo indica perché l'autenticazione non è riuscita. I due errori comuni sono: nome utente e password errati, quando un utente immette credenziali errate; e «l'autorizzazione di accesso remoto per l'account utente è stata negata» quando l'account utente è impostato su Negare accesso o la politica di rete configurata in NPS non consente l'accesso per quell'utente. Se NPS registra che l'autenticazione ha avuto esito positivo, ma il client riceve un nome utente o password errato, il segreto RADIUS configurato in NPS e Firew4LL non corrisponde.

I registri NPS nel Visualizzatore eventi possono essere facilmente trovati in Viste personalizzate, quindi Ruoli server e infine Criteri di rete e Servizi di accesso.

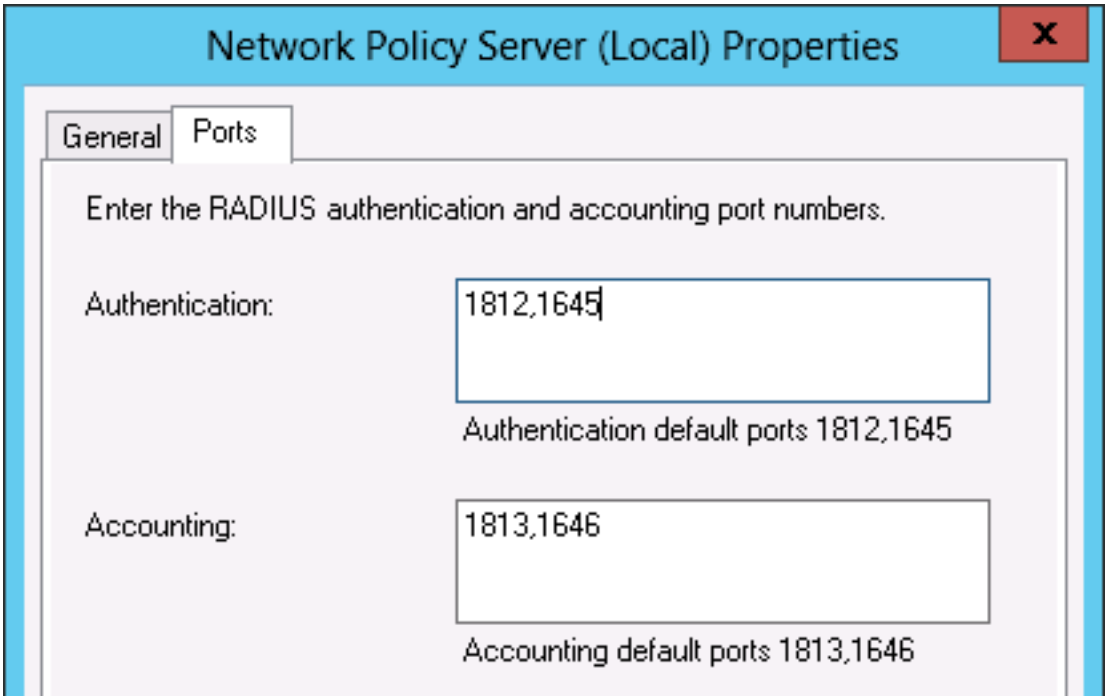


Fig.5: Porte NPS

26.2 Server di Syslog su Windows con Kiwi Syslog

Firew4LL può inviare registri a un server esterno tramite il protocollo syslog (*Registrazione remota con Syslog*). Per gli utenti di Windows,Il server di Syslog di Kiwi (Kiwi Syslog Server) è una bella opzione gratuita per la raccolta di registri dai firewall Firew4LL. Può essere installato come servizio per la raccolta dei registri a lungo termine o come applicazione per esigenze a breve termine. È compatibile con entrambe le versioni server e desktop di Windows 2000 e successive. L'installazione è semplice e non richiede molta configurazione. La guida è disponibile nella sua documentazione dopo l'installazione.

26.3 Usare il software dal sistema di porte di FreeBSD (pacchetti)

Poiché Firew4LL è basato su FreeBSD, molti pacchetti familiari di FreeBSD sono disponibili per l'uso da parte degli amministratori di sistema di FreeBSD.

> **Avvertimento:** L'installazione del software in questo modo non è per inesperti, in quanto potrebbe avere effetti indesiderati e non è consigliata né supportata

Molte parti di FreeBSD non sono incluse, quindi possono verificarsi problemi con la libreria e altri problemi quando si tenta di usare il software installato in questo modo. Firew4LL non include un compilatore nel sistema di base per molte ragioni e poiché tale software non può essere creato localmente. Tuttavia, i pacchetti possono essere installati dal repository di pacchetti predefinito di FreeBSD.

26.3.1 Preoccupazioni/avvertenze

Diversi problemi importanti devono essere considerati da qualsiasi amministratore prima di decidere di installare un software aggiuntivo a un firewall Firew4LL, in particolare il software che non è un pacchetto sanzionato.

Problemi di sicurezza

Qualsiasi software aggiuntivo aggiunto a un firewall è un problema di sicurezza e deve essere valutato completamente prima dell'installazione. Se la necessità supera il rischio, può valere la pena assumerla. I pacchetti ufficiali di Firew4LL non sono immuni da questo problema. Qualsiasi servizio aggiuntivo è un altro potenziale vettore di attacco.

Preoccupazioni per le prestazioni

La maggior parte dell'hardware che esegue Firew4LL è in grado di gestire il carico di traffico con cui è assegnato. Se l'hardware del firewall ha una potenza di riserva, potrebbe non danneggiare il sistema per aggiungere un software aggiuntivo. Detto questo, bisogna essere consapevoli delle risorse consumate dal software aggiunto.

Software in conflitto

Se un pacchetto installato duplica la funzionalità rilevata nel sistema di base o sostituisce un pacchetto di sistema di base con una versione più recente, potrebbe causare un'instabilità del sistema imprevedibile. Assicurarsi che il software non esista già in Firew4LL prima di provare a installare qualcosa.

Mancanza di integrazione

Qualsiasi software aggiuntivo installato non avrà l'integrazione della GUI. Per alcuni, questo non è un problema, ma ci sono state persone che si aspettavano di installare un pacchetto e di far apparire magicamente una GUI per la sua configurazione. Questi pacchetti dovranno essere configurati manualmente. Se si tratta di un servizio, significa anche assicurarsi che tutti gli script di avvio soddisfino i metodi utilizzati da Firew4LL.

Il software può anche installare pagine Web aggiuntive che non sono protette dal processo di autenticazione su Firew4LL. Testare qualsiasi software installato per assicurarsi che l'accesso sia protetto o filtrato in qualche modo.

Mancanza di backup

I pacchetti installati in questo modo devono essere sottoposti a backup manuale di qualsiasi configurazione o altro file necessario.

Non verrà eseguito il backup di questi file durante un normale backup di Firew4LL e il backup potrebbe andare perso o modificato durante un aggiornamento del firmware. Il pacchetto aggiuntivo descritto in *File e directory di backup con il pacchetto di backup* è in grado di eseguire il backup di file come questi.

26.3.2 Installazione dei pacchetti

Per installare un pacchetto, è necessario utilizzare il sito del pacchetto corretto. Firew4LL è compilato su uno specifico ramo di RELEASE di FreeBSD e ha solo un set specifico di pacchetti ospitati sui server di progetto.

I pacchetti situati nel repository dei pacchetti Firew4LL, inclusi alcuni pacchetti software FreeBSD che non fanno parte di Firew4LL, possono essere installati direttamente usando Pkg install

```
# pkg install iftop
```

Oppure usare un URL completo per aggiungere un pacchetto per aggiungerlo dai server dei pacchetti di FreeBSD:

```
# pkg add http://pkg.freebsd.org/freebsd:11:x86:64/quarterly/All/iftop-1.0.p4.txz
```

Il pacchetto verrà scaricato e installato, insieme a tutte le dipendenze necessarie.

Inoltre, il set completo di pacchetti FreeBSD può essere reso disponibile modificando /usr/local/etc/pkg/repos/ Firew4LL.conf e cambiando la prima riga in:

FreeBSD: { enabled: yes }

Avvertimento: L'aggiunta di software dai repository di pacchetti di FreeBSD può introdurre problemi con le dipendenze dei pacchetti, specialmente se un pacchetto dipende da un altro software già esistente su pfSense che potrebbe essere stato creato con opzioni in conflitto. Prestare estrema attenzione quando si aggiungono pacchetti in questo modo.

I pacchetti personalizzati possono anche essere creati su un altro computer che esegue FreeBSD e quindi il file del pacchetto può essere copiato e installato su un firewall Firew4LL. A causa della complessità di questo argomento, non verrà trattato qui.

26.3.3 Mantenimento dei pacchetti

Il seguente comando stampa un elenco di tutti i pacchetti attualmente installati, inclusi i pacchetti Firew4LL e parti del sistema di base di Firew4LL:

```
# pkg info
```

Per eliminare un pacchetto installato, passare il nome completo o utilizzare un carattere wildcard:

```
# pkg_delete iftop-1.0.p4
# pkg_delete pstree-\*
```

26.4 Configurare BIND come un server DNS dinamico RFC 2136

Se il DNS per un dominio è controllato direttamente su un server BIND, il supporto DNS dinamico RFC 2136 può essere impostato per essere utilizzato da Firew4LL. Questa sezione mostra come configurare BIND per supportare questa funzione.

La posizione esatta della directory di configurazione per BIND varierà in base al sistema operativo. Potrebbe essere in /usr/ local/etc/namedb/, /etc/namedb/ o altrove.

Vedi anche:

Vedere *Configurazione degli aggiornamenti DNS dinamici RFC 2136* per ulteriori informazioni sul DNS dinamico RFC 2136.

26.4.1 Configurare il server BIND

Sul server in named.conf, aggiungere il seguente blocco:

include «/etc/namedb/dns.keys.conf»; zone «dyn.example.com» {

type master; file «dynamic/dyn.example.com»; update-policy { grant *.dyn.example.com. self dyn.example.com. A AAAA; };

};

Quindi creare il file di zona iniziale. BIND richiede l'accesso con lettura/scrittura a questo file e alla directory in cui risiede in modo che la zona e il suo diario possano essere aggiornati.

Avvertimento: BIND riscriverà questo file di zona, motivo per cui un sottodominio viene utilizzato nell'esempio.

Da lì, creare il file di zona per la nuova zona dinamica, dynamic/dyn.example.com:

```
$ORIGIN .
$TTL 30 ; 30 seconds
```

dyn.example.com IN SOA ns.example.com. hostmaster.example.com. (

2016062801 ; serial 3600 ; refresh (1 hour) 600 ; retry (10 minutes) 2600 ; expire (43 minutes 20 seconds) 30 ; minimum (30 seconds))

NS ns.example.com. NS ns2.example.com.

Ricaricare il servizio denominato utilizzando rndc reload o un comando simile, quindi se sono presenti server di nomi slave, aggiungere anche una zona a tali server:

zone «dyn.example.com» { type slave; file «dynamic/dyn.example.com»; masters{ 192.0.2.5; };

};

Sul server dei nomi master, creare la directory delle chiavi:

```
# mkdir -p /etc/namedb/keys
```

E ora generare una chiave host. La seconda riga è l'output del comando, non parte del comando stesso.:

```
# /usr/sbin/dnssec-keygen -K /etc/namedb/keys -a HMAC-MD5 -b 128 -n HOST myhost.dyn.
↪example.com.
```

Kmyhost.dyn.example.com.+157+32768

L'uscita Kmyhost.dyn.example.com.+157+32768 è la prima parte del nome del file per la chiave, si aggiungerà .private a un file e .key per un altro. Entrambi contengono gli stessi dati in diversi formati.

Ora leggere la chiave dal nuovo file chiave:

```
# /usr/bin/grep ^Key: /etc/namedb/keys/Kmyhost.dyn.example.com.+157+32768.private | /
↪usr/bin/awk '{ print $2; }'
```

/0/4bxF9A08n/zke/vANyQ==

E poi aggiungere quella chiave al dns.keys.conf:

key myhost.dyn.example.com. { algorithm hmac-md5; secret «/0/4bxF9A08n/zke/vANyQ==»;

};

Questo può essere automatizzato con un semplice script, make-ddns-host.sh:

```
#!/bin/sh
KEY_NAME=${1}
KEY_DIR=/etc/namedb/keys
KEYS_CONFIG=/etc/namedb/dns.keys.conf
/bin/mkdir -p ${KEY_DIR}
cd ${KEY_DIR}
KEY_FILE_NAME=`/usr/sbin/dnssec-keygen -K ${KEY_DIR} -a HMAC-MD5 -b 128 -n HOST ${KEY_
↪NAME}.
KEY_TEXT=`/usr/bin/grep "^Key:" ${KEY_DIR}/${KEY_FILE_NAME}.private | /usr/bin/awk '
↪{print $2; }'`
echo "key ${KEY_NAME}. {" >> ${KEYS_CONFIG}
echo " algorithm hmac-md5;" >> ${KEYS_CONFIG}
echo " secret \"${KEY_TEXT}\";" >> ${KEYS_CONFIG}
echo "};" >> ${KEYS_CONFIG}
echo "Key for ${KEY_NAME} is: ${KEY_TEXT}"
```

Dopo aver creato il file, renderlo eseguibile:

```
# chmod u+x make-ddns-host.sh
```

Usare lo script:

```
# ./make-ddns-host.sh mynewhost.dyn.example.com
# rndc reload
```

26.4.2 Configurare un client in Firew4LL

Per aggiungere una voce DynDNS nella GUI di Firew4LL:

- Passare a **Servizi>DNS dinamico**, scheda **RFC 2136**
- Cliccare  **Aggiungere** per creare una nuova voce con le seguenti impostazioni:

  Abilitare Selezionato

  Interfaccia *WAN*

  Hostname L'hostname completo, ad esempio xxxxx.dyn.example.com

  TTL 30

  Nome chiave Di nuovo l'hostname completo, esattamente: xxxxx.dyn.example.com

  Host del tipo di chiave

  Chiave Chiave segreta per questo hostname

  Server L'indirizzo IP o l'hostname del server BIND

  Protocollo Non selezionato

  Descrizione Mia voce DynDNS

- Fare clic su **Salvare**

Supponendo che il firewall abbia connettività al server dei nomi e che non vi siano altre politiche di accesso che impediscano l'aggiornamento, il servizio RFDN 2136 DynDNS ora funziona. Se l'aggiornamento non funziona, controllare il registro BIND e il registro di sistema su Firew4LL.

Mentre questo libro è incentrato su Firew4LL, esistono numerosi pacchetti software di terze parti che possono essere configurati per interagire con Firew4LL o aumentarne la funzionalità. In questo contesto, il software di terze parti

si riferisce al software disponibile da altri fornitori o fonti che può essere utilizzato insieme a Firew4LL, ma non è considerato parte del «sistema Firew4LL». Questi sono diversi dai pacchetti Firew4LL, che sono software extra che girano sul sistema Firew4LL e si integrano nella GUI del sistema.

CAPITOLO 27

Guida ai menu

27.1 Sistema

Il menu del **Sistema** contiene opzioni per il firewall stesso, opzioni generali e avanzate, aggiornamenti, pacchetti aggiuntivi, utenti e routing.

Avanzate Impostazioni avanzate per firewall, hardware, SSH, notifiche, parametri sintonizzabili e molti altri. Vedere *Opzioni di configurazione avanzate*.

Gestione dei certificati Gestire le autorità di certificazione, i certificati e gli elenchi di revoche di certificati (x.509). Vedere *Gestione dei certificati*.

Impostazioni generali Impostazioni generali come hostname, dominio e server DNS. Vedere *Opzioni della configurazione generale*.

Sync con elevata disponibilità Controlla il modo in cui i nodi Firew4LL in un cluster ad alta disponibilità (HA) sincronizzano gli stati e la configurazione. Vedere *Elevata disponibilità*.

Disconnettersi Esce dalla GUI, riportando l'utente alla schermata di accesso. Vedere *Gestione utenti e Autenticazione*.

Gestione di pacchetti Componenti aggiuntivi dei software aggiuntivi per Firew4LL per espandere la sua funzionalità. Vedere *Pacchi*.

Routing Gestisce gateway, route statiche e gruppi gateway per multi-WAN. Vedere *Routing*.

Procedura guidata di configurazione La procedura guidata di configurazione esegue la configurazione iniziale di base. Vedere ***Installazione guidata***.

Aggiornare Aggiorna Firew4LL all'ultima versione. Vedere *Aggiornamento tramite WebGUI*.

Gestione utenti Gestire utenti, gruppi e server di autenticazione (RADIUS o LDAP) per l'accesso alla GUI, l'accesso VPN, ecc. Vedere *Gestione e autenticazione dell'utente*.

> **Nota:** Se un utente dispone del privilegio *WebCfg - Sistema: Gestione della password dell'utente*, questa opzione di menu porta l'utente a una pagina in cui è possibile modificare la propria password ma non apportare modifiche ad altri utenti.

Impostazioni utente Se le impostazioni per utente sono abilitate, questa pagina consente agli utenti di ignorare le opzioni di comportamento predefinite disponibili in **Impostazione generale**.

27.2 Interfacce

Il menu **Interfacce** contiene una voce per l'assegnazione delle interfacce e voci per ciascuna interfaccia attualmente assegnata. Le interfacce assegnate mostreranno i loro nomi configurati o i nomi standard se non sono stati modificati (ad es. WAN, LAN, OPTx)

(assegnare) Assegna interfacce a ruoli logici (ad es. WAN, LAN, OPT) e creare/mantenere VLAN e altri tipi di interfacce virtuali. Vedere *Configurazione dell'interfaccia*, *Tipi di interfaccia e configurazione*, e *LAN virtuali (VLAN)*.

WAN Configura l'interfaccia WAN. Vedere *Configurazione dell'interfaccia*.

LAN Configura l'interfaccia LAN. Vedere *Configurazione dell'interfaccia*.

OPTX Configura eventuali interfacce opzionali aggiuntive. Vedere *Configurazione dell'interfaccia*.

27.3 Firewall

Le voci del menu **Firewall** configurano le regole del firewall, le regole NAT e la loro struttura di supporto.

Alias Gestisce raccolte di indirizzi IP, reti o porte per semplificare la creazione e la gestione delle regole. Vedere *alias*.

NAT Gestisce le regole NAT che controllano le porte forward, NAT 1:1 e il comportamento NAT in uscita. Vedere *Traduzione dell'indirizzo di rete*.

Regole Configura le regole del firewall. C'è una scheda su questa schermata per ogni interfaccia configurata, oltre a schede per gruppi e diversi tipi di VPN, quando abilitati. Vedere *Introduzione alla schermata delle regole del firewall*.

Pianificazioni Gestisce le pianificazioni delle regole basate sul tempo. Vedere *Regole basate sul tempo*.

Shaper del traffico Gestisce le impostazioni di shaping del traffico/Qualità di servizio (QoS). Vedere *Shaper del traffico*.

IP virtuali Configura gli indirizzi IP virtuali che consentono a Firew4LL di gestire il traffico per più di un indirizzo IP per interfaccia, in genere per le regole NAT o la disponibilità elevata. Vedere *Indirizzi IP virtuali*.

27.4 Servizi

Il menu **Servizi** contiene elementi che controllano i servizi forniti dai daemon in esecuzione sul firewall. Vedere *Servizi*.

captive portal Controlla il servizio Cadel captive portal che indirizza gli utenti a una pagina Web per l'autenticazione prima di consentire l'accesso a Internet. Vedere *captive portal*.

Relay DHCP Configura il servizio di relay di DHCP che inoltra le richieste DHCP da un segmento di rete a un altro. Vedere *Relay DHCP e DHCPv6*.

Server DHCP Configura il servizio DHCP che fornisce la configurazione automatica dell'indirizzo IP per i client. Vedere *Server DHCP IPv4*.

Relay DHCPv6 Configura il servizio di inoltro DHCP per IPv6 che inoltra richieste DHCPv6 da un segmento di rete a un altro. Vedere *Relay DHCP e DHCPv6*.

Server DHCPv6 e RA Configura il servizio DHCP per IPv6 e gli annunci router che forniscono la configurazione automatica dell'indirizzo IPv6 per i client. Vedere *Server DHCP IPv6 e annunci del router.*

Forwarder del DNS Configura il forwarder del DNS di cache incorporato. Vedere *Forwarder del DNS*.

Risolutore del DNS Configura il risolutore DNS di cache incorporato. Vedere *Risolutore del DNS*.

DNS dinamico Configura i servizi DNS dinamici («dyndns») che aggiorna un server dei nomi remoto quando l'indirizzo IP della WAN di questo firewall è cambiato. Vedere *DNS dinamico*.

Proxy IGMP Configura il proxy del protocollo di gestione del gruppo interno per il passaggio del traffico multicast tra le interfacce. Vedere *Proxy IGMP*.

Bilanciatore del carico Configura il bilanciatore del carico, che bilancia le connessioni in entrata su più server locali. Vedere *Bilanciamento del carico del server*.

NTP Configura il demone del server del protocollo dell'orario di rete. Vedere *NTPD*.

Server PPPoE Configura il server PPPoE che accetta e autentica le connessioni dai client PPPoE su reti locali. Vedere *Server PPPoE*.

SNMP Configura il demone SNMP (Protocollo di gestione della rete semplice, Simple Network Management Protocol) per consentire la raccolta di statistiche basate sulla rete da questo firewall. Vedere *SNMP*.

UPnP e NAT-PMP Configura il servizio Universal Plug and Play (UPnP) e il protocollo di mappatura delle porte del NAT che configura automaticamente le regole NAT e firewall per i dispositivi che supportano gli standard UPnP o NAT-PMP. Questa voce di menu appare solo se è assegnata più di un'interfaccia. Vedere *UPnP e NAT-PMP*.

Attivare la LAN Configura le voci Attivare la LAN che attivano in remoto i dispositivi dei client locali. Vedere *Attivare la LAN*.

27.5 VPN

Il menu VPN contiene elementi relativi alle reti private virtuali (VPN), tra cui IPsec, OpenVPN e L2TP. Vedere *Reti private virtuali*.

IPsec Configura tunnel VPN di IPsec, IPsec mobile e impostazioni IPsec. Vedere *IPsec*.

L2TP Configura i servizi e gli utenti L2TP. Vedere *VPN con L2TP*.

OpenVPN Configura server e client OpenVPN, nonché la configurazione specifica del client. Vedere *OpenVPN*.

27.6 Stato

Le voci del menu **Stato** mostrano informazioni sullo stato e registri per vari componenti e servizi del sistema.

captive portal Quando il captive portal è abilitato, questa voce mostra lo stato dell'utente e del voucher. Vedere *Portale captive*.

CARP (failover) Mostra lo stato degli indirizzi IP del CARP su questo firewall, come lo stato MASTER/BACKUP per ciascun VIP del CARP. Ha anche controlli per la modalità di manutenzione HA. Vedere *Controllare lo stato CARP*.

Pannello di controllo Un collegamento alla pagina principale del firewall Firew4LL, che visualizza informazioni generali sul sistema. Vedere *Pannello di controllo*.

Locazioni di DHCP Mostra un elenco di tutte le locazioni di DHCP IPv4 assegnate da questo firewall e fornisce controlli basati su tali leasing, come l'aggiunta di mappature statiche. Vedere *Locazioni*.

Leasing DHCPv6 Mostra un elenco di tutti i lease DHCP IPv6 assegnati da questo firewall. Vedere *Locazioni*

Ricaricare filtro Mostra lo stato dell'ultima richiesta di ricarica del filtro, comprese le azioni di ricarica attive. Fornisce inoltre un mezzo per forzare un ricaricamento del filtro e per forzare una sincronizzazione della configurazione XMLRPC quando è configurato HA. Vedere *Risoluzione dei problemi relativi alle regole del firewall*.

Gateway Mostra lo stato dei gateway e dei gruppi gateway per multi-WAN. Vedere *Routing*.

Interfacce Mostra lo stato hardware per le interfacce di rete, equivalente all'utilizzo di ifconfig sulla console. Vedere *Stato dell'interfaccia*.

IPsec Mostra lo stato di tutti i tunnel IPsec configurati. Vedere *IPsec*.

Bilanciamento del carico Mostra lo stato dei pool di bilanciamento del carico del server. Vedere*Visualizzazione dello stato del bilanciamento del carico*.

Monitoraggio Mostra i dati rappresentati graficamente per le statistiche di sistema come larghezza di banda utilizzata, utilizzo della CPU, stati del firewall, ecc. Vedere *Grafici di monitoraggio*.

NTP Mostra lo stato del daemon del server del protocollo dell'orario di rete. Vedere *NTPD*.

OpenVPN Mostra lo stato di tutte le istanze OpenVPN configurate. Vedere *Verifica dello stato di OpenVPN **Clienti e server***.

Registro dei pacchetti Visualizza i log da alcuni pacchetti supportati.

Code Mostra lo stato delle code che modellano il traffico. Vedere*Monitoraggio delle code*.

Servizi Mostra lo stato dei demoni del sistema e del servizio pacchetti. Vedere*Stato del servizio*.

Registri di sistema Mostra i registri del sistema e i servizi di sistema come firewall, DHCP, VPN, ecc. Vedere *Registri di sistema*.

Grafico del traffico Visualizza un grafico del traffico dinamico in tempo reale per un'interfaccia. Vedere*Grafici del traffico*.

UPnP e NAT-PMP Mostra un elenco di qualsiasi porta UPnP attualmente attiva. Questa voce è presente solo quando il firewall contiene più di un'interfaccia. Vedere*UPnP e NAT-PMP*.

Wireless Mostra un elenco di tutte le reti wireless attualmente disponibili nel raggio d'azione, insieme ai livelli del segnale. Questa voce di menu è presente solo se al firewall è assegnata un'interfaccia wireless. Vedere*Controllare lo stato del wireles*.

27.7 Diagnostica

Le voci nel menu **Diagnostica** eseguono varie attività diagnostiche e amministrative.

Tabella ARP Visualizza un elenco di dispositivi visti localmente dal firewall. L'elenco include un indirizzo IP, un indirizzo MAC, un hostname, l'interfaccia in cui è stato visualizzato il dispositivo e altre informazioni correlate.

Autenticazione Verifica l'autenticazione su un server RADIUS o LDAP definito. Vedere *Risoluzione dei problemi*.

Backup e ripristino Backup e ripristino dei file di configurazione. Vedere *Backup e ripristino*.

Prompt dei comandi Esegue i comandi della shell o il codice PHP e carica/scarica i file sul/dal firewall. Usare con cautela.

Ricerca DNS Esegue una ricerca DNS per risolvere i nomi host a fini diagnostici e per testare la connettività ai server DNS. Vedere *Testare il DNS*.

Modifica del file Modifica un file sul filesystem del firewall.

Impostazioni di fabbrica Ripristina la configurazione ai valori predefiniti. Tenere presente, tuttavia, che ciò non altera il filesystem o disinstalla i file del pacchetto; cambia solo le impostazioni di configurazione. Vedere *Ripristinare le impostazioni di fabbrica predefinite*.

Mirror GEOM Se il firewall contiene un mirror del disco GEOM, questa pagina mostra lo stato del mirror e fornisce i controlli per la gestione del mirror.

Sistema di arresto Chiude il firewall e disattiva l'alimentazione ove possibile. Vedere *Sistema di arresto*.

Informazioni sul limitatore Mostra lo stato di tutti i limitatori e il traffico che scorre al loro interno. Vedere *Controllo dell'uso del limitatore*.

Tabella NDP Mostra un elenco di dispositivi IPv6 locali visti dal firewall. L'elenco include un indirizzo IPv6, un indirizzo MAC, un hostname (se noto al firewall) e l'interfaccia.

Acquisizione pacchetti Esegue un'acquisizione di pacchetti per ispezionare il traffico, quindi visualizzare o scaricare i risultati. Vedere *Acquisizione di pacchetti dalla WebGUI*.

PFInfo Visualizza le statistiche sul filtro pacchetti, inclusi i tassi di traffico generali, i tassi di connessione, le informazioni sulla tabella di stato e vari altri contatori. Vedere *PFInfo*.

pfTop Visualizza un elenco delle principali connessioni attive in base a una metrica selezionabile come byte, frequenza, età, ecc. Vedere *Visualizzazione degli stati con pfTop*.

ping Invia richieste di eco ICMP a un determinato indirizzo IP, inviato tramite un'interfaccia scelta.

Riavvio del sistema Riavvia il firewall. Il completamento dell'operazione può richiedere alcuni minuti, a seconda dell'hardware e delle funzionalità abilitate. Vedere *Riavvio del sistema*.

Itinerari Mostra i contenuti della tabella di routing. Vedere *Visualizzazione dei percorsi*.

Stato SMART Visualizza le informazioni diagnostiche sulle unità disco, se supportate dall'hardware. Può anche eseguire test di guida. Vedere *Stato del disco rigido SMART*.

Sockets Visualizza un elenco di processi sul firewall che sono collegati alle porte di rete, ascoltando le connessioni o effettuando connessioni in uscita dal firewall stesso.

Stati Mostra gli stati del firewall attualmente attivi. Vedere *Stati del firewall*.

Riepilogo degli stati Visualizza le informazioni sulla tabella di stato, per visualizzare le attività riepilogate per indirizzo IP. Vedere *Riepilogo degli stati*.

Attività di sistema Mostra l'utilizzo della memoria e un elenco di processi attivi e thread di sistema sul firewall, l'output proviene da top -aSH. Vedere *Attività di sistema (in alto)*.

Tabelle Visualizza e modifica i contenuti di varie tabelle e alias firewall. Vedere *Visualizzazione dei contenuti di **tabelle***.

Porta di prova Esegue un semplice test di connessione TCP dal firewall per determinare se un host remoto sta accettando connessioni su una porta specifica.

Traceroute Traccia il percorso seguito dai pacchetti tra questo firewall e un sistema remoto. Vedere *Utilizzando **traceroute***.

Questa sezione è una guida alle scelte di menu standard disponibili in Firew4LL. Questa guida aiuterà a identificare rapidamente lo scopo di una determinata opzione di menu e fare riferimento ai luoghi del libro in cui tali opzioni sono discusse in modo più dettagliato.

I pacchetti possono aggiungere elementi a qualsiasi menu, quindi controllare ogni menu o consultare la documentazione di un pacchetto per individuare le voci del menu. In genere, i pacchetti installano le voci nel menu Servizi, ma ci sono numerose eccezioni.

CAPITOLO 28

Guide raccomandate

- *Gestione Certificati* - Confiurare certificati Let's Encrypt con Pacchetto ACME.
- *MultiWAN* - Imparare a configurare WAN failover e bilanciamento di carico con Firew4LL.

CAPITOLO 29

Risorse commerciali

- Firew4LL - Supporto
- InSecureNet - Servizi