

Manuale utente

EnterNet FireWall™

EnterNet FireWall Manager™

EnterNet FireWall Logger™

Sommario

1. Informazioni sul documento	7
1.1 Note legali	7
1.2 Convenzioni tipografiche	8
1.3 Aggiornamenti	8
2. Introduzione alla protezione di rete	9
2.1 Introduzione	9
2.2 Cos'è un firewall?	9
2.3 Vulnerabilità dei dispositivi di protezione	10
2.4 Come funziona un firewall?	10
2.5 Quali sono i limiti del firewall?	11
2.5.1 Attacchi ai componenti preinstallati non protetti	12
2.5.2 Utenti inesperti di reti protette	12
2.5.3 Attacchi alle reti guidati dai dati	13
2.5.4 Attacchi interni	16
2.5.5 Connessioni modem e VPN	16
2.5.6 Buchi tra zone demilitarizzate e reti interne	17
2.6 Quali sono i bersagli degli attacchi?	19
3. EnterNet FireWall	21
3.1 Panoramica su EnterNet FireWall	21
3.2 Funzioni di EnterNet FireWall	21
3.3 Componenti del sistema	25
3.4 Esempi di architetture di rete	26
3.4.1 Esempio 1: soluzione di protezione perimetrale tradizionale	28
3.4.2 Esempio 2: soluzione di protezione segmentata	29
3.4.3 Esempio 3: segmentazione di una rete aziendale	30
3.4.4 Esempio 4: soluzione firewall ISP/ASP	31
3.5 Modello di licenza di EnterNet FireWall	32
3.5.1 Modello di licenza	32
3.5.2 Gestione delle licenze EnterNet tramite pagine Web	33

4.	Hardware e prestazioni del firewall	35
4.1	Panoramica	35
4.2	Prestazioni del firewall	35
4.3	Scelta dei componenti hardware	37
4.3.1	CPU	38
4.3.2	RAM	38
4.3.3	Scheda madre/bus di sistema	39
4.3.4	Supporti di avvio	40
4.3.5	Schede di rete	41
4.3.6	Configurazione del BIOS	43
4.3.7	Altri requisiti	43
5.	Aggiornamento dalla versione 5.x	45
5.1	Procedura di aggiornamento 1: accesso fisico	45
5.2	Procedura di aggiornamento 2: accesso remoto	47
6.	Operazioni preliminari	49
6.1	Avvio rapido	49
6.2	Preparativi iniziali	49
6.3	Creazione di un firewall in FireWall Manager	50
6.4	Modifica delle impostazioni predefinite	52
6.4.1	Indirizzi di rete locale Selezionare la scheda Nets per modificare le impostazioni degli indirizzi di rete.	53
6.4.2	Indirizzi IP locali	54
6.4.3	Definizione delle impostazioni della scheda di rete	56
6.4.4	Configurazione dell'interfaccia	57
6.5	Salvataggio della configurazione	58
6.6	Messa in funzione di EnterNet FireWall	59
6.6.1	Creazione di un supporto di avvio per EnterNet FireWall	59
6.6.2	Collegamento delle schede di rete del firewall	59
6.6.3	Installazione della chiave hardware	60
6.6.4	Avvio di EnterNet FireWall Manager	60
6.7	Se il firewall non funziona	61
7.	EnterNet FireWall Manager	65
7.1	Installazione di FireWall Manager	66
7.1.1	Procedura di installazione	66
7.1.2	Maggiore sicurezza a livello locale per FireWall Manager	66

7.1.3	Database di amministrazione	67
7.2	Finestra principale: FireWall List	68
7.2.1	Barra degli strumenti	70
7.2.2	Menu File	71
7.2.3	Menu FireWall	71
7.2.4	Menu Tools	79
7.2.5	Menu Log	82
7.2.6	Menu View	82
7.3	Finestra di configurazione	83
7.3.1	Menu File	86
7.3.2	Scheda Settings	87
7.3.3	Scheda Hosts	115
7.3.4	Scheda Nets	116
7.3.5	Scheda Pipes	117
7.3.6	Scheda Interfaces	120
7.3.7	Scheda ARP	121
7.3.8	Scheda Routes	123
7.3.9	Scheda Access	125
7.3.10	Scheda Rules	127
7.3.11	Scheda Loghosts	140
7.3.12	Scheda Remotes	141
7.4	Visualizzazione delle statistiche	142
7.4.1	Statistiche relative al firewall	143
7.4.2	Statistiche di utilizzo per le regole	143
7.4.3	Statistiche sui pipe	144
7.4.4	Statistiche per ciascuna interfaccia	146

8. EnterNet FireWall 147

8.1	Traduzione degli indirizzi	147
8.1.1	Traduzione dinamica degli indirizzi di rete	148
8.1.2	Quali protocolli può elaborare la regola NAT Hide?	148
8.1.3	Perché NAT Hide modifica la porta di origine?	149
8.1.4	Traduzione di intervalli di indirizzi e di porte	150
8.1.5	Quale delle regole SAT viene eseguita se il firewall trova più corrispondenze?	151
8.1.6	Quali protocolli possono essere gestiti dalla funzione SAT?	152
8.1.7	Esempi di traduzione degli indirizzi	153
8.2	Console del firewall	159
8.2.1	Barra di stato della console	160
8.2.2	Comandi della console	161
8.3	Supporti di avvio di EnterNet FireWall	168
8.4	Considerazioni generali prima della configurazione	170

8.5	Esempi di configurazione	171
8.5.1	Esempio 1: Default	172
8.5.2	Esempio 2: Default-ProxyARP	181
8.5.3	Esempio 3: DMZ	182
8.5.4	Esempio 4: DMZ-MailFwd-DNS	195
8.5.5	Esempio 5: DMZ-ProxyARP	205
8.5.6	Esempio 6: DMZ-Shared-Extnet	206
<u>9. Auditing da EnterNet Firewall</u>		207
9.1	Cosa viene registrato da EnterNet FireWall?	207
9.2	EnterNet FireWall Logger	211
9.2.1	Installazione di FireWall Logger	211
9.2.2	Configurazione di EnterNet FireWall Logger	212
9.3	Strumento di analisi dei log	216
9.3.1	Visualizzazione Wizard	217
9.3.2	Visualizzazione Results	221
9.3.3	Visualizzazione E-SQL	224
9.4	Riferimenti E-SQL	225
9.5	Log inviati a destinatari syslog	232
9.6	Visualizzazione Real-Time dei Log	233
<u>10. Configurazione del traffico</u>		235
10.1	Premessa	236
10.1.1	Nozioni di base su Traffic Shaping	237
10.2	Configurazione del traffico su EnterNet FireWall	240
10.2.1	Nozioni di base sui pipe	241
10.2.2	Precedenze	248
10.2.3	Raggruppamento degli utenti di un pipe	258
10.2.4	Bilanciamento dinamico della larghezza di banda	261
10.3	Esempi pratici di utilizzo dei pipe	262
<u>11. Internet e TCP/IP</u>		265
11.1	Numeri di protocollo IP	265
11.2	Numeri di porta utilizzati comunemente	271
<u>12. Domande frequenti (FAQ)</u>		283
<u>13. Glossario</u>		295

1. Informazioni sul documento

1.1 Note legali

È vietata la riproduzione completa o parziale del contenuto di questo documento senza previa autorizzazione scritta di EnterNet Technologies in base alle disposizioni di legge sul diritto di autore in vigore in Svezia del 30 dicembre 1960. Tali vincoli vengono applicati a tutte le forme di riproduzione, inclusa la trasmissione, la stampa, la copia, la serigrafia, la registrazione, la duplicazione o la pubblicazione in formato elettronico e così via.

Copyright © 1998-2001 EnterNet Technologies.
Tutti i diritti riservati.

3Com 3c509 EtherLink III e 3Com 3c905 Fast EtherLink 10/100 sono marchi di 3Com® Corporation.

Intel EtherExpress PRO/100 è un marchio di Intel® Corporation.

Novell Netware è un marchio di Novell®, Inc.

MS-DOS, Windows 95, 98, NT, Microsoft Access e Internet Explorer sono marchi di Microsoft® Corporation.

Caldera DR-DOS è un marchio di Caldera®, Inc.

Netscape Navigator è un marchio di Netscape® Communications Corporation.

WS_FTP è un marchio di Ipswitch™, Inc.

Adobe Acrobat è un marchio di Adobe® Systems, Inc.

EnterNet FireWall, EnterNet FireWall Manager ed EnterNet FireWall Logger sono marchi di EnterNet Technologies.

Tutti gli altri marchi appartengono ai rispettivi proprietari.

1.2 Convenzioni tipografiche

Per il testo normale viene utilizzato questo carattere.

Il testo per il quale è richiesto l'input dell'utente è in carattere a "larghezza fissa".

I nomi di menu, comandi, cartelle, pulsanti o tutti gli altri riferimenti al software è in **Grassetto**, di solito con la prima lettera maiuscola.

1.3 Aggiornamenti

Gli aggiornamenti al presente Manuale utente si possono scaricare in formato PDF di Adobe Acrobat all'indirizzo <http://www.enternet.net>.

2. Introduzione alla protezione di rete

2.1 Introduzione

È ormai un dato di fatto che la rapida espansione di Internet e lo sviluppo di soluzioni per reti intranet ed extranet hanno esposto le aziende e le organizzazioni a nuove minacce relative alla sicurezza. Sono sempre più numerose le notizie che riguardano crimini compiuti sui dati elettronici che viaggiano nelle reti di aziende e organizzazioni governative, ad esempio furti di informazioni e violazioni alla sicurezza da parte di pirati informatici.

- In che modo è possibile evitare accessi non autorizzati alle reti di un'azienda?
- In che modo è possibile controllare il flusso di dati che viaggia tra due reti differenti?
- Quanto costano i sistemi di protezione delle reti?

Queste sono le domande sempre più frequenti che si pongono i responsabili di numerose aziende e organizzazioni.

2.2 Cos'è un firewall?

Quando si collega un computer a una rete locale o di altro tipo, ad esempio Internet, è necessario prendere i debiti provvedimenti per impedire l'accesso di intrusi indesiderati alle risorse e alle informazioni riservate e delicate. Per raggiungere questo obiettivo, è necessario installare un firewall all'interno della rete. Il firewall, infatti, garantisce che solo le comunicazioni autorizzate vengano trasferite tra due reti mentre quelle non autorizzate vengono immediatamente bloccate e registrate.

2.3 Vulnerabilità dei dispositivi di protezione

I moderni problemi di sicurezza sono dovuti principalmente a bug o errori di altro tipo presenti nel programma utilizzato.

Le applicazioni sono sviluppate da programmatori che, in quanto esseri umani, possono commettere degli errori.

La situazione diventa ancora più critica quando questi programmatori vengono messi sotto pressione dalle loro stesse aziende affinché introducano nuove funzioni all'interno dei programmi software senza considerare il tempo necessario per valutare gli aspetti relativi alla sicurezza.

Un'altra causa molto comune di scarsa sicurezza è data dalla mancanza di esperienza o di tempo dedicato alla protezione dei sistemi privati. Purtroppo, i consumatori si fidano ciecamente dei produttori di programmi i quali affermano che i loro sistemi vengono commercializzati nella massima sicurezza. In realtà, quasi tutti i fornitori di software sono principalmente interessati a offrire sistemi molto semplici da utilizzare e questo, molto spesso, a discapito della sicurezza. Infatti, un'applicazione facile da usare può essere attaccata con altrettanta semplicità.

2.4 Come funziona un firewall?

Lo scopo principale dell'uso di un firewall è di implementare un insieme di criteri di protezione che definiscono le modalità di una comunicazione e le relative autorizzazioni.

Per eseguire queste operazioni, il firewall analizza il traffico in rete e confronta le informazioni rilevate con un insieme di regole programmato al suo interno, quindi prende una decisione in base a determinati fattori, quali l'indirizzo del mittente e del destinatario, il protocollo e le porte utilizzate. In questo modo, è possibile installare su reti protette applicazioni non troppo sicure evitando, però, l'accesso a utenti non autorizzati.

Quasi tutti i firewall, incluso EnterNet FireWall, garantiscono comunicazioni compatibili con le specifiche dei protocolli attuali. Questo per evitare l'accesso di dati imprevisti che potrebbero provocare l'arresto o il crash dei software client e di server protetti sui quali sono stati installati servizi non protetti.

In conclusione, il firewall è la risposta della rete ai sistemi host poco protetti.

2.5 Quali sono i limiti del firewall?

La sicurezza non viene garantita solo mediante l'utilizzo di firewall. Anche se l'inserimento di un firewall rappresenta il primo passo indispensabile per la protezione di reti e computer.



Questa sezione non è dedicata specificamente a EnterNet FireWall bensì ai firewall in generale. Infatti, i problemi che verranno descritti riguardano tutti i firewall.

I firewall vengono erroneamente considerati come l'unico mezzo necessario a garantire la sicurezza di una comunicazione.

Falso.

Molti responsabili marketing e commerciali affermano sorridendo che i firewall da loro offerti sono in grado di proteggere le reti da *qualsiasi cosa*. Si spera che si tratti di una questione di mera ignoranza da parte loro e non di un tentativo consapevole di ingannare i potenziali acquirenti.



Infatti, un firewall viene progettato per riconoscere determinati elementi che possono violare la sicurezza di un sistema. Tuttavia, non è possibile prevedere tutti i bug che potrebbero essere inclusi nei programmi software. Inoltre, in numerose circostanze un firewall *non può* garantire da solo la protezione di una rete perché semplicemente non riceve tutte le comunicazioni.

Qui di seguito verranno elencati alcuni problemi di sicurezza che spesso i firewall non riescono a gestire. Alcuni esempi includono anche le relative soluzioni.

L'argomento verrà trattato in generale poiché le problematiche in questo campo sono numerose.

Per raggiungere un elevato livello di protezione è innanzitutto necessario conoscere tutti i possibili difetti dei protocolli di rete e dei programmi utilizzati e, successivamente, sarà possibile adottare le soluzioni più appropriate.

2.5.1 Attacchi ai componenti preinstallati non protetti

Spesso i sistemi operativi contengono componenti preinstallati non protetti, i quali includono servizi non documentati presenti sui computer collegati a Internet. Questo consente l'accesso di dati provenienti da reti esterne. Un esempio di questo tipo di vulnerabilità è dato dalla "semplificazione" dei componenti che consentono l'accesso diretto ODBC nei server Web tramite il protocollo HTTP.

La maggior parte di questi componenti non è stata progettata per l'utilizzo su reti pubbliche, in cui si trovano intrusi indesiderati che possono sfruttare le funzionalità aggiuntive ed accedere facilmente nel sistema. Purtroppo, i sistemi moderni vengono spesso commercializzati con tali componenti già integrati per semplificare l'utilizzo del programma.

Una buona precauzione da adottare è di controllare tutti i sistemi collegati a Internet, client e server, e di rimuovere le funzioni non necessarie.

2.5.2 Utenti inesperti di reti protette

Nessun firewall al mondo è in grado di proteggere una rete sicura dai danni provocati da utenti inesperti.

Se questi "collaborano" in qualche modo con un intruso indesiderato, ad esempio aprendo un programma sconosciuto ricevuto per posta elettronica quale "merryxmas2001.exe", rischiano di provocare danni maggiori rispetto ai bug presenti nelle applicazioni e nei sistemi operativi.

Prima di procedere alla protezione delle reti di un'azienda sarebbe pertanto opportuno effettuare un'accurata analisi delle operazioni da autorizzare o meno ai propri utenti. Il risultato di questa indagine dovrebbe portare alla stesura di alcuni *criteri di protezione* da applicare a tutti i settori dell'azienda, a partire dall'amministrazione. È importante che gli utenti siano a conoscenza dei criteri utilizzati e dei motivi per i quali è necessario rispettarli. Solo in questo modo, infatti, le politiche di protezione adottate potranno funzionare.

2.5.3 Attacchi alle reti guidati dai dati

Generalmente, un firewall è in grado di proteggere un sistema da attacchi *guidati dai dati* solo in circostanze speciali. Tali attacchi includono:

- pagine HTML contenenti dati Javascript o Java che attaccano la rete "dall'interno" dopo che la pagina viene visualizzata in un browser o in un programma di posta elettronica. L'unica protezione possibile da questo tipo di attacchi, a parte la compilazione di un programma migliore, consiste nel disabilitare questi servizi oppure nell'autorizzare le connessioni Internet solo ai computer che gestiscono informazioni poco importanti;
- pagine HTML che fanno riferimento al contenuto dei file locali aperti *senza script*. Spesso insospettabili utenti locali vengono attirati, a loro insaputa, a selezionare un pulsante della pagina, e il file a essa collegato viene immediatamente inviato a un server Internet sconosciuto;
- documenti inoltrati per posta elettronica contenenti script pericolosi che vengono attivati dopo l'apertura del documento. Per proteggere il sistema da questi attacchi è necessario evitare l'utilizzo dei programmi di posta elettronica basati su browser oppure disabilitare lo scripting e introdurre gateway di posta in grado di bloccare gli script e qualsiasi altro tipo di codice eseguibile.

- sovraccarico di buffer da cui raramente i firewall riescono a proteggere il sistema. Questo tipo di errore può avvenire in tutte le applicazioni. Ne consegue che gli intrusi indesiderati riescono a ingannare i computer protetti e a fare in modo che essi eseguano qualsiasi comando. In questo caso, l'unica soluzione possibile è di installare e utilizzare solo programmi sicuri e quindi specificamente progettati per essere immuni da questo tipo di attacchi. Purtroppo, quasi tutti gli attuali software *non* vengono sviluppati tenendo in considerazione questo problema. Pertanto, i sovraccarichi di buffer rappresentano l'attacco basato su rete attualmente più pericoloso, poiché coinvolgono la maggior parte dei programmi.
- virus e cavalli di Troia. Anche se un firewall può essere collegato a programmi antivirus, a gateway di posta o ad altri dispositivi simili che consentono di aumentare la sicurezza, è importante ricordare che la funzione fondamentale di un firewall *non* prevede normalmente questo tipo di protezione.
- a volte poi, pur utilizzando il firewall in combinazione con un programma antivirus può succedere che i virus siano nascosti talmente bene da venire ignorati. Inoltre, un programma antivirus è in grado di rilevare solo i virus che riconosce. Se un malintenzionato crea un virus appositamente per attaccare un particolare sistema o un piccolo gruppo di utenti, oppure se il cavallo di Troia o il virus in questione sono in circolazione da poco tempo e quindi sono ancora poco conosciuti, il programma antivirus non sarà in grado di riconoscerlo.

Attualmente, le destinazioni più comuni di questo tipo di attacchi sono:

- server pubblici, ad esempio server di posta elettronica, server DNS e server Web. I server Web sono i più rappresentativi di questa categoria a causa della loro enorme complessità.

- script personalizzati nei server Web. È davvero facile ormai estendere le funzionalità di un server Web compilando piccoli programmi personalizzati in grado di gestire numerose attività. Tuttavia, una scarsa conoscenza dei potenziali problemi è molto spesso causa di piccoli errori, difficili da rilevare, tramite i quali un intruso indesiderato potrebbe riuscire a entrare nel sistema.
- browser Web. I processi di automazione e le operazioni di semplificazione a vantaggio degli utenti aumentano la complessità all'interno del sistema e, di conseguenza, i rischi di vulnerabilità.
- programmi per i computer desktop, principalmente quelli che contengono numerosi script, sono soggetti agli stessi pericoli dei browser. Infatti, i linguaggi di scripting offrono accesso quasi illimitato ai computer locali e a tutte le risorse di rete a essi collegate. Pertanto, gli utenti interni che aprono documenti contenenti script pericolosi sottopongono il sistema a qualsiasi tipo di problema.

2.5.4 Attacchi interni

Un firewall è in grado di filtrare solo i dati che *riceve*. Pertanto, non garantisce alcuna protezione dagli attacchi interni alle reti locali tramite le quali tutti i computer comunicano tra loro direttamente.

Inoltre, i firewall non possono garantire la protezione del sistema quando gli utenti locali utilizzano dischi floppy per installare programmi pericolosi in rete oppure per esportare informazioni delicate.

Questo punto potrebbe sembrare ovvio. Tuttavia, quasi tutti gli utenti sottovalutano l'effetto di questo tipo di danni.

Anche se le cifre variano in base alle fonti, è ormai certo che più del 50% di tutti i problemi relativi alla sicurezza dei dati derivano da attacchi interni. Secondo alcune statistiche questa percentuale ammonta addirittura all'80%.

2.5.5 Connessioni modem e VPN

Spesso i gateway VPN e i modem vengono considerati sicuri come una rete protetta e quindi vengono collegati direttamente a essa senza alcuna protezione.

Purtroppo, i gruppi di modem possono essere soggetti ad attacchi diretti e, in casi estremi, è possibile intercettare le linee telefoniche. Qualsiasi intruso indesiderato, infatti, potrebbe riprogrammare in remoto i parametri di qualsiasi centralino posto sulla rete di telecomunicazioni.

Per quanto riguarda i collegamenti VPN, è importante ricordare che anche se la connessione stessa è ben protetta, il livello generale di sicurezza è direttamente proporzionale a quella dei punti finali del tunnel.

Sempre più di frequente gli utenti in viaggio per lavoro effettuano connessioni VPN tra i laptop e la rete della loro società. Tuttavia, tali portatili spesso non sono protetti. In sostanza, un intruso indesiderato può accedere alla rete provvista di protezione di una società tramite un laptop non protetto e connessioni VPN già aperte.

Quindi, per proteggere la rete dagli attacchi derivanti da connessioni VPN e modem, si consiglia di evitare di collegare direttamente i portatili a Internet. Sarebbe opportuno, piuttosto, instradare le comunicazioni attraverso la connessione modem o VPN e la rete dell'azienda, indipendentemente dal destinatario del messaggio. Solo in questo modo è possibile garantire più o meno lo stesso livello di sicurezza del resto della rete. Per le connessioni VPN è possibile installare sul portatile un apposito client in grado di bloccare tutto il traffico Internet in ingresso, ad eccezione dei dati che passano attraverso la connessione VPN.



Una connessione VPN o una combinazione di modem non dovrebbe mai essere considerata come parte diretta di una rete protetta. Sarebbe invece opportuno posizionare i punti finali VPN in una speciale rete demilitarizzata o all'esterno di un firewall dedicato a questo scopo. In questo modo, è possibile limitare l'accesso tramite modem e VPN a determinati servizi per proteggerli da attacchi pericolosi.

Se un firewall contiene un gateway VPN integrato, è generalmente possibile stabilire i tipi di comunicazione autorizzati. Il modulo IPsec VPN di EnterNet FireWall supporta proprio questa funzione.

2.5.6 Buchi tra zone demilitarizzate e reti interne

Le connessioni extranet e il commercio elettronico hanno aperto nuove frontiere di sviluppo. L'aumento della presenza di aziende in Internet, che pubblicano i propri dati interni mediante server Web, ha esteso di conseguenza i pericoli relativi alla sicurezza delle informazioni.

È diventata ormai una prassi molto comune posizionare i server Web in zone demilitarizzate, che consentono di comunicare con le fonti di dati situate nelle reti protette. In questi casi, gli attacchi guidati dai dati rappresentano un pericolo enorme.

I buchi tra le zone demilitarizzate e le reti interne possono rappresentare un vero problema se utilizzati in modo errato. Infatti, molti utenti aprono tali buchi senza considerare i problemi che ne potrebbero derivare. Perciò questo argomento è stato trattato in una sezione separata.

Dal momento che non è possibile considerare un server Web immune da qualsiasi rischio, si è pensato di posizionarlo in una zona demilitarizzata. Se però un intruso indesiderato riesce a prendere il controllo di un server che presenta un buco aperto, potrà accedere grazie a esso ai dati di una rete interna. Il risultato è che la rete “protetta” è soggetta ad attacchi esterni che utilizzano proprio il server Web come intermediario.



Non bisogna sottovalutare gli effetti di questa vulnerabilità!

Persino i pirati informatici meno esperti riescono ad accedere in pochi minuti a reti protette utilizzando tecniche ormai note e standardizzate, progettate appositamente per sfruttare questo tipo di buchi.

La difesa più semplice da tali attacchi consiste nell’aumentare la segmentazione della rete. Se si posiziona l’origine dei dati, ad esempio un server SQL, in un segmento separato della rete in modo da impedire le comunicazioni dirette con il resto del sistema, è possibile limitare i danni provocati dagli attacchi tramite i buchi.



Nota: in questo caso, il problema non è rappresentato dai pacchetti IP instradati alla zona demilitarizzata tramite i server, il cui inoltro potrebbe venire disabilitato per *non* garantire più alcuna protezione. Il rischio maggiore consiste nel fatto che intrusi indesiderati possono eseguire comandi sui server proprio come da una qualsiasi tastiera di un computer dell’azienda.



Tuttavia, anche se il canale tra la zona demilitarizzata e la rete stessa è costituito da protocolli non instradabili, quali NetBEUI, una rete interna può comunque essere soggetta ad attacchi pericolosi. Anche in questo caso, il problema non è rappresentato dai pacchetti IP che viaggiano da reti non protette verso una rete interna. Piuttosto, c’è il rischio che macchine non protette eseguano comandi su quelle “protette”.

Un altro tipo di protezione degna di considerazione consiste nel creare un'origine dati separata che includa un numero limitato di informazioni accessibili da parte del server Web. Ovviamente, i dati disponibili dovranno essere poco importanti. Per realizzare questa procedura è necessario effettuare l'esportazione automatica delle informazioni dall'origine dati esterna a quella interna ogni volta che è necessario aggiornare i dati. In alternativa, è possibile eseguire questa operazione in ore programmate della giornata. Un problema di difficile risoluzione potrebbe verificarsi qualora fosse necessario aggiornare l'origine dei dati nel server Web. In questo caso, la soluzione migliore è spostare l'origine dei dati in questione in un segmento separato della rete per ridurre gli eventuali danni provocati da accessi indesiderati.

2.6 Quali sono i bersagli degli attacchi?

Per motivi di maggiore sicurezza, tutti utilizzano una porta d'ingresso munita di serratura e, a volte, anche un sistema di allarme.

Dal momento che le transazioni commerciali, anche di notevole importanza, eseguite attraverso i computer aumentano con enorme rapidità, non è più possibile ignorare i pericoli esistenti.

A volte le informazioni archiviate in un computer, ad esempio annotazioni su clienti e offerte, vengono considerate poco importanti. Tuttavia, è facile immaginare quali sarebbero le conseguenze se alcuni articoli non ancora fatturati dovessero scomparire all'improvviso oppure se fosse necessario ricompilare un'offerta con il conseguente rischio di perdere un appalto.

Per ulteriori informazioni si consiglia di visitare l'indirizzo <http://www.attrition.org/mirror/attrition/> in cui si può consultare l'elenco delle aziende i cui siti sono stati distrutti dai pirati informatici, insieme alle copie di tali siti dopo il terribile evento. Vengono rappresentati tutti i tipi di organizzazioni, dal fioraio di quartiere alle basi militari. Anche se le violazioni a un sito Web non provocano danni molto gravi, l'elenco include esempi significativi di aziende vittime di attacchi che non avrebbero mai pensato in passato di diventare bersaglio di pirati informatici.

I pirati informatici più pericolosi dai quali bisogna proteggersi, indipendentemente dalle aziende prese di mira, sono i “cibervandali”. In genere, scelgono il bersaglio casualmente, prediligendo i sistemi meno protetti. I danni che possono provocare sono di vario tipo e misura, dalla cancellazione di dischi rigidi e modifica di siti Web alla modifica di documenti e fatture. I più fortunati ricevono un messaggio che commenta in modo negativo la sicurezza del loro sistema.

I rischi sono talmente numerosi che il denaro necessario per acquistare un firewall rappresenta una minima parte delle spese che bisogna investire in altri dispositivi per la sicurezza e il lavoro. Infatti, finché i sistemi standard saranno distribuiti in condizioni non protette e con una struttura interna sempre più complessa, non sarà possibile ridurre i costi relativi alla sicurezza. Anzi, continueranno ad aumentare.

I pericoli sopra citati rappresentano solo la punta dell’iceberg. Del resto le misure che è necessario adottare per poter ritenere un sistema “sicuro” sono così numerose che non è possibile trattarle tutte insieme.

Se all’interno dell’azienda non sono disponibili tecnici esperti in sicurezza, è consigliabile rivolgersi a consulenti esterni per elaborare una buona struttura di rete, “rafforzare” i server e le workstation, configurare il firewall e quindi collaudare tale configurazione dall’esterno.

3. EnterNet FireWall

3.1 Panoramica su EnterNet FireWall

EnterNet FireWall rappresenta la soluzione più economica per la protezione delle reti, idonea a tutti i tipi di aziende. Grazie alle elevate prestazioni, allo straordinario livello di sicurezza, al basso costo ed alla efficiente tecnologia di protezione utilizzata, EnterNet FireWall costituisce la scelta ideale per la sicurezza delle reti interne ed esterne.

3.2 Funzioni di EnterNet FireWall

Nessun sistema operativo

EnterNet FireWall non utilizza alcun sistema operativo. Questo significa che il rischio di attacchi al firewall praticamente non esiste, visto che non c'è nulla da attaccare. La procedura di installazione risulta quindi notevolmente accelerata e semplificata perché non è necessario “consolidare” i sistemi operativi. Viene inoltre eliminata la necessità di effettuare aggiornamenti o di installare patch aggiuntivi che potrebbero alterare le funzionalità del firewall.

Prestazioni senza paragoni

In assenza di un sistema operativo, EnterNet FireWall utilizza esclusivamente le funzioni hardware, rendendolo pertanto uno dei firewall più veloci attualmente disponibili sul mercato.

Stateful inspection

EnterNet FireWall utilizza la tecnologia stateful inspection che consente al firewall di funzionare in modo più rapido ed efficiente. Tale funzione richiede un minor utilizzo della CPU rispetto ai firewall proxy. Questo consente di raddoppiare le prestazioni e richiede specifiche hardware notevolmente inferiori. Inoltre, con la tecnologia stateful inspection il firewall risulta invisibile alla rete protetta. Di conseguenza, non è necessario che gli host protetti siano a conoscenza della presenza del firewall dal momento che non sono richieste impostazioni proxy. Questo semplifica le procedure di configurazione di EnterNet FireWall per la gestione dei nuovi protocolli. Infatti, non è più necessario attendere che fornitori di terze parti sviluppino sistemi proxy per i nuovi protocolli.

64 interfacce separate

EnterNet FireWall 6.0 supporta fino a 64 schede di rete, ad esempio una connessione esterna a Internet, un'interfaccia alla rete interna e una o più reti separate con server protetti accessibili solo pubblicamente.

Traffic Shaping

Grazie alle funzioni di traffic shaping EnterNet FireWall può essere utilizzato per limitare, garantire o assegnare priorità ai messaggi che raggiungono il firewall.

Elevata disponibilità

È possibile creare un sistema firewall ridondante aggiungendo la funzione opzionale di elevata disponibilità (High Availability).

Configurazione e controllo remoto

La configurazione viene eseguita tramite un'applicazione Windows, denominata EnterNet FireWall Manager, e memorizzata in un database basato su file o compatibile con ODBC. Per aumentare il livello di sicurezza, il trasferimento delle informazioni a EnterNet FireWall viene effettuato utilizzando una crittografia a 128 bit.

Le informazioni relative alla configurazione vengono pertanto archiviate in due posizioni diverse, nel firewall e nel database. Se per qualsiasi motivo l'hardware del firewall dovesse arrestarsi, sarà comunque possibile trovare nel database le informazioni necessarie per configurare un nuovo firewall.

Filtri

EnterNet FireWall supporta filtri configurabili per:

- gli indirizzi sorgente e di destinazione
- le interfacce sorgente e di destinazione
- gli indirizzi IP "spoofed"
- i numeri di protocollo IP
- i numeri di porte TCP e UDP
- messaggi ICMP
- le connessioni nuove/esistenti
- i tipi di opzioni nei protocolli IP e TCP
- le combinazioni di flag nei protocolli IP e TCP
- le sovrapposizioni o i frammenti non validi

Zone demilitarizzate (DMZ, Demilitarized Zones)

È possibile posizionare nelle zone demilitarizzate i server accessibili pubblicamente e collegarli a EnterNet FireWall tramite un'apposita scheda di rete separata. Questa procedura consente di proteggere i server e fare in modo che essi non rappresentino un pericolo per la rete interna. Infatti, sarà impossibile utilizzarli come mezzo per attaccare la rete. EnterNet FireWall consente di creare numerose zone separate collegate tra loro tramite interfacce firewall distinte.

Traduzione dell'indirizzo di rete (NAT, Network Address Translation)

EnterNet FireWall supporta la traduzione dinamica degli indirizzi, spesso denominata "NAT Hide", "NAT Dynamic" o "IP masquerading".

Gli indirizzi IP delle reti protette vengono nascosti all'esterno e tutto il traffico in uscita sembra provenire da un unico indirizzo, ovvero l'indirizzo IP esterno del firewall. È inoltre possibile specificare l'indirizzo di origine utilizzato dai vari utenti.

Traduzione statica dell'indirizzo (SAT– Static Address Translation)

Conosciuta anche come NAT Static, consente al firewall di pubblicare uno o più indirizzi IP tramite una scheda di rete esterna e quindi di inoltrare i dati ad altri indirizzi IP di una rete interna. Tale funzione consente inoltre di tradurre gli indirizzi non pubblicati sul firewall a condizione che il traffico verso questi indirizzi non venga instradato attraverso il firewall. La funzione SAT può essere utilizzata per l'accesso da Internet ai server interni che includono indirizzi privati oppure per effettuare una traduzione dell'indirizzo temporanea durante il trasferimento di un host.

Coerenza dei pacchetti

Tutti i pacchetti che raggiungono il firewall sono soggetti a una serie di test strutturali relativi alle dimensioni dell'intestazione, alle opzioni, alla frammentazione e ai flag. Tali test consentono di proteggere la rete dagli attacchi a livello di trasporto di tipo "Denial of service", ad esempio WinNuke, Teardrop, Boink, Land, Nestea e relative variazioni.

Struttura simmetrica

EnterNet FireWall è completamente "simmetrico". Ciò significa che il firewall non richiede la connessione di tutte le interfacce a un sistema "interno, "esterno" o di altro tipo. Pertanto, può essere utilizzato per collegare organizzazioni o uffici che non sono in rapporti confidenziali oppure per proteggere un'azienda da attacchi Internet.

Nascondere le informazioni

Un aspetto importante della sicurezza di una rete è di nascondere il maggior numero di informazioni possibili sulla rete protetta, ad esempio tramite la traduzione degli indirizzi. Tuttavia, sarebbe molto importante coprire anche i dati relativi al sistema operativo e al numero di versione utilizzati. Questo per evitare che intrusi indesiderati riescano a ottenere informazioni anticipate sul tipo di attacco da adottare.

Tuttavia, pur nascondendo tali informazioni la sicurezza non è garantita poiché i pirati informatici potranno comunque raggiungere il loro obiettivo anche se gli sforzi necessari per eseguire questa operazione saranno maggiori.

EnterNet FireWall supporta la protezione attiva per il "fingerprinting" del sistema operativo e il "firewalking".

IPsec VPN

È possibile trasformare il firewall in un gateway VPN ad elevate prestazioni, completamente compatibile con gli standard Ipsec, semplicemente aggiungendo un componente VPN EnterNet opzionale. La configurazione, integrata in EnterNet FireWall Manager, consente l'amministrazione simultanea delle connessioni VPN e dei criteri di protezione del firewall.

3.3 Componenti del sistema

Il sistema EnterNet FireWall è composto da tre componenti principali:

EnterNet FireWall Core

Il software del FireWall è il componente centrale del sistema, ovvero il programma eseguito all'interno del firewall stesso.

EnterNet FireWall Manager

FireWall Manager viene utilizzato per amministrare il firewall, prima dell'avvio e, successivamente, per il controllo in remoto. È possibile installare ed eseguire l'applicazione in Windows 95, 98, NT 4.0, Windows 2000 e Windows Me.

Tutte le informazioni relative alla configurazione del firewall sono archiviate centralmente come insieme di file di dati oppure in uno o più database compatibili con ODBC. All'interno di questo documento, l'archivio dei dati relativi alla configurazione verrà denominata *origine dati*, indipendentemente dal tipo di memoria utilizzato.

È possibile installare, configurare ed eseguire EnterNet FireWall senza FireWall Manager. Tuttavia, questa procedura non è consigliata agli utenti meno esperti.

EnterNet FireWall Logger

FireWall Logger consente di ricevere e archiviare i dati di log provenienti dal firewall. Per ridurre l'utilizzo dei dispositivi hardware e migliorare le prestazioni, non avviene alcuna registrazione all'interno del computer firewall. Piuttosto, i dati vengono memorizzati nella macchina sulla quale è stato installato FireWall Logger come servizio.

Generalmente si tratta di server o workstation che eseguono Windows NT 4.0 o successivo. Attualmente sono in corso aggiornamenti di FireWall Logger per renderlo compatibile con i vari linguaggi Unix. Ogni firewall può inviare dati di log a un massimo di otto FireWall Logger. EnterNet FireWall è in grado di inviare dati di log ai terminali syslog.



Se il sistema viene utilizzato solo per quest'ultimo tipo di trasmissioni, non sarà necessario installare FireWall Logger.

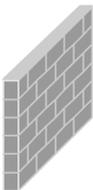
3.4 Esempi di architetture di rete

I firewall tradizionali vengono spesso progettati per uno scopo particolare, ovvero la protezione perimetrale, e supportano una connessione a Internet, un collegamento a una rete interna e una o più connessioni alle zone demilitarizzate (generalmente una sola per i firewall più semplici).

EnterNet FireWall inoltre ha una struttura completamente simmetrica che, unitamente alle elevate prestazioni e alle numerose possibilità di interfacciamento, ne fanno uno strumento molto flessibile. Infatti, può essere utilizzato in svariate situazioni, dalla protezione di semplici connessioni Internet, alla segmentazione di complesse reti aziendali e persino nelle soluzioni distribuite per la sicurezza in situazioni ASP o ISP.

Questa sezione include alcuni esempi schematici delle diverse situazioni di utilizzo di EnterNet FireWall.

È necessario fare alcune considerazioni sull'ubicazione all'interno di una rete di componenti importanti quali FireWall Manager e FireWall Logger. Negli esempi seguenti alcuni computer verranno contrassegnati con i simboli illustrati qui di seguito, i quali rappresentano i diversi componenti.



EnterNet FireWall

Il dispositivo hardware che esegue il software di EnterNet FireWall.



EnterNet FireWall Manager

Una workstation o un server basato su Windows che esegue il programma EnterNet FireWall Manager.

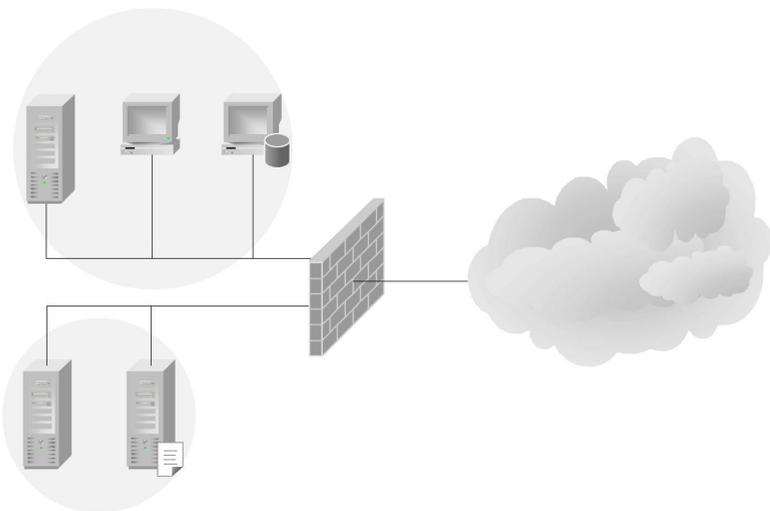


EnterNet FireWall Logger

Una workstation o un server che esegue il servizio e/o daemon EnterNet FireWall Logger.

Potrebbe anche trattarsi di un server che esegue un sistema di ricezione di dati di log con formato syslog.

3.4.1 Esempio 1: soluzione di protezione perimetrale tradizionale

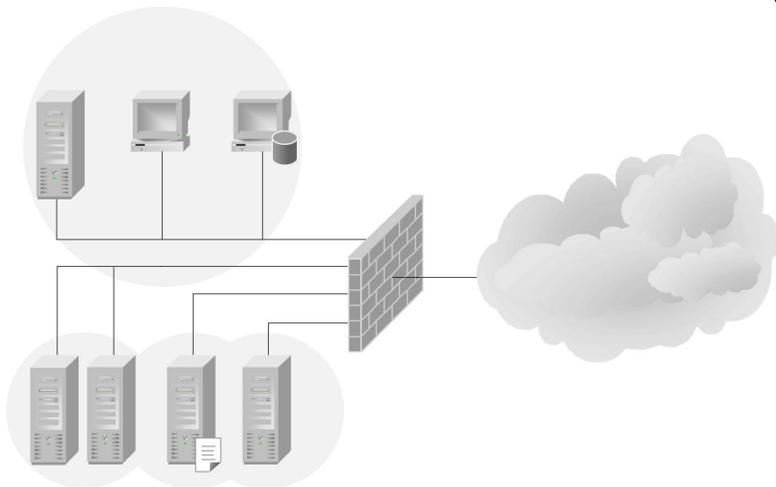


Nella figura viene illustrato l'uso di EnterNet FireWall in una soluzione di protezione perimetrale tradizionale.

Il firewall ha tre schede di rete, di cui una viene utilizzata per le connessioni Internet e un'altra per i collegamenti a una rete interna sulla quale è installata una workstation che esegue EnterNet FireWall Manager.

Infine, la terza scheda di rete è collegata a una zona demilitarizzata che ospita due server, uno dei quali esegue il servizio EnterNet FireWall Logger.

3.4.2 Esempio 2: soluzione di protezione segmentata



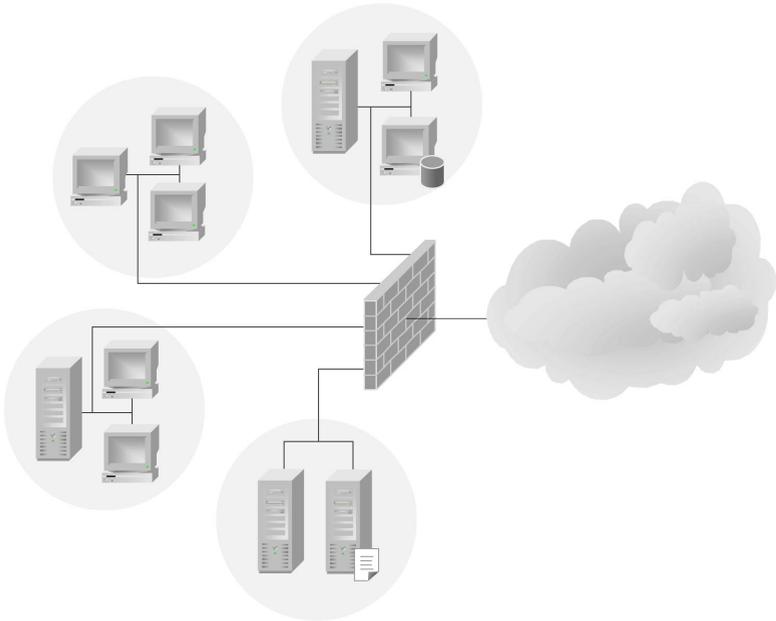
Da un punto di vista della sicurezza non è mai consigliabile installare nello stesso segmento di rete più server ad accesso pubblico. Infatti, indipendentemente dal fatto che il segmento rappresenti una zona demilitarizzata o meno, un singolo segmento di rete costituisce sempre una strada aperta agli intrusi indesiderati.

Per questo motivo, è necessario segmentare il più possibile le reti che contengono server pubblici. In questo esempio viene illustrato l'uso di EnterNet FireWall in una soluzione che prevede un'elevata segmentazione della rete.

Il firewall ha cinque schede di rete, di cui una viene utilizzata per le connessioni Internet e un'altra per i collegamenti a una rete interna sulla quale è installata una workstation che esegue EnterNet FireWall Manager.

In questo caso, però, sono presenti tre diverse zone demilitarizzate, due delle quali sono state appositamente progettate per ospitare un solo server ciascuna per motivi di sicurezza.

3.4.3 Esempio 3: segmentazione di una rete aziendale

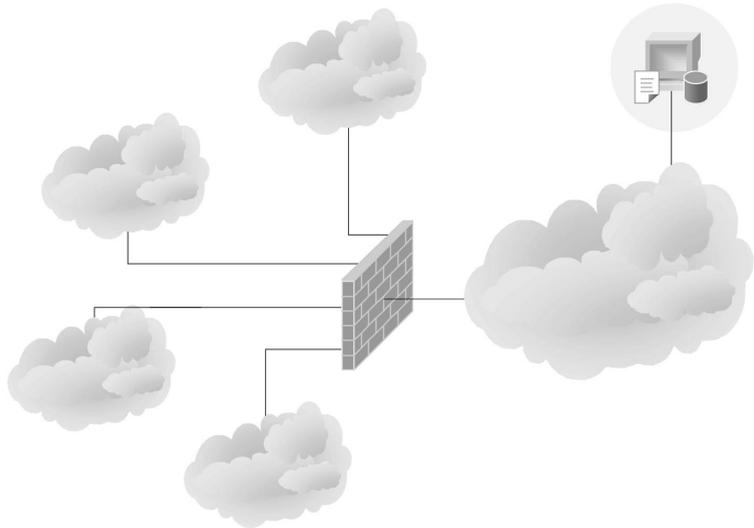


È ormai certo che la maggior parte degli accessi indesiderati alle reti sono provocati da utenti che si trovano *all'interno* di un'azienda. Questo discorso è valido in modo particolare per le grandi aziende.

Quindi, la protezione reciproca di ogni singola parte di una rete aziendale è importante quanto la sicurezza di tutto il sistema dagli attacchi Internet.

La figura illustra l'uso di EnterNet FireWall in una soluzione nella quale i diversi reparti di una rete aziendale sono protetti uno dall'altro oltre che da Internet. L'implementazione di questo tipo di soluzione non deriva necessariamente dalla mancanza di fiducia nel personale dipendente. Piuttosto, la segmentazione di una rete interna consente di limitare la diffusione di eventuali problemi. Infatti, se un pirata informatico o un virus riesce a entrare nella rete di un reparto, la segmentazione consentirà di ridurre i danni conseguenti.

3.4.4 Esempio 4: soluzione firewall ISP/ASP



Nelle reti a banda larga e in altri ambienti nei quali connessioni Internet e altri servizi basati su IP devono essere distribuiti a società e utenti privati, sono principalmente richiesti larghezza di banda, disponibilità e controllo del traffico.

Questo esempio illustra l'uso di EnterNet FireWall in uno scenario in cui il firewall non solo protegge numerosi utenti ma consente anche di limitare o garantire la larghezza di banda a ciascun cliente nonché di analizzare l'utilizzo della rete.

3.5 Modello di licenza di EnterNet FireWall

3.5.1 Modello di licenza

Queste sezioni includono una breve panoramica sul modello di licenza di EnterNet FireWall.

3.5.1.1 Licenza

Per ogni firewall utilizzato è necessario collegare un'apposita chiave hardware alla porta parallela. Altrimenti, il firewall funzionerà solo in modalità demo e sarà necessario riavviarlo ogni due ore. Ciascuna chiave corrisponde a una licenza per l'utilizzo di una copia di EnterNet FireWall.

3.5.1.2 Utenti

EnterNet FireWall viene concesso in licenza in base al numero di utenti che dovranno utilizzarlo.

Per "utente" si intende il numero di computer (workstation, server o altri dispositivi di rete che utilizzano il protocollo TCP/IP) installati sulle reti appositamente configurate per comunicare attraverso il firewall.

3.5.1.3 Numero di licenza

Ogni prodotto EnterNet è munito di un solo numero di licenza che è riportato sul Certificato di autenticità incluso nella confezione.

Il numero di licenza consente di registrare il nuovo prodotto e ne garantisce l'autenticità.



Se per qualsiasi ragione tale numero dovesse andare perduto, contattare il proprio fornitore per riceverne uno nuovo.

3.5.2 Gestione delle licenze Enternet tramite pagine Web

EnterNet utilizza un sistema di gestione delle licenze tramite pagine Web che include aggiornamenti e supporti tecnici per i vari prodotti.

Per usufruire di questo servizio, si consiglia di registrare i dati dell'azienda fin dal primo utilizzo del servizio di gestione delle licenze EnterNet tramite pagine Web.



Le informazioni inserite sono protette e verranno utilizzate solo all'interno di EnterNet. Per motivi di privacy, esse non verranno pubblicate sulle pagine Web di EnterNet nemmeno durante la connessione. Tutti i nomi e gli indirizzi specificati verranno inviati a un server interno tramite una connessione unidirezionale, pertanto non saranno mai archiviati nel server stesso.

Il servizio di gestione delle licenze Enternet mediante pagine Web è disponibile all'indirizzo www.enternet.net.

4. Hardware e prestazioni del firewall

4.1 Panoramica

Per scegliere la soluzione firewall più idonea alle proprie esigenze, è innanzitutto necessario conoscere come i vari dispositivi hardware e le configurazioni disponibili ne influenzano le prestazioni e l'affidabilità.

Questo capitolo contiene una descrizione delle diverse soluzioni in commercio, dei requisiti minimi necessari per garantire l'esecuzione del firewall e dei criteri da considerare durante la scelta dell'hardware per raggiungere elevate prestazioni e affidabilità.

4.2 Prestazioni del firewall

È difficile definire con precisione le prestazioni del firewall, a causa delle diverse esigenze, della struttura della rete e delle varianti nella distribuzione del tipo di protocollo.

Tuttavia, sono disponibili alcuni sistemi di misura che semplificano questa procedura.

Larghezza di banda, bps (bit al secondo)

La misurazione della larghezza di banda consente di definire il numero di dati che un sistema è in grado di trasmettere in un determinato lasso di tempo.

Flusso di pacchetti, pps (pacchetti al secondo)

La misurazione del flusso di pacchetti consente di definire il numero di pacchetti al secondo che un sistema è in grado di trasmettere in un determinato lasso di tempo.

Latenza, ms (millisecondi)

La misurazione della latenza consente di definire il ritardo con il quale un pacchetto dati viene trasmesso dal sistema.

È possibile utilizzare tali sistemi di misurazione in un paio di test campione che, insieme o da soli, possono offrire una panoramica delle prestazioni di un determinato sistema firewall.

Prestazioni del software

La funzione Core Software Performance indica le prestazioni del firewall software in un determinato dispositivo hardware. In genere, questo tipo di test viene eseguito creando un numero di interfacce loopback (interfacce software) all'interno della configurazione firewall e facendo quindi eseguire un loop nel software firewall al traffico di rete generato automaticamente.

Approssimativamente, il software di EnterNet FireWall raggiunge una larghezza di banda di circa 4 Gbps su un processore Intel Pentium III da 733 MHz.

Tramite il test Core Software Performance è quindi possibile stabilire la velocità del programma ma non il livello esatto di prestazioni di un firewall. Per questo motivo, è necessario eseguire un test che coinvolga le componenti hardware di rete.

Velocità di trasmissione

La funzione Raw Network Throughput consente di eseguire test campione sul traffico di rete fisico. Il test viene effettuato collegando tra loro le interfacce del firewall e quindi lasciando eseguire un loop nel sistema al traffico di rete generato automaticamente che presenta la massima dimensione di pacchetto. Questa configurazione da un'idea delle reali capacità di trasmissione dati del firewall. Se però alle dimensioni del pacchetto si unisce l'apertura e la chiusura di numerose connessioni, il numero riportato sarà inferiore. È comunque difficile stabilire una "combinazione" ideale e i risultati derivanti dall'esecuzione di due test sarebbero immancabilmente diversi. In questo senso, la velocità effettiva della rete risulta migliore quando si valutano le prestazioni di un sistema poiché il numero di dati emesso sarà sempre lo stesso, indipendentemente da chi effettua il test.

4.3 Scelta dei componenti hardware

Per eseguire EnterNet FireWall è necessaria una capacità hardware ridotta. Questo perché il software del firewall è di piccole dimensioni ed estremamente ottimizzato. Un sistema firewall completo include i seguenti componenti essenziali:

- CPU Intel compatibile : 486 a 25 Mhz
- RAM 4 MB
- Scheda madre
- Supporti di avvio: Unità floppy, flash rimovibile, disco su chip, disco su modulo o disco rigido
- 2 schede di rete
- Una porta parallela

Per eseguire EnterNet FireWall non è necessario utilizzare schede grafiche, monitor o tastiere. Tuttavia, durante la configurazione iniziale si consiglia di collegare al firewall un monitor e una tastiera. Tali dispositivi sono inoltre necessari per definire le impostazioni della scheda di rete che consentono di configurare ed eseguire il firewall.

EnterNet FireWall non necessita di un'unità disco rigido. Infatti, se si sceglie di avviare il firewall da un supporto non meccanico, ad esempio una piccola unità flash, esso non presenterà parti mobili a tutto vantaggio di una maggiore stabilità del sistema. Un disco flash da 4 MB sarà sufficiente per archiviare le espansioni successive.

L'utilizzo di dischi floppy presenta degli svantaggi non tanto nelle prestazioni, dal momento che un firewall in funzione non accede alle memorie di massa, bensì nei tempi di avvio che risultano più lenti. Del resto, i dischi floppy non sono certamente noti per la loro eccellente stabilità durante le lunghe procedure di elaborazione.

4.3.1 CPU

È possibile eseguire EnterNet FireWall 6.0 su tutti i tipi di processori Intel x86 (e compatibili), a partire da Intel 486 a 25 Mhz.

La scelta della CPU è importante per le prestazioni del firewall fino a una certa larghezza di banda.

Generalmente, un sistema con più processori *non* aumenta le prestazioni di EnterNet FireWall.

L'elenco seguente illustra come varia la larghezza di banda in base al processore e ai relativi componenti hardware utilizzati. Tuttavia, i grafici che raffigurano la larghezza di banda sono approssimativi. Infatti, esistono tanti altri fattori e componenti che incidono sulle prestazioni.

CPU	Larghezza di banda
486 25 Mhz	2 Mbps
Pentium 90 Mhz	50 Mbps
Pentium II 233 Mhz	200 Mbps
Pentium III 500 Mhz	300 Mbps
Pentium III 733 Mhz	400 Mbps

4.3.2 RAM

Poiché il software di EnterNet FireWall occupa meno di 512 KB, sarà possibile utilizzare la memoria del sistema principalmente per i buffer dei pacchetti e le voci della tabella di stato (connessioni).

La quantità di memoria utilizzata dal sistema dipende dal numero delle interfacce di rete, dal numero di utenti e dalla scelta dei moduli del software del firewall abilitato.

La memoria minima richiesta è di 4 MB (8 o 16 MB per le configurazioni di sistema più estese).

Le prestazioni dei chip di memoria più moderni sono di gran lunga superiori alla velocità di trasferimento dei bus PCI, pertanto è possibile utilizzare qualsiasi tipo di memoria. Tuttavia, negli ambienti ad elevate prestazioni (numerose centinaia di Mbps) è consigliabile installare i chip di memoria più veloci .

4.3.3 Scheda madre/bus di sistema

La scelta dei bus di sistema e della CPU è importante per raggiungere prestazioni elevate del firewall.

EnterNet FireWall supporta i tipi di bus PCI, ISA e EISA; consultare la sezione 4.3.5, Schede di rete.

Per ottenere le massime prestazioni è consigliabile utilizzare i bus PCI. Per questo motivo, nella seguente sezione verranno illustrate solamente le modalità di installazione di un sistema PCI appropriato.

Il bus PCI rappresenta un supporto condiviso, ovvero consente a EnterNet Firewall solamente di inviare e ricevere dati sulla stessa interfaccia di rete alla volta. Di conseguenza, la velocità complessiva del bus PCI verrà condivisa da tutte le interfacce di rete a esso collegate.

Inoltre, la velocità massima di un bus PCI dipende da numerosi fattori, ad esempio le dimensioni dei relativi bit, la frequenza utilizzata e la qualità delle componenti circostanti, quali i chipset PCI, gli adattatori PCI e così via.

Un bus PCI a 32 bit con frequenza di 33 MHz può raggiungere teoricamente una velocità massima di circa 1,2 Gbps in modalità burst. Tuttavia, durante l'invio o la ricezione di pacchetti di rete che contengono parti di dati la velocità massima effettiva corrisponde a 600 Mbps.

Infatti, per l'elaborazione di ogni pacchetto dati da parte del firewall sono necessari almeno due insiemi di cicli PCI, uno per la lettura dall'interfaccia di rete in ingresso e uno per la scrittura sull'interfaccia in uscita.

Quindi, la larghezza di banda effettiva che passa attraverso il firewall presenta una velocità pari alla metà di quella del bus PCI. Nel caso di un bus a 32 bit con frequenza di 33 MHz la larghezza di banda massima sarà di circa 300 Mbps.

È comunque possibile utilizzare le seguenti configurazioni hardware.

- Utilizzare un bus PCI con frequenza e ampiezza di dati elevate, ad esempio a 64 bit e 66 MHz. Questo consentirà di quadruplicare la velocità. Tuttavia, per garantire un aumento delle prestazioni, è necessario che anche gli altri componenti del sistema, ad esempio i bus degli indirizzi e dei dati tra la CPU, la memoria e il controller PCI siano appositamente progettate per le alte velocità.
- Utilizzare una scheda madre con bus PCI singoli e doppi. I bus singoli lavorano indipendentemente l'uno dall'altro. Posizionando le interfacce di rete in modo da distribuire equamente il relativo carico tra i due bus PCI sarà possibile in teoria raddoppiare le prestazioni.



Molti sistemi contengono più di un numero bus. Questo *non* significa necessariamente che includano più bus singoli, ma semplicemente che il primo bus potrebbe essere stato esteso con una scheda PCI per ottenere più slot PCI disponibili e non tanto per ottimizzare la velocità.

4.3.4 Supporti di avvio

Il software EnterNet FireWall insieme ai file di avvio, i file di configurazione e i driver occupano meno di 1 MB di memoria. L'accesso ai dispositivi utilizzati per l'archiviazione di tali file viene effettuato solo all'avvio del sistema e durante le operazioni di amministrazione remota. Inoltre, poiché tutti i log vengono inviati ai relativi sistemi di ricezione nella rete, il firewall non necessita di un'unità disco rigido di supporto.

Durante l'installazione, FireWall Manager crea un supporto di avvio con i file necessari al funzionamento del firewall. In questo modo, è possibile avviare ed eseguire il firewall direttamente dal supporto di avvio creato senza coinvolgere le componenti hardware del firewall.

EnterNet FireWall Manager è in grado di creare file di avvio su qualsiasi supporto avviabile, dato che quest'ultimo può essere rappresentato persino da un normale file di Windows. Generalmente, EnterNet FireWall viene eseguito da un *disco flash* o *floppy*.

Tuttavia, in configurazioni critiche, si consiglia di utilizzare un disco flash in modo da eliminare quasi tutte le parti mobili del firewall e ridurre quindi il rischio di errori hardware.

Le unità disco su modulo consentono di semplificare le operazioni e garantiscono maggiore stabilità. Inoltre, sono abbastanza economiche e possono essere collegate direttamente ai socket IDE. Per trasferire i file di avvio alle unità disco su modulo, è possibile connettere tali unità a un socket IDE nella workstation di amministrazione. In alternativa, è possibile creare un disco floppy di avvio e inviare i file al disco su modulo della stessa macchina firewall.

4.3.5 Schede di rete

EnterNet FireWall contiene i driver integrati per le schede 3Com serie 3c905B/C e per le interfacce di rete basate sui chip Ethernet DEC/Intel 21x4x (ad esempio, DEC 21140). Queste ultime supportano schede di rete di vari fornitori tra i quali, Accton, Adaptec, Cogent e D-Link.

EnterNet FireWall supporta un massimo di 64 interfacce di rete simultanee in un sistema.

Nota: i driver incorporati *non* supportano il modello originale 3c905 ma solo i modelli 3c905B e 3c905C, ovvero gli unici in commercio da alcuni anni.

Per motivi di compatibilità con i sistemi esistenti, EnterNet FireWall supporta anche tutti i tipi di schede di rete che presentano driver ODI a 16 bit, come quelli utilizzati da Novell Netware. I driver ODI per le schede 3Com 3c509 EtherLink III, 3Com 3c905 Fast EtherLink 10/100 e Intel EtherExpress Pro/100 sono inclusi nel pacchetto software.



Per garantire le massime prestazioni, si consiglia di utilizzare solo i driver integrati. I driver ODI non possono utilizzare le memorie buffer dei pacchetti posizionati oltre 1MB di RAM e funzionano in modalità 16 bit. Per questo motivo, durante l'invio e la ricezione dei pacchetti, il software del firewall è costretto a ridurre il relativo numero di memorie buffer e a effettuare passaggi tra la modalità a 32 e a 16 bit a svantaggio delle prestazioni.

In fase di installazione è importante conoscere alcune informazioni sulle impostazioni della scheda di rete. Per le schede PCI è necessario specificare il numero SLOT mentre per quelli ISA è indispensabile inserire i numeri IRQ (interrupt) e PORT. In genere queste informazioni sono incluse nel programma di configurazione della scheda, ad esempio in 3c5x9cfg.exe per le schede 3Com EtherLink III oppure nel software PCIScan.exe per i dispositivi PCI.

Il programma di configurazione per le schede 3Com 3C509 EtherLink III, 3Com Fast EtherLink 10/100 e Intel EtherExpress Pro/100 è incluso in EnterNet FireWall. Consultare il paragrafo 6.4.4, Configurazione dell'interfaccia_{Configurazione} dell'interfaccia.



Alcuni programmi di installazione consentono di regolare le prestazioni delle schede di rete. I modelli 3c90x di 3Com, ad esempio, includono un'opzione denominata "Maximize Network Throughput". La possibilità di modificare questo tipo di impostazioni è molto importante per ottenere prestazioni elevate. Tuttavia, queste vengono generalmente ignorate quando EnterNet FireWall viene eseguito a una velocità di 10 Mbps o inferiore.

4.3.6 Configurazione del BIOS

Probabilmente sarà necessario modificare tutte o parte delle seguenti impostazioni del BIOS.

- Disattivazione di tutte le funzioni relative al risparmio energetico, ad esempio arresto della CPU o della scheda di rete. È comunque possibile che le funzioni di salvaschermo rimangano attive.
- Modifica della sequenza di avvio delle unità in modo che la lettera del supporto di avvio utilizzato (ad esempio A: per il disco floppy) venga utilizzata prima di quella dell'unità a disco rigido, ovvero C:.
- Se si desidera rimuovere successivamente la tastiera, sarà probabilmente necessario selezionare una sequenza di avvio non soggetta a interruzioni in caso di eventuali errori, quali "Halt on: No Errors". Questo è importante perché quasi tutti i BIOS interpretano come un "errore" la mancanza di una tastiera e richiedono pertanto la pressione di un tasto per continuare.

4.3.7 Altri requisiti

Per eseguire EnterNet FireWall è necessario inserire una chiave hardware nella porta parallela.

In questa circostanza è consigliabile utilizzare la porta parallela standard. Infatti, se la chiave hardware viene inserita nelle porte parallele di schede PCI aggiuntive o simili, potrebbero verificarsi problemi.



In assenza della chiave, sarà possibile eseguire EnterNet FireWall in modalità demo solo per due ore, quindi il programma si arresterà e sarà necessario riavviarlo per continuare.

5. Aggiornamento dalla versione 5.x

Leggere questa sezione se si sta effettuando un aggiornamento da una versione precedente di EnterNet FireWall. <0> {0}>It will help explain how the upgrade procedure is carried out.<.<0}>Di seguito verrà descritto come eseguire la procedura di aggiornamento.<0}

Se invece è la prima volta che si installa EnterNet FireWall, passare al capitolo 6, Operazioni preliminari Operazioni preliminari.

EnterNet FireWall 6.0 utilizza un nuovo protocollo di gestione remota, più sicuro rispetto a quelli inclusi nelle precedenti versioni del firewall. Purtroppo la nuova versione di FireWall Manager non è in grado di controllare in remoto le versioni precedenti.

Viceversa, le versione precedente di FireWall Manager riesce a controllare la nuova versione 6.0 solo se il vecchio protocollo di gestione non è disabilitato nel software. Poiché, per motivi di sicurezza, non è consigliabile lasciare attivo tale protocollo,

diventa necessario seguire una procedura specifica per aggiornare il nuovo software del firewall senza però perdere il controllo del firewall stesso.

Esistono due procedure per eseguire l'aggiornamento.

5.1 Procedura di aggiornamento 1: accesso fisico

Utilizzare questa procedura se si ha accesso locale all'hardware del firewall per estrarre il floppy. Questo metodo consente di risolvere eventuali errori di aggiornamento con estrema facilità.

1. Installare la nuova versione di FireWall Manager. La procedura viene descritta nel capitolo 7.1, Installazione di FireWall Manager. La nuova versione del programma di gestione utilizza un formato di file differente rispetto alla precedente. È possibile eseguire l'installazione nella stessa directory senza sovrascrivere la versione 5.x.

2. Avviare la nuova versione di FireWall Manager. Il programma richiederà se si desidera collegare il vecchio database di amministrazione "FWList". Rispondere **No**, a meno che non si preferisca continuare a utilizzare l'origine dati ODBC.
3. Ripetere i passi 4 a 11 per ogni firewall che si desidera aggiornare.
4. Estrarre il floppy dal firewall.
5. Nella versione 6 del programma di gestione creare un nuovo firewall con le stesse proprietà del firewall che si sta aggiornando e lasciare vuota la configurazione.
6. Se, dopo l'aggiornamento, si desidera controllare il firewall da FireWall Manager 5.x (non consigliato), selezionare l'opzione **Load Key from Boot Media** dal menu **FireWall, Advanced**.
7. Aprire la configurazione, quindi selezionare **Open from Boot Media** dal menu **File** per visualizzare le impostazioni correnti nel disco floppy.
8. Verificare che la regola del firewall consenta di stabilire una connessione con la porta TCP 999 corrispondente dalla workstation di amministrazione. Se la workstation di amministrazione si trova nella rete interna, la connessione viene autorizzata, per impostazione predefinita, dalla regola FwdFast che permette al traffico di ritornare sull'interfaccia interna del firewall.
9. Se si desidera conservare il vecchio floppy di avvio del firewall (consigliato), inserire un nuovo disco floppy vuoto. In alternativa, è possibile utilizzare lo stesso floppy per la nuova versione.
10. Selezionare **Create Boot Media** dal menu **Firewall, Advanced**.
11. Inserire il floppy nel firewall e riavviare il sistema.

5.2 Procedura di aggiornamento 2: accesso remoto

Utilizzare la seguente procedura se non è possibile gestire il floppy di avvio tramite il firewall.

Rispetto alle versioni precedenti, EnterNet FireWall 6.0 è più restrittiva per quanto riguarda l'analisi della configurazione. Quindi, se la vecchia configurazione presenta errori, il software del firewall non funzionerà perché non riuscirà a leggere i relativi file di configurazione. In particolare, i nuovi software non consentono conflitti di nomi tra host, reti, interfacce e le connessioni VPN.

1. Installare la nuova versione di FireWall Manager. Questa procedura viene descritta nel capitolo 7.1, Installazione di FireWall Manager. La nuova versione del programma di gestione utilizza un formato di file differente rispetto alla precedente. È possibile eseguire l'installazione nella stessa directory senza sovrascrivere la versione 5.x.
2. Avviare la versione 5.x di FireWall Manager.
3. Verificare che le regole di aggiornamento di tutti i firewall consentano di stabilire una connessione con la porta TCP 999 corrispondente alla workstation di gestione. Se la workstation di amministrazione si trova nella rete interna, la connessione viene autorizzata, per impostazione predefinita, dalla regola FwdFast che permette al traffico di ritornare sull'interfaccia interna del firewall. Qualora fosse necessario apportare modifiche, caricare la configurazione nel firewall.
4. Selezionare **Upload New Core** dal menu **Firewall, Advanced**. Selezionare la versione 6.0 del firewall nella finestra di dialogo. Il file viene denominato FWC_600.exe. Al termine dell'operazione, riavviare il firewall o i firewall.
5. Chiudere FireWall Manager.
6. Avviare l'utilità **DBConvert** installata dal CD di EnterNet FireWall 6.0.

7. Tale utilità si collegherà al database di amministrazione "FWList" e visualizzerà un elenco di tutti i firewall con versione 5.x disponibili. Selezionare i firewall che si desidera aggiornare, fare clic su **Add** e quindi su **Convert**.
8. Avviare la nuova versione di FireWall Manager. Il programma richiederà se si desidera collegare il database di amministrazione "FWList". Selezionare **Yes**.
9. Per aumentare la sicurezza durante l'amministrazione remota, selezionare l'opzione **Change Firewall Keys** dal menu **FireWall, Advanced** affinché i firewall accettino solo il nuovo protocollo di gestione. La vecchia implementazione del protocollo di gestione non può utilizzare i nuovi file chiave e pertanto verrà disabilitata.

6. Operazioni preliminari

6.1 Avvio rapido

Questo capitolo contiene una breve descrizione delle modalità di installazione ed esecuzione del software EnterNet FireWall. Nei capitoli che seguono verranno illustrate nel dettaglio le varie funzioni, tecniche e procedure.

Le fasi del processo di installazione di EnterNet FireWall sono le seguenti:

- preparazione delle componenti hardware per EnterNet FireWall;
- installazione di EnterNet FireWall Manager nella workstation che verrà utilizzata per amministrare il firewall;
- preparazione della configurazione in FireWall Manager;
- creazione di un supporto di avvio per il firewall;
- avvio del firewall.

6.2 Preparativi iniziali

Prima di iniziare il processo di installazione effettivo è necessario seguire due fasi preliminari che riguardano la preparazione dei componenti hardware del firewall e l'installazione del software EnterNet FireWall Manager.

1. Preparazione dei componenti hardware del firewall

Preparare i dispositivi hardware che consentono di eseguire EnterNet FireWall Core. Per maggiori informazioni sulla scelta e sulla configurazione dell'hardware, consultare la sezione 4.3, Scelta dei componenti hardware.

2. Installazione di EnterNet FireWall Manager

È necessario installare EnterNet FireWall Manager nella workstation che verrà utilizzata per amministrare il firewall; la procedura viene descritta nel capitolo 7.1, Installazione di FireWall Manager.

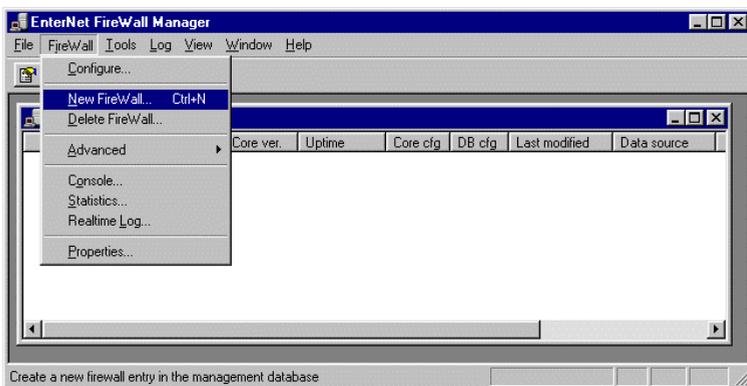
Dopo aver eseguito queste due operazioni, è possibile continuare il processo di installazione seguendo le istruzioni descritte nelle sezioni più avanti.

6.3 Creazione di un firewall in FireWall Manager

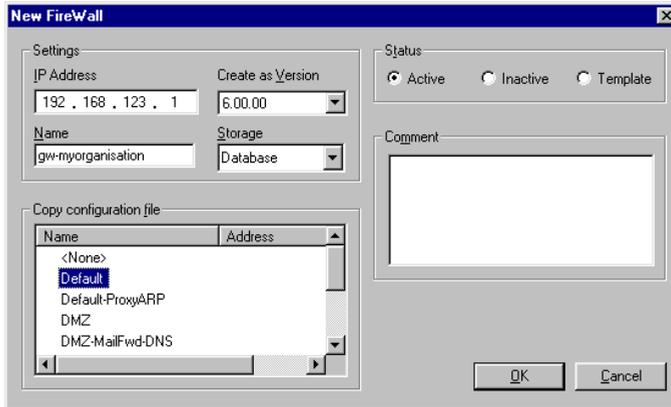
Avviare EnterNet FireWall Manager.

Verrà visualizzata la finestra FireWall List, ovvero la finestra principale di FireWall Manager. Questo argomento verrà trattato più approfonditamente nella sezione 7.2. Finestra principale: FireWall List.

Per creare un nuovo firewall, selezionare **FireWall** dalla barra dei menu e quindi scegliere **New FireWall**.



Verrà visualizzata una finestra di dialogo che richiede di immettere alcune impostazioni di base relative al firewall che si desidera creare.



Immettere l'indirizzo IP dell'interfaccia firewall più vicina. Questo corrisponderà quasi sicuramente al *gateway predefinito* che verrà utilizzato dalla rete protetta dopo l'installazione del firewall. FireWall Manager comunicherà con il firewall tramite l'indirizzo IP appena specificato per le operazioni di controllo in remoto. Tuttavia, questa impostazione *non* influenzerà le modalità di configurazione del firewall.

Assegnare un nome al firewall. Si tratta di una procedura puramente simbolica che non ha alcun effetto diretto sul firewall.

Infine, selezionare un modello di configurazione da copiare. Se uno dei modelli di configurazioni disponibili soddisfa le proprie esigenze, scegliendolo sarà possibile semplificare e velocizzare le prime fasi del processo. Per ulteriori informazioni su ciascun modello di configurazione, consultare la sezione 8.5, Esempi di configurazione.

Scegliere **OK** per continuare.

Verrà aggiunto così un nuovo firewall al database di amministrazione. Copiare il modello di configurazione selezionato e creare una nuova chiave di crittografia che verrà utilizzata da FireWall Manager per la gestione remota del firewall.

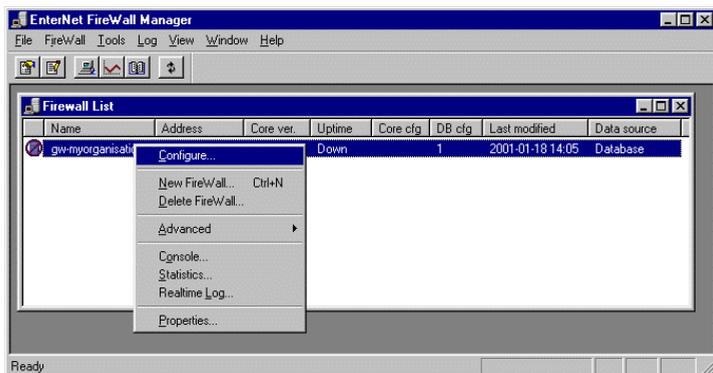
A questo punto la finestra di dialogo si chiude e compare di nuovo la finestra principale che contiene il nuovo firewall preceduto da un'icona con un punto interrogativo. Questo verrà presto sostituito da un altro simbolo il quale indica che non è possibile contattare il firewall appena aggiunto. Si tratta di una procedura normale che si verifica sempre prima di configurare, installare ed eseguire il firewall.

6.4 Modifica delle impostazioni predefinite

Questa sezione è basata sul modello di configurazione **Default**. Qualora fosse necessario apportare alcune variazioni alle modifiche descritte in questa sezione per adattarle ad un altro modello di configurazione, è possibile utilizzare i commenti inclusi in ogni modello appositamente progettati per semplificare le procedure.

Se il firewall appena creato si basa sul modello **Default**, saranno disponibili due interfacce. Verrà eseguita la traduzione dinamica dell'indirizzo sulle connessioni originate internamente e non saranno autorizzate le connessioni originate esternamente. Inoltre, le regole consentono di effettuare connessioni a un server Web o a un server di posta di una rete interna utilizzando la traduzione di indirizzi statici tramite l'indirizzo IP esterno del firewall, ovvero l'unico a essere visibile dall'esterno.

A questo punto, è possibile inserire le informazioni specifiche per il proprio tipo di installazione, tra cui le impostazioni della scheda di rete e gli indirizzi IP.

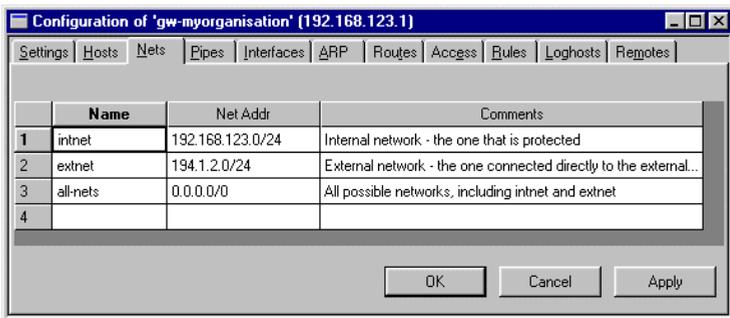


Fare clic con il pulsante destro del mouse sul nuovo firewall e quindi selezionare **Configurare** dal menu a discesa. Verrà visualizzata la finestra di configurazione del firewall.

Per ulteriori informazioni sulla visualizzazione della configurazione, consultare il capitolo 7, EnterNet FireWall Manager_{EnterNet} FireWall Manager, più avanti.

Verrà visualizzata la regola per il firewall. Se le funzioni di base descritte qui di seguito soddisfano le proprie esigenze non sarà necessario apportare modifiche.

6.4.1 Indirizzi di rete locale **Selezionare la scheda Nets per modificare le impostazioni degli indirizzi di rete.**



A questo punto, è necessario modificare gli indirizzi per le reti **intnet** e **extnet**. EnterNet FireWall consente di definire gli indirizzi di rete in modo diverso.

Intervalli di indirizzi IP

EnterNet FireWall utilizza *intervalli di indirizzi* come definizione di rete predefinita. Tali intervalli vengono scritti nella forma a.b.c.d-e.f.g.h.

Gli intervalli degli indirizzi non sono limitati dalla netmask ma possono anche includere qualsiasi estensione di indirizzi IP.

Ad esempio, una rete di *server Web*, costituito da quattro server Web, può essere definito come l'intervallo di indirizzo 192.168.124.45 - 192.168.124.48.

CIDR, Classless Inter Domain Routing

La funzione CIDR utilizza una barra e un numero (compreso tra 0 e 32) per indicare la dimensione della rete (maschera). /24 corrisponde a una rete di classe C con 256 indirizzi (maschera 255.255.255.0), /27 corrisponde a una rete a 32 indirizzi (maschera 255.255.255.224).

I numeri tra 0 e 32 corrispondono al numero di cifre binarie nella maschera.

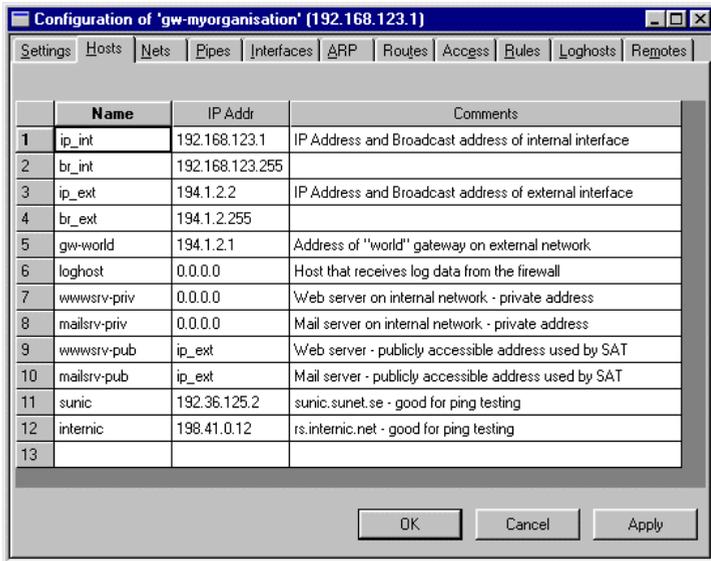
Numero di rete e netmask

Naturalmente, è possibile definire le reti IP utilizzando un numero di rete e una maschera.

192.168.123.0 / 255.255.255.0

6.4.2 Indirizzi IP locali

La sezione **Hosts** contiene nomi simbolici per gli indirizzi IP. In questo modo, è possibile utilizzare i nomi degli indirizzi IP al posto dei numeri nelle sezioni successive. Quindi, se si desidera modificare un indirizzo, sarà necessario eseguire tale operazione solo in questa sezione. Questa procedura migliora la leggibilità della configurazione e semplifica la comprensione del resto della configurazione. È comunque possibile utilizzare solo indirizzi IP numerici in tutto il file di configurazione.



In questa sezione sarà necessario cambiare **ip_int** nell'indirizzo interno desiderato del firewall e **br_int** nell'indirizzo broadcast della rete interna. L'indirizzo broadcast è il più alto della rete. Nel caso di una rete di classe C (maschera 255.255.255.0), tale indirizzo corrisponde a 255. Nel caso di una rete a 32 indirizzi, esso equivale all'indirizzo di rete +31. Ad esempio, l'indirizzo di rete 192.168.123.64 produce un indirizzo broadcast 192.168.123.95.

Modificare **ip_ext** e **br_ext** nello stesso modo.

Cambiare **gw-world** nell'indirizzo IP del *gateway predefinito* posizionato all'esterno del firewall. Generalmente, questo indirizzo viene fornito dal provider di servizi Internet (ISP).

La voce **loghost** viene utilizzata in questo modello per definire l'indirizzo IP al quale inviare i dati di log. La sezione, 9, Auditing da EnterNet Firewall, descrive le funzioni di registrazione, ma se si è scelto di non installare alcun sistema di ricevimento di log, le impostazioni **loghost** possono essere lasciate invariate.

Per fare in modo che il server Web o di posta sia accessibile tramite l'indirizzo IP del firewall, sarà necessario cambiare le voci **wwwsrv-priv** e **mailsrv-priv** negli indirizzi del server Web e del server di posta della rete protetta.

Con questa configurazione sarà possibile accedere ai server pubblici tramite l'indirizzo IP esterno del firewall. Per consentire l'accesso ai server pubblici tramite indirizzi diversi, cambiare **wwwsrv-pub** e **mailsrv-pub** negli indirizzi desiderati. Questi due indirizzi vengono pubblicati automaticamente nella sezione ARP dalla configurazione in oggetto.

6.4.3 Definizione delle impostazioni della scheda di rete

Se si conoscono già le impostazioni hardware della schede di rete, è possibile saltare questa sezione.

Generalmente, le impostazioni relative alla scheda di rete sono incluse nel programma di configurazione fornito in dotazione con la scheda stessa, ad esempio 3c5x9cfg.exe per le schede 3om 3C509 EtherLink III.

EnterNet FireWall 6.0 contiene il software di configurazione per le schede 3Com Fast EtherLink XL 10/100, 3Com EtherLink III e Intel EtherExpress Pro/100. Include inoltre un'ulteriore utilità di analisi PCI che consente di consultare con rapidità i parametri di bus e slot relativi a qualsiasi tipo di scheda di rete PCI.

Per creare un disco di avvio che includa i programmi di configurazione relativi alle schede di rete sopra citate, selezionare **Create NIC Setup Disk** dal menu **Tools**.

Dopo aver creato il disco di avvio, inserirlo nel computer firewall e avviare la macchina. A questo punto è possibile aprire il programma di configurazione della scheda.

Se si utilizzano schede ISA, è necessario inserire i seguenti valori:

- il numero di interrupt (IRQ), un valore compreso tra 1 e 15;
- il numero di porta, un valore esadecimale a tre cifre.

Se si utilizzano schede PCI, è necessario inserire i seguenti valori:

- il numero di slot, generalmente un valore compreso tra 1 e 30;

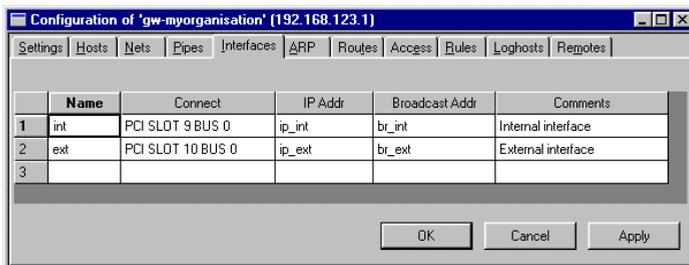
- il numero di bus, generalmente compreso tra 0 e 1. Qualora il numero di bus non fosse disponibile, è possibile adottare il numero 0.

È necessario impostare alcuni valori all'interno del software di configurazione della scheda di rete.

- Se le schede di rete supportano numerosi tipi di supporti, ad esempio TP BNC, AUI, è necessario configurarle solo per i tipi di supporti che verranno utilizzati. Quando la scheda di rete non è collegata alla rete in fase di avvio, nella maggior parte dei casi non sarà in grado di rilevare automaticamente il tipo di supporto adeguato.
- Se le schede di rete supportano diverse velocità, ad esempio 10 e 100 Mbps, è necessario configurarle solo per la velocità che verrà utilizzata. Quando la scheda di rete non è collegata alla rete in fase di avvio, nella maggior parte dei casi non sarà in grado di rilevare automaticamente la velocità corretta, di conseguenza il processo di avvio non verrà eseguito correttamente. Inoltre, se le schede di rete sono collegate a hub o dispositivi che supportano le velocità 10 e 100 Mbps, potrebbero verificarsi problemi durante il rilevamento della velocità appropriata.
- Se i driver supportano diversi livelli di prestazioni e di utilizzo della CPU, è possibile selezionare l'opzione "Maximize Network Throughput" o un valore equivalente.

6.4.4 Configurazione dell'interfaccia

La scheda **Interfaces** include le impostazioni per le schede di rete installate nelle componenti hardware del firewall.



Alcuni indirizzi inseriti nella sezione **Hosts** verranno qui utilizzati per specificare gli indirizzi delle schede di rete corrispondenti.

È necessario modificare le impostazioni della colonna **NIC Driver** per entrambe le interfacce. Selezionare ciascuna cella della colonna per visualizzare la finestra di dialogo relativa alla configurazione di entrambe le schede di rete. L'interfaccia **int** verrà collegata alla rete interna, ovvero quella protetta. L'interfaccia **ext** verrà connessa alla rete esterna, probabilmente al router collegato al provider di servizi Internet (ISP).



NIC è l'acronimo di "Network Interface Card". In alcuni casi le schede di rete vengono denominate MAC "Media Adapter Card".

Selezionare il driver corretto per la scheda di rete, il bus appropriato (PCI, ISA o EISA) e le impostazioni specifiche del bus per la scheda di rete. Tali impostazioni sono state descritte nel paragrafo 6.4.3.

I driver preceduti da un'icona con una scheda di rete sono incorporati, mentre quelli preceduti da icone con una finestra vuota sono di tipo ODI. Generalmente, i driver incorporati sono molto più veloci di quelli ODI, tuttavia al di sotto dei 50 Mbps è molto difficile percepire la differenza di velocità.

Se il driver relativo alla propria scheda di rete non è disponibile nell'elenco, selezionare **Have disk...** per individuare il driver desiderato. Questa versione di EnterNet FireWall utilizza i driver ODI a 16 bit di Novell.

Dopo aver inserito tutte le impostazioni, scegliere **OK** per salvare la configurazione della scheda di rete selezionata. Il testo contenuto nella colonna **NIC Driver** cambierà per riflettere alcune delle impostazioni inserite nella finestra di dialogo. Ripetere questa procedura per tutte le schede di rete.

6.5 Salvataggio della configurazione

A questo punto è possibile utilizzare la configurazione di base. Scegliere **OK** nella finestra di configurazione per salvarla nel database di amministrazione.

Verrà richiesto se si desidera inviare la configurazione al firewall tramite la rete. Rispondere **No** poiché attualmente non è ancora disponibile alcun firewall al quale poter inviare la configurazione.

6.6 Messa in funzione di EnterNet FireWall

6.6.1 Creazione di un supporto di avvio per EnterNet FireWall

Generalmente, EnterNet FireWall Manager viene avviato da un disco floppy. Pertanto, nella sezione seguente verranno descritte le operazioni di avvio tramite questo tipo di supporto. Se si desidera modificare il tipo di supporto di avvio, consultare il paragrafo 7.2.4, Menu Tools: Selezione del supporto di avvio.

Inserire un disco formattato nell'unità A:

Selezionare il firewall per il quale si desidera creare un disco di avvio dall'elenco corrispondente. Ad esempio, è possibile scegliere il firewall creato nel paragrafo 6.3.

Selezionare **Advanced/Create Boot Media** dal menu **Firewall**. Verrà creato un disco di avvio compatibile con DOS che include:

- i file di avvio Caldera DR-DOS;
- il software di EnterNet FireWall;
- i driver di rete selezionati, a meno che non siano già incorporati;
- i file di configurazione per le schede di rete e il firewall;
- le chiavi di crittografia per l'amministrazione remota.

Consultare la sezione 8.3 per ulteriori informazioni sul contenuto del disco di avvio.

6.6.2 Collegamento delle schede di rete del firewall

Collegare le schede di rete del firewall alle rispettive reti. Qualora l'interfaccia esterna dovesse essere direttamente connessa a un router, in contrapposizione ad un hub o uno switch, sarà probabilmente necessario utilizzare un cavo "X-Ethernet", ovvero l'equivalente Ethernet di un "cavo null modem".

6.6.3 Installazione della chiave hardware

Installare la chiave hardware nella porta parallela del firewall. Senza questo dispositivo il software del firewall verrà avviato in modalità demo e cesserà di funzionare dopo due ore di attività. Quindi, sarà necessario riavviarlo.

6.6.4 Avvio di EnterNet FireWall Manager

Inserire il disco di avvio nel computer che ospiterà il firewall e quindi riavviare il sistema. Verificare che i driver della scheda di rete siano stati installati e che sia abilitata la console blu del firewall. Se il firewall è riuscito a leggere la configurazione e a utilizzare le schede di rete corrispondenti, verrà visualizzato il messaggio "System Running...".

Assicurarsi di poter accedere al firewall tramite FireWall Manager premendo F5 o selezionando **Refresh** dal menu **View**. Se tutto funziona correttamente, verrà visualizzata l'icona del firewall senza punto interrogativo o segnale di stop, e la colonna **Uptime** cambierà per visualizzare i giorni, le ore, i minuti e i secondi.

Se il firewall viene visualizzato nell'elenco come funzionante, è molto probabile che anche la nuova e sicura connessione sia già in funzione.

6.7 Se il firewall non funziona

Se il firewall *non* viene visualizzato nell'elenco come funzionante, nonostante siano state apportate solamente le modifiche sopra descritte, è possibile che si sia verificato uno dei seguenti errori.

Errori di connessione alle interfacce

È possibile risolvere questo problema tramite il comando **arpsnoop** nella console del firewall. Digitare `arpsnoop all` e premere Invio. Verranno visualizzate tutte le query ARP presenti nelle interfacce. Se dopo un certo lasso di tempo non compare nulla, provare a inviare messaggi eseguendo il ping di diversi indirizzi dagli host connessi alle rispettive reti.

Nell'output del comando `arpsnoop`, il nome dell'interfaccia in ogni riga dovrebbe corrispondere agli indirizzi IP visualizzati da tutte le interfacce. In caso contrario, è possibile che i cavi di rete siano stati collegati alla scheda di rete errata. Provare a spostare i cavi di rete. Per ulteriori informazioni sulla console del firewall console e sul comando `arpsnoop`, consultare la sezione 8.2, Console del firewall_{console} del firewall.

Utilizzo di una scheda NIC 3c905 (non 905B o 905C)

Il modello originale "3c905" presenta numerosi problemi. Innanzitutto, sono stati rilevati errori durante la negoziazione di una corretta velocità di collegamento. Inoltre, i driver integrati in EnterNet FireWall non supportano questo tipo di schede in quanto molto diverse dai modelli B e C. Se non è possibile sostituire la scheda NIC con i modelli 905B o 905C, è consigliabile utilizzare il driver `ODI 3c90x.com`.

Schede di rete non collegate correttamente

Verificare gli indicatori di collegamenti di tutte le schede di rete. Se non viene visualizzata alcuna indicazione di collegamento, è possibile che si sia verificato un problema con cavi o che le impostazioni della scheda di rete non siano corrette. Vedere di seguito.

Impostazioni hardware delle schede di rete non corrette

È possibile che le impostazioni hardware delle schede di rete siano errate. Verificare che le impostazioni del tipo di bus utilizzato corrispondano a quelle riportate dal software di configurazione della scheda di rete. *Non* utilizzare le informazioni sullo slot PCI visualizzate nella schermata di avvio del computer o i numeri della scheda madre.

Tipo di supporto o velocità non corretti

È possibile che le schede di rete siano impostate per un tipo di supporto o per una velocità non corretta, oppure che le schede abbiano rilevato automaticamente tali impostazioni in modo errato. Controllare quindi le impostazioni in oggetto nel software di configurazione della scheda di rete.

Tipo di cavo non corretto

Se il firewall è direttamente collegato ad un router o ad un host, il cavo utilizzato per la connessione deve essere di tipo "X-ethernet". Se si utilizza un altro cavo, è molto probabile che i led presenti sugli adattatori indichino l'errore.

In alternativa, è possibile connettere il firewall e l'altra unità a un hub separato.

Alcuni host non riescono a comunicare attraverso il firewall

Quasi tutti i problemi "misteriosi" riscontrati nei supporti sono correlati all'instradamento IP. Se è possibile eseguire il ping di un host dal firewall e viceversa, è *probabile* che l'errore sia da attribuire alle regole. Generalmente si tratta di un problema di instradamento piuttosto che di un'errata configurazione del firewall. Spesso, però, il problema è causato anche da altri fattori.

- Se il computer host non utilizza la regola NAT, il router all'esterno del firewall è in grado di restituire i messaggi attraverso il firewall? Se la risposta è no, cambiare le tabelle di instradamento nel router esterno, oppure pubblicare l'indirizzo IP sull'interfaccia esterna del firewall tramite Proxy ARP nella scheda dei percorsi, oppure utilizzando direttamente le informazioni ARP contenute nella scheda ARP.

- Il gateway predefinito è impostato correttamente nell'host che presenta il problema?
- L'host in questione comprende più di un NIC? L'altro NIC contiene un gateway predefinito che fa riferimento ad altri indirizzi? In genere, è *controproducente* utilizzare più gateway predefiniti. Quindi, si consiglia di rimuovere il secondo gateway predefinito a meno che non ci sia una buona ragione per mantenerlo.
- Ricontrollare, nel firewall e negli host che presentano problemi, tutte le definizioni e le netmask.

Il firewall continua a non funzionare.

Se nessuna delle istruzioni precedenti dovesse avere effetto, controllare le statistiche di tutte le interfacce tramite la funzione **ifstat**. Digitare i seguenti comandi nella console del firewall:

```
ifstat int  
ifstat ext
```

Verrà visualizzato un numero di contatori per ogni interfaccia di rete.

Se i contatori "Input" della sezione Hardware non sono in aumento, è molto probabile che l'errore sia da attribuire ai cavi o alle impostazioni della scheda. La scheda potrebbe essere avere un guasto. Oppure, è probabile che i pacchetti non vengano inviati al firewall. È opportuno verificare quest'ultima eventualità collegando uno sniffer di pacchetti alla rete in questione.

Se i contatori "Input" della sezione Hardware sono in aumento, mentre i corrispondenti contatori nella sezione Software diminuiscono, è molto probabile che l'errore sia da attribuire alle impostazioni del driver. I numeri del bus, dello slot, della porta o IRQ potrebbero non essere corretti, oppure è possibile che la scheda non sia compatibile con il driver utilizzato. Accertarsi di utilizzare i driver ODI più recenti.

Se i contatori "Input" di entrambe le sezioni sono in aumento, è probabile che le interfacce siano collegate alle reti fisiche non appropriate. Oppure, potrebbe trattarsi di un problema nella sezione Nets della configurazione. Infine, le informazioni di instradamento incluse negli host o nei router connessi potrebbero essere errate.

Se le suddette istruzioni non dovessero comunque risolvere il problema, contattare il proprio fornitore oppure il servizio assistenza di EnterNet.

7. EnterNet FireWall Manager

EnterNet FireWall Manager è stato progettato per semplificare la gestione di EnterNet FireWall, sia in remoto che durante l'installazione.

All'interno di FireWall Manager, infatti, è possibile archiviare informazioni sulle impostazioni delle schede di rete, sulla configurazione e sulla chiave di crittografia di ogni firewall. In questo modo, se un firewall dovesse danneggiarsi oppure dovesse scomparire dalla configurazione, sarà possibile ricreare rapidamente i dischi di avvio corrispondenti. È comunque possibile utilizzare il firewall senza FireWall Manager.

Infatti, viene eseguito il backup di tutti i dati sia all'interno del database di amministrazione di FireWall Manager che in ogni singolo firewall.

Quindi, eventuali modifiche alla configurazione tramite FireWall Manager non influenzeranno direttamente il firewall anzi, sarà necessario inviare ad esso la nuova configurazione. È possibile eseguire questa operazione in due modi diversi:

- inviando la configurazione tramite la rete da una workstation autorizzata ad amministrare il firewall in remoto; oppure
- estraendo il supporto di avvio dal firewall per inserirlo nella workstation, quindi salvando la nuova configurazione su tale supporto e infine reintrodurlo nel firewall. Per attivare la nuova configurazione, è necessario digitare il comando `reconfigure` nella console del firewall. Consultare la sezione 8.2, Console del firewall_{Console} del firewall.

7.1 Installazione di FireWall Manager

EnterNet FireWall Manager può essere installato in una o più workstation ed essere eseguito in Windows 95, 98, NT 4.0, Windows 2000 e Windows Me.



Se si desidera utilizzare FireWall Manager in più workstation, è consigliabile installare il programma su una rete condivisa. In questo modo, è possibile salvare i driver e il software del firewall aggiornato nella stessa directory nella quale è stato installato FireWall Manager per consentire agli utenti di accedervi facilmente.

Per utilizzare le applicazioni da varie workstation, è necessario memorizzare il database in una posizione facilmente accessibile da parte di tutti gli utenti autorizzati.

Per ulteriori informazioni sull'impostazione di più FireWall Manager per amministrare un singolo firewall, consultare il paragrafo 7.1.3, *Database* di amministrazione, più avanti.

7.1.1 Procedura di installazione

Inserire il CD di EnterNet FireWall nel computer che verrà utilizzato per amministrare il firewall. Verrà avviato automaticamente il sistema di menu "EnterNet FireWall".

In caso contrario, selezionare **Run** dal menu Start di Windows, quindi digitare `D:\setup.exe` (D: rappresenta la lettera dell'unità CD-ROM).

Selezionare "Install EnterNet FireWall 6.0" nel menu. Verrà avviato il programma di installazione. Selezionare FireWall Manager e seguire le istruzioni sullo schermo.

7.1.2 Maggiore sicurezza a livello locale per FireWall Manager

Per evitare che il firewall venga controllato in modalità remota da utenti non autorizzati oppure da programmi che potrebbero violare la sicurezza dei computer locali, è consigliabile proteggere il database di amministrazione di EnterNet FireWall Manager.

È necessario almeno cambiare i diritti di accesso ai file del database (FWList.mdb) oppure se si utilizza il database predefinito includere solamente gli utenti autorizzati ad amministrare il firewall in modalità remota.

Sarebbe comunque molto più sicuro spostare il file in un server di file e assegnare i relativi diritti di accesso. È inoltre possibile spostare l'intero database su un altro tipo di server dotato di un proprio sistema di autenticazione, ad esempio un server SQL.

Per ulteriori informazioni sullo spostamento di un database, consultare il paragrafo 7.1.3, *Database* di amministrazione, più avanti.

7.1.3 Database di amministrazione

Tutte le informazioni relative alla configurazione vengono archiviate come un insieme di file di dati e/o all'interno di uno o più database compatibili con ODBC. Il termine *origine dati* viene utilizzato in FireWall Manager per indicare i database ODBC e quelli basati su file.

Dopo aver installato EnterNet FireWall Manager, verranno installati e configurati due origini dati basate su file:

- “Default”, utilizzata per memorizzare i dati di configurazione relativi alle nuove impostazioni del firewall.
- “Template”, utilizzata dai modelli di configurazione distribuiti con l'installazione.

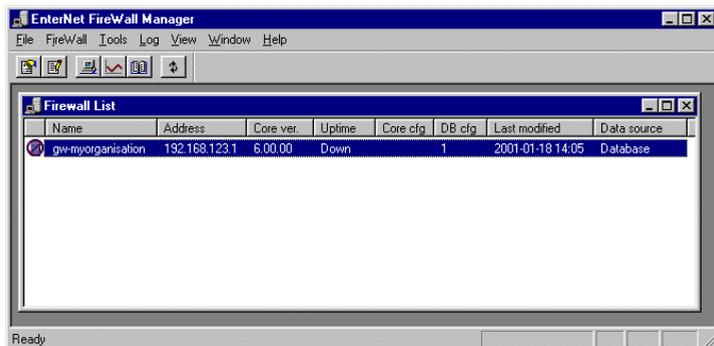
Se si esegue l'aggiornamento di una vecchia versione di EnterNet FireWall Manager, oltre alle origini dati sopra citate verrà configurato automaticamente anche il file “FWList” basato su ODBC.

Per gestire il firewall da più workstation, è necessario spostare il database in un server di file per consentire l'accesso. In alternativa, è possibile esportare il database in un server SQL.

Per ulteriori informazioni su come impostare e gestire i database di amministrazione, consultare il paragrafo 7.2.4, *Menu Tools*: Definizione dell'origine dati di amministrazione.

7.2 Finestra principale: FireWall List

La prima finestra che viene visualizzata all'avvio dell'applicazione corrisponde a un elenco dei firewall presenti nel database di amministrazione. Da questo elenco centralizzato è possibile gestire tutte le applicazioni EnterNet FireWall installati nell'azienda. Per ogni firewall verranno visualizzate le seguenti informazioni:



- Icon  indica che il firewall sta rispondendo alle query sullo stato effettuate da FireWall Manager. Tuttavia questo *non* significa necessariamente che la workstation su cui viene eseguito FireWall Manager sia autorizzata ad amministrare tale applicazione in remoto.
-  indica che il firewall non ha risposto recentemente alle query sullo stato.
-  indica che non è stato possibile accedere al firewall per un periodo di tempo molto lungo oppure che il firewall non ha risposto alle query dall'avvio di FireWall Manager.
-  indica che il firewall è stato definito come inattivo, pertanto FireWall Manager non tenterà di contattarlo, oppure comunicherà che non è possibile accedere al firewall.

- **Nome** Questo nome viene utilizzato solo all'interno di FireWall Manager per semplificare la leggibilità dell'elenco. Quindi, non è in correlazione con i nomi DNS, le risorse di dominio o le informazioni NDS.
- **Address** Indirizzo IP utilizzato da FireWall Manager per contattare il firewall.
- **Core ver.** Versione del software di EnterNet FireWall, ovvero il programma eseguito nel computer firewall sul quale è installato il software di firewall corrente.
- **Uptime** Periodo di funzionamento del software del firewall, visualizzato in giorni ore, minuti e secondi. Per azzerare questo orologio, digitare il comando `shut down` nella console del firewall. Consultare la sezione 8.2, Console del firewall_{console} del firewall.
- **Core cfg** Numero di versione della configurazione correntemente utilizzata nel firewall. Tale numero aumenta ogni volta che la configurazione viene modificata e attivata.
- **DB cfg** Numero di versione della configurazione archiviata nel database di amministrazione.
- **Last mod.** Data più recente nella quale la configurazione archiviata nel database di amministrazione è stata modificata e salvata.
- **Datasource** Nome dell'origine dati che contiene la voce del firewall in oggetto. Non corrisponde necessariamente ai nomi dell'origine dati ODBC, ma piuttosto al nome immesso tramite l'opzione **Specify Management Datasources** del menu **Tools**.



Se il valore **DB cfg** è maggiore di quello **Core cfg**, le modifiche apportate alla configurazione contenuta nel database di amministrazione non sono ancora state trasmesse al firewall.

Se il valore **Core cfg** è maggiore di quello **DB cfg**, le modifiche apportate al firewall non state notificate all'applicazione FireWall Manager in uso. È possibile effettuare tali modifiche tramite l'applicazione FireWall Manager collegata a un altro database di amministrazione, oppure direttamente dal disco di avvio. Non è consigliabile gestire un singolo firewall da due database separati, a meno che non si sia a conoscenza dei rischi che ne potrebbero derivare.

7.2.1 Barra degli strumenti



Nella barra degli strumenti relativa all'elenco dei firewall sono disponibili collegamenti che semplificano l'accesso alle funzioni seguenti:

- Proprietà del firewall selezionato, consultare la sezione 7.2.3 – proprietà.
- Configurazione del firewall selezionato, consultare la sezione 7.2.3 – Configurazione.
- Connessione alla console del firewall selezionato, consultare la sezione 7.2.3 – Console
- Statistiche per il firewall selezionato, consultare la sezione 7.2.3 – Statistiche
- Visualizzazione in tempo reale dei dati di log relativi al firewall selezionato, consultare la sezione 7.2.3 – Mostra in tempo reale
- Aggiornamento dello stato del firewall e tempo di attività nell'elenco del firewall.

7.2.2 Menu File



Print

Consente di stampare l'elenco dei firewall.

Print Preview

Consente di visualizzare un'anteprima del documento attivo.

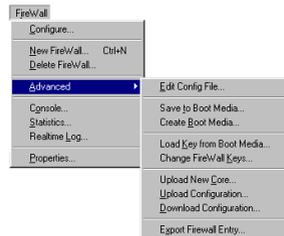
Print Setup

Consente di modificare le impostazioni della stampante per il documento attivo.

Exit

Consente di chiudere EnterNet FireWall Manager. Non è possibile chiudere l'applicazione durante la modifica di una configurazione del firewall.

7.2.3 Menu FireWall



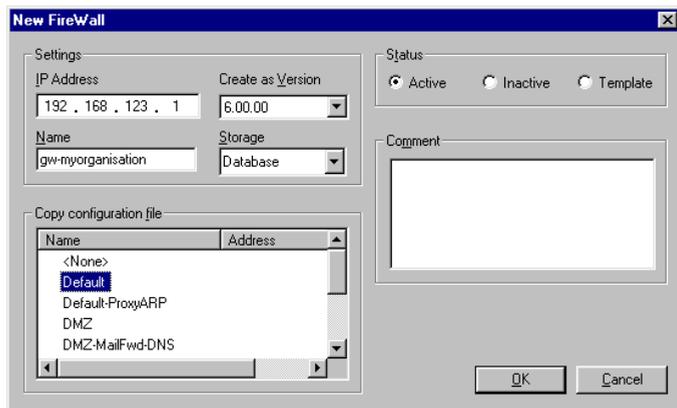
Configure

Consente di aprire la finestra di configurazione relativa al firewall selezionato. Dalla finestra di configurazione è possibile controllare tutti gli aspetti del firewall, dal tipo di scheda di rete agli indirizzi IP dell'interfaccia e alle regole che gestiscono le operazioni di blocco.

Consultare la sezione 7.3, Finestra di configurazione. Dalla finestra di configurazione è possibile controllare tutti gli aspetti del firewall..

New FireWall

Consente di aprire la seguente finestra di dialogo per creare un nuovo firewall nel database di amministrazione.



Creazione di un nuovo firewall nel database di amministrazione.

L'**indirizzo IP** specificato nella finestra di dialogo *non* influenza la configurazione del firewall ma definisce solamente l'indirizzo che FireWall Manager tenterà di utilizzare durante la comunicazione con il firewall.

Il nome specificato nel campo **Name** rappresenta un identificatore univoco per il firewall. Esso ha un valore puramente simbolico e non ha alcun effetto sul firewall.

Dal menu a discesa **Create as version** è possibile specificare la versione di EnterNet FireWall per la quale è stato progettato il nuovo elemento di configurazione.



È comunque possibile installare nel firewall la versione desiderata, indipendentemente dall'opzione specificata in **Create as version**. Poiché FireWall Manager è in grado di gestire le configurazioni tramite diverse versioni di EnterNet FireWall, è necessario conoscere la versione del firewall che si desidera utilizzare. Infatti, dal numero di versione dipende la modalità di configurazione del nuovo firewall.

L'elenco a discesa **Storage** consente di selezionare l'origine dati nella quale archiviare le informazioni relative al nuovo firewall. La gestione delle voci incluse nell'elenco viene descritta nel paragrafo 7.2.4, Menu Tools: Definizione dell'origine dati di amministrazione.

La casella di riepilogo **Copy configuration file** consente di selezionare un file di configurazione da utilizzare come modello per il nuovo firewall. Tuttavia, anche i firewall precedentemente creati possono essere usati come modelli.

Per specificare lo stato iniziale del nuovo firewall, scegliere il pulsante di opzione **Status** appropriato. Se si seleziona la funzione *Active*, l'applicazione effettuerà periodicamente un'interrogazione ciclica del firewall per rilevare le informazioni sullo stato. Se si seleziona la funzione *Template*, invece, il firewall in oggetto verrà creato solo per essere utilizzato come modello di configurazione.

Nel campo **Comment** è possibile immettere informazioni opzionali sul firewall in oggetto. Tali informazioni non influenzano assolutamente le configurazioni.

Infine, viene creata una chiave di crittografia a 128 bit non visibile da parte degli utenti. Tale chiave verrà utilizzata durante l'amministrazione remota del firewall.

Delete FireWall

Consente di eliminare il firewall selezionato dal database di amministrazione. Anche se questa operazione non ha alcun effetto sul firewall, in caso di cancellazione non intenzionale sarà necessario recuperare manualmente il file di configurazione e la chiave di crittografia dal disco di avvio del firewall. Per ulteriori informazioni, consultare il capitolo 12, Domande frequenti (FAQ).

Advanced

Consente di aprire un sottomenu per le operazioni avanzate o utilizzate meno di frequente.

Consultare il paragrafo 7.2.3.1.

Console

Consente di aprire una connessione ai comandi del firewall selezionato. È possibile utilizzare anche i comandi che sono stati immessi fisicamente nella console. Inoltre, i dati di input visualizzati nella schermata del firewall equivalgono a quelli mostrati in questa finestra. Questo comando corrisponde al doppio clic con il mouse sul firewall nell'elenco del firewall.

Consultare la sezione 8.2, Console del firewall_{console} del firewall.

Statistics

Consente di visualizzare le statistiche in tempo reale del firewall selezionato. Tale finestra contiene diversi aspetti dell'ambiente operativo del firewall sotto forma di diagrammi.

Consultare la sezione 7.4, Visualizzazione delle statistiche.

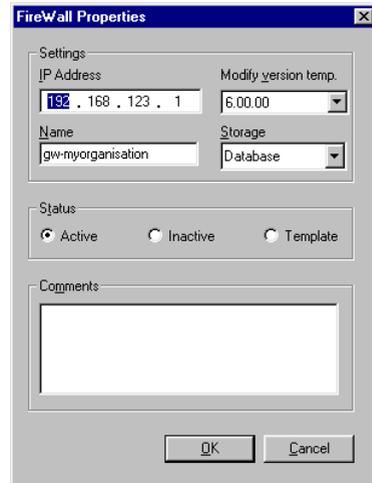
Show Realtime Log

Consente di visualizzare una finestra con i dati di log ricevuti in tempo reale dal firewall selezionato. Tuttavia, verranno visualizzati solo gli eventi *correnti* e non quelli che si sono verificati prima dell'apertura della finestra. Al limite, è possibile tornare indietro di un centinaio di righe.

Consultare il capitolo 9, Auditing da EnterNet Firewall

Properties

La finestra di dialogo delle proprietà consente di modificare alcuni dei parametri precedentemente inseriti tramite l'opzione **New FireWall**.



Tuttavia, *non* consente di apportare modifiche al firewall stesso. Ad esempio, se viene modificato l'indirizzo IP in questa finestra, cambierà solo l'indirizzo IP archiviato nel database di amministrazione e utilizzato per le comunicazioni gestionali con il firewall. È possibile modificare la configurazione IP corrente del firewall tramite l'apposita finestra di configurazione. Vedere la sezione **Configure**.

Questa finestra di dialogo consente di cambiare lo stato del firewall, ad esempio è possibile passare dallo stato attivo a quello inattivo. Per visualizzare o non visualizzare i firewall modello o quelli non attivi nel relativo elenco, selezionare le opzioni **Show Inactive** e **Show Templates** del menu **View**. FireWall Manager non eseguirà le ricerche sullo stato dei firewall contrassegnati come inattivi o modello.

È inoltre possibile cambiare temporaneamente il numero di versione della configurazione del firewall utilizzando l'elenco a discesa **Modify version temporarily**.



Nota: se viene modificato il numero della versione tramite questa finestra, il firewall *non* verrà aggiornato di conseguenza. Poiché FireWall Manager è in grado di gestire le configurazioni tramite diverse versioni di EnterNet FireWall, è necessario conoscere la versione del firewall che si desidera utilizzare. Infatti, dal numero di versione dipende la modalità di gestione della configurazione del firewall esistente nella relativa finestra.

7.2.3.1 Menu FireWall/Advanced

Edit Config File

Consente di aprire la configurazione memorizzata nel database di amministrazione come un file di testo. Pertanto, sarà possibile modificarla senza utilizzare l'ambiente grafico ed inoltre sarà possibile stampare il file su carta per conservarne una copia nei propri archivi oppure per inviarle ad altri utenti.

Quando si utilizza l'editor di configurazione basato su testo, nel menu File è disponibile l'opzione **Open from Boot Media** che consente di sostituire il file di configurazione in uso con quello incluso nel supporto di avvio.

Eventuali modifiche nel file di configurazione generano una ricerca relativa al caricamento automatico della nuova configurazione sul firewall corrente.

Save to Boot Media

Consente di salvare la configurazione e la chiave di crittografia del firewall selezionato in un supporto di avvio di EnterNet FireWall. All'interno di FWCore_O.cfg verrà copiato anche il file FWCore.cfg incluso nella directory Firewall del supporto di avvio. Se il programma stabilisce che il supporto utilizzato non corrisponde a quello di avvio di EnterNet FireWall, verrà richiesto di crearne uno nuovo. L'opzione Create Boot Media descritta più avanti consente di ottenere gli stessi risultati.

Per maggiori informazioni sul contenuto del supporto di avvio, vedere la sezione 8.3, Supporti di avvio di EnterNet FireWall.

Create Boot Media

Consente di creare un supporto di avvio contenente i file di sistema per EnterNet FireWall. Tale supporto verrà utilizzato per archiviare le configurazioni e la chiave di crittografia.

Consultare il paragrafo 6.6.1, Creazione di un supporto di avvio per EnterNet FireWall .

Per maggiori informazioni sul contenuto del supporto, consultare la sezione 8.3, Supporti di avvio di EnterNet FireWall.

Per informazioni sulla modifica del tipo di supporto, consultare il comando **Select Boot Media Device** nel paragrafo 7.2.4, Menu Tools.

Load Key from Boot Media

Consente di copiare la chiave di crittografia da un supporto di avvio di EnterNet FireWall in un determinato firewall del database di amministrazione. Ad esempio, è possibile utilizzare questa funzione per ripristinare manualmente il database di amministrazione nel caso fosse stato inavvertitamente eliminato un firewall dall'elenco. Inoltre, questa opzione consente di trasferire un firewall da un database di amministrazione all'altro. In questo caso, però, si consiglia di creare una nuova chiave di crittografia per ogni nuovo database e di salvarla nel supporto di avvio del firewall per evitare che un singolo firewall venga accidentalmente amministrato due volte.

Change FireWall Keys

EnterNet FireWall Manager utilizza un sistema di comunicazione crittografata per tutte le attività di gestione remota. Di solito, queste chiavi di crittografia vengono generate ogni volta che viene creato un nuovo firewall nel database di amministrazione.

A volte però è necessario modificare manualmente tali chiavi, ad esempio quando si aggiorna una vecchia versione del firewall, oppure quando si trasferisce la gestione di un firewall da un'autorità ad un'altra.

Upload New Core

Consente di inviare una nuova versione di software al firewall specificato. È possibile utilizzare questa funzione quando viene rilasciata una nuova versione di EnterNet FireWall e si desidera aggiornare il software del firewall.

Upload Configuration

Consente di inviare al firewall la configurazione memorizzata nel database di amministrazione tramite la rete. Al termine del trasferimento, il firewall in questione riceve le informazioni necessarie per attivare la nuova configurazione tramite la rilettura del file di configurazione dal supporto di avvio.

Dopo la riconfigurazione, EnterNet FireWall utilizza un processo di verifica bidirezionale per controllare la comunicazione tra FireWall Manager e il firewall. Se per qualsiasi motivo fosse impossibile eseguire la comunicazione, il firewall ritornerà automaticamente alla configurazione precedente.

Questa procedura consente di non perdere quasi mai il controllo di un firewall remoto.

Download Configuration

Consente di recuperare la configurazione in esecuzione dal firewall selezionato e di salvarla direttamente nel database di amministrazione, oppure di visualizzarla nell'editor di configurazione.

Export Firewall Data

Consente di esportare le proprietà e la configurazione del firewall selezionato nella directory desiderata.

I file esportati tramite questa opzione hanno lo stesso formato di quelli archiviati in un database di amministrazione basato su file. Pertanto, se si desidera importare in questo tipo di database i file esportati, basterà semplicemente copiarli nella directory appropriata.

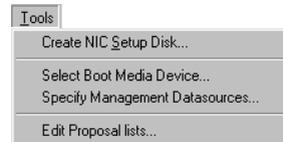
Inoltre, questa opzione consente di inviare la configurazione al provider, se necessario. In tal caso, può essere opportuno inviare solo il file ".efc" che contiene soltanto la configurazione. Il file ".efw" include, tra le altre informazioni, anche le chiavi di crittografia del firewall che normalmente non servono al provider. Qualora fosse necessario inviare questo file, si consiglia di modificare le chiavi del firewall al termine dell'operazione per evitare che finiscano in mani sbagliate.

7.2.4 Menu Tools

Create NIC Setup Disk

Consente di creare un supporto di avvio Caldera DR-DOS con il programma di configurazione per le schede di rete 3Com 3C509 EtherLink III, 3Com 3C90x Fast EtherLink XL 10/100 e Intel EtherExpress PRO/100.

Qualsiasi utente può modificare i dati salvati su questo disco tramite la directory `{INSTALLDIR}\Images\NICCfg`.



Select Boot Media Device

Consente di visualizzare una finestra di dialogo tramite la quale è possibile selezionare il dispositivo da utilizzare per la scrittura dei supporti di avvio. Verranno elencati tutti i dischi fissi o rimovibili disponibili.

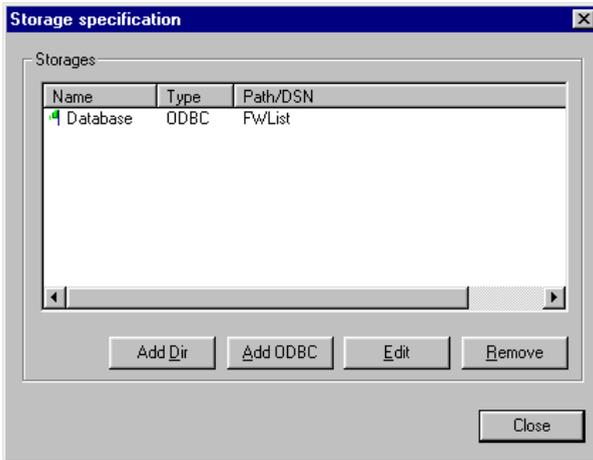
Il dispositivo selezionato verrà inoltre utilizzato durante la creazione di un disco di installazione NIC.

Il sistema Windows 9x supporta solo i floppy come dischi di avvio mentre con i sistemi NT è possibile utilizzare qualsiasi tipo di supporto.

Tuttavia, prima di scrivere i file di avvio sull'apposito supporto, è necessario formattare il dispositivo con un formato del file system FAT 12 o FAT 16.

Specify Management Datasources

EnterNet FireWall Manager consente di utilizzare più database di amministrazione di diversi tipi. Tramite questa opzione è possibile visualizzare una finestra di dialogo che consente di gestire le connessioni all'origine dati come illustrato qui di seguito.



Gestione delle connessioni amministrative all'origine dati.

L'elenco riporta le origini dati configurate correntemente con il relativo *nome*, *tipo* (ODBC o DIR) e specifiche, ovvero il percorso e il DSN.

Se all'inizio della riga viene visualizzata un flag verde, l'origine dati è abilitata. Viceversa, un flag rosso indica che l'origine dati è disattivata.

Selezionando i pulsanti **Add Dir**, **Add ODBC** o **Edit** verrà visualizzata la seguente finestra di dialogo che consente rispettivamente di aggiungere una nuova origine dati basata su file, una nuova origine dati basata su ODBC oppure di modificare un'origine dati esistente.

L'opzione **Name** consente di identificare l'origine dati in tutto il sistema e verrà utilizzato ad esempio nell'elenco a discesa relativo all'archiviazione incluso nella finestra di dialogo "New FireWall".



In base al tipo di origine dati, l'opzione **Path/DSN string** consente di specificare la directory di memorizzazione dei file di dati oppure della stringa ODBC DSN.

L'opzione **Browse** consente di selezionare un percorso dalla finestra di dialogo del file oppure un DSN da un elenco dei nomi origine dati DSN disponibili.

Per attivare o disattivare l'origine dati, selezionare o deselezionare la casella di controllo **Enable**.

Edit Proposal Lists

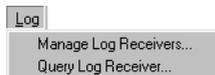
Consente di visualizzare una finestra di dialogo tramite la quale è possibile modificare gli elenchi inclusi nel componente aggiuntivo EnterNet VPN. Per ulteriori informazioni su questa opzione, consultare il manuale *EnterNet VPN Users Guide*.

7.2.5 Menu Log

Manage Log Receivers

Consente di visualizzare una finestra di dialogo tramite la quale è possibile effettuare le connessioni e configurare EnterNet FireWall Logger.

Per ulteriori **informazioni** sulle modalità di configurazione e di utilizzo del sistema di registrazione, consultare il capitolo 9, Auditing da EnterNet Firewall.

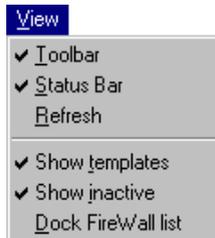


Query Log Receivers

Consente di visualizzare lo strumento per la ricerca dei dati di log. Per ulteriori informazioni su questo strumento, consultare la sezione 9, Auditing da EnterNet Firewall.

7.2.6 Menu View

Le opzioni del menu View consentono di specificare le modalità di visualizzazione delle informazioni da parte di FireWall Manager. Eventuali modifiche a questo menu non influenzeranno i dati salvati o i firewall esistenti.



Toolbar

Consente di visualizzare o nascondere la barra degli strumenti descritta nel paragrafo 7.2.1.

Status Bar

Consente di visualizzare o nascondere la barra di stato nella parte inferiore della finestra principale.

Refresh

Consente di avviare una nuova ricerca sullo stato di tutti i firewall nel database di amministrazione. Se sono presenti più firewall e una query sullo stato è già in esecuzione, è necessario attendere che questa venga completata prima di iniziarne una nuova.

Show templates

Consente di includere nell'elenco dei firewall i modelli di configurazione esistenti. Tali configurazioni vengono visualizzate nell'elenco senza un'icona. Indipendentemente dal fatto che tali modelli vengano visualizzati o meno, sarà sempre possibile copiarli durante la creazione di un nuovo firewall.

Show inactive

Consente di includere i file contrassegnati come inattivi nell'elenco dei firewall. Tali firewall vengono visualizzati nell'elenco con un'icona trasparente. Indipendentemente dal fatto che i firewall visualizzati siano inattivi o meno, sarà sempre possibile copiarli durante la creazione di un nuovo firewall.

Dock FireWall List

Consente di inserire l'elenco dei firewall in uno dei menu ai bordi della finestra principale, come una barra degli strumenti. Quindi, è possibile trascinare l'elenco in un'altra posizione sempre ai lati della schermata.

7.3 Finestra di configurazione

Dalla finestra di configurazione è possibile controllare tutti gli aspetti del firewall.

Tale visualizzazione contiene numerose schede. Qui di seguito viene fornita una breve descrizione delle funzioni di ogni scheda.

Settings

Contiene impostazioni globali relative al firewall, inclusi i limiti delle dimensioni dei pacchetti relativi ai vari protocolli, gli intervalli di attesa delle connessioni, le verifiche dell'integrità strutturale dei pacchetti e così via.

Hosts

La tabella di traduzione tra i nomi simbolici e gli indirizzi IP numerici.

Nets

Tabella di traduzione tra i nomi di rete simbolici e gli indirizzi di rete numerici con le dimensioni di rete (maschere).

Pipes

Tabella che definisce i pipe utilizzati per la modellazione del traffico.

Ifaces

Consente di configurare la scheda di rete con impostazioni quali i nomi, gli indirizzi IP e le impostazioni hardware.

ARP

Acronimo di Address Resolution Protocol. Consente di effettuare associazioni statiche tra gli indirizzi IP e gli indirizzi hardware e di pubblicare gli indirizzi IP sulle interfacce firewall.

Routes

Tabella di instradamento. Comunica al firewall la direzione nella quale inviare i pacchetti destinati ai diversi indirizzi IP. Questa scheda consente di controllare la funzione Proxy ARP.

Access

Offre protezione contro lo spoofing IP. Stabilisce gli indirizzi IP che il firewall deve accettare come mittenti in ogni interfaccia. I pacchetti ai quali è stato negato l'accesso in questa sezione vengono immediatamente eliminati, pertanto *non* potranno passare alla sezione Rules.

Rules

Regole che controllano le attività di EnterNet FireWall; ad esempio, filtrano gli indirizzi del mittente e del destinatario, i protocolli e i numeri di porta e così via. Tali regole gestiscono anche la traduzione degli indirizzi.

Loghosts

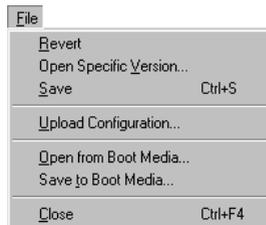
Specifica gli indirizzi IP ai quali EnterNet FireWall deve inviare i dati di log.

Remotes

Specifica gli indirizzi IP autorizzati ad amministrare in remoto EnterNet FireWall nonché gli aspetti del firewall che essi potrebbero controllare.

7.3.1 Menu File

Quando la finestra di configurazione è attiva, il menu File cambia per visualizzare i comandi specifici relativi alla configurazione.



Revert

Consente di sostituire la configurazione corrente con quella salvata più di recente. Tutte le modifiche verranno eliminate.

Open Specific Version

EnterNet FireWall Manager memorizza ogni versione della configurazione, pertanto questa opzione consente di aprire una specifica versione della configurazione.

Save

Consente di salvare la configurazione corrente nel database di amministrazione.

Upload Configuration

Simile al menu **Firewall, Advanced**.

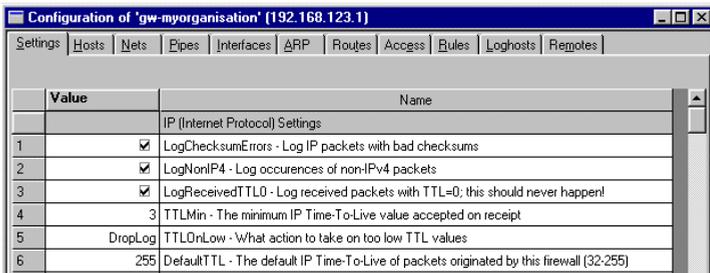
Open from Boot Media

Consente di aprire il file di configurazione memorizzato in un supporto di avvio per eseguire alcune modifiche.

Save to Boot Media

Simile al menu **Firewall, Advanced**.

7.3.2 Scheda Settings



La scheda Settings include diverse impostazioni globali per EnterNet FireWall in termini di limiti delle dimensioni dei pacchetti, timeout della connessione, verifiche dell'integrità strutturale alle quali è soggetto ogni pacchetto e così via. In molti casi, i valori predefiniti di questa scheda sono appropriati per quasi tutte le installazioni.

La parti della scheda Settings utilizzate più di frequente verranno descritte nelle sezioni seguenti:

- **7.3.2.5**, Impostazioni Stateful Inspection
- **7.3.2.6**, Timeout di una connessione
- **7.3.2.7**, Limiti di dimensioni in base al protocollo

Tramite le caselle di riepilogo è possibile specificare alcuni dei valori della sezione Settings. I valori seguenti rappresentano quelli più comunemente utilizzati:

- **ValidateSilent** – Verifica se è stato soddisfatto un determinato requisito. Se il requisito non viene soddisfatto, il pacchetto viene eliminato senza essere registrato.
- **ValidateLogBad** – Verifica se è stato soddisfatto un determinato requisito. Se il requisito non viene soddisfatto, il pacchetto verrà registrato e quindi eliminato.

- **ValidateLog** – Verifica se è stato soddisfatto un determinato requisito. In caso contrario, il pacchetto verrà eliminato. Tuttavia, i pacchetti vengono sempre registrati, indipendentemente dal fatto che il requisito sia soddisfatto o meno. Si tratta di una funzione utile per le opzioni TCP poco utilizzate e così via.
- **StripSilent** – Elimina le informazioni specifiche del pacchetto, se presente, senza effettuare la registrazione. In alcuni casi, viene verificata la correttezza di tali informazioni come in ValidateSilent.
- **StripLogBad** – Verifica la correttezza delle informazioni specifiche. In caso di dati non corretti, i pacchetti vengono eliminati e registrati. Le informazioni vengono sempre cancellate dal pacchetto.
- **StripSilent** – Elimina le informazioni specifiche dal pacchetto, se presenti. Effettua sempre le registrazioni. In alcuni casi, viene verificata la correttezza di tali informazioni come in ValidateLog.
- **Drop** – Elimina sempre il pacchetto. Non effettua la registrazione.
- **DropLog** – Effettua sempre la registrazione ed elimina il pacchetto.
- **Drop** – Elimina sempre il pacchetto. Invia una risposta al mittente per comunicare che il pacchetto non è stato autorizzato all'accesso. Non effettua la registrazione.
- **RejectLog** – Effettua sempre la registrazione ed elimina il pacchetto. Invia una risposta al mittente per comunicare che il pacchetto è stato rifiutato.
- **Ignore** – Ignora la presenza di informazioni specifiche.
- **Log** – Registra esclusivamente le informazioni specifiche.

Tali valori vengono visualizzati in varie caselle di riepilogo, come già descritto in precedenza. Tuttavia, le caselle di riepilogo non contengono *tutti* questi valori contemporaneamente. Inoltre, il loro significato può variare leggermente in base alla singola impostazione. Per ulteriori informazioni su questo argomento, consultare i paragrafi descritti più avanti.

Il paragrafo seguente include una descrizione dettagliata di tutte le impostazioni della sezione Settings.

7.3.2.1 Impostazioni di livello IP

LogChecksumErrors

Consente di registrare le occorrenze dei pacchetti IP che contengono checksum errate. Generalmente, è il risultato del pacchetto che viene danneggiato durante il trasporto in rete. Tutte le unità della rete, ovvero i router e le workstation, restituiscono i pacchetti IP che contengono checksum errati. Sono comunque rari i casi di violazioni della sicurezza tramite checksum non validi. *Impostazione predefinita: ENABLED.*

LogNonIP4

Consente di registrare le occorrenze dei pacchetti IP che non appartengono alla versione 4. Infatti, la versione 5 di EnterNet FireWall accetta solo i pacchetti IP della versione 4, tutto il resto viene eliminato. *Impostazione predefinita: ENABLED.*

LogReceivedTTL0

Consente di registrare le occorrenze dei pacchetti IP ricevute con il valore TTL (Time To Live) impostato su zero. Un'unità di rete non dovrebbe in nessun caso inviare pacchetti con il valore TTL impostato su 0. *Impostazione predefinita: ENABLED.*

TTLMin

Il valore TTL minimo accettato in conferma. *Impostazione predefinita: 3.*

TTLonLow

Consente di stabilire l'azione da intraprendere sui pacchetti che presentano valori TTL inferiori a quelli minimi stabiliti.

Impostazione predefinita: DropLog

DefaultTTL

Consente di specificare il valore TTL che EnterNet FireWall dovrà utilizzare durante la creazione di un pacchetto. Tali valori sono generalmente compresi tra 64 e 255 255.

LayerSizeConsistency

Verifica che le informazioni sulle dimensioni contenute in ciascun livello (Ethernet, IP, TCP, UDP, ICMP) siano coerenti con quelle degli altri livelli. *Impostazione predefinita:*

ValidateLogBad.

IPOptionSizes

Verifica le dimensioni delle opzioni IP. Tali opzioni rappresentano piccoli blocchi di informazioni che possono essere aggiunti alla fine di ogni intestazione IP. Questa funzione consente di verificare le dimensioni dei tipi di opzioni note e garantisce che nessuna opzione superi il limite fissato dall'intestazione IP stessa. *Impostazione predefinita:*

ValidateLogBad.

IPOPT_SR

Indica se le opzioni relative all'origine di instradamento sono autorizzate. Tramite queste opzioni il mittente del pacchetto è in grado di controllare le relative modalità di instradamento attraverso ciascun router e firewall. Poiché ciò rappresenta un grave rischio per la sicurezza, EnterNet FireWall non rispetta mai i percorsi di origine specificati da queste opzioni, indipendentemente dall'impostazione. *Impostazione predefinita: DropLog*

IPOPT_TS

Le opzioni relative all'indicatore di orario consentono di comunicare a tutti i router e firewall il percorso del pacchetto per stabilire in quale ora esso è stato inoltrato in quel percorso. Tali opzioni non vengono utilizzate nel traffico normale. Inoltre, gli indicatori orari consentono di "registrare" il percorso intrapreso da un pacchetto, dal mittente al destinatario finale. EnterNet FireWall non consente di inserire dati all'interno di queste opzioni, indipendentemente dall'impostazione in oggetto. *Impostazione predefinita: DropLog.*

IPOPT_OTHER

Tutte le opzioni ad eccezione di quelle sopra descritte. *Impostazione predefinita: DropLog.*

DirectedBroadcasts

Indica se il firewall inoltrerà i pacchetti che sono diretti all'indirizzo broadcast delle reti ad esso direttamente collegate. È possibile utilizzare tale funzione dalla sezione Rules, dopo aver aggiunto delle righe. Tuttavia, l'opzione è inclusa anche in questo menu per semplificare le procedure. Questo metodo di convalida è più veloce delle voci nella sezione Rules, in quanto più particolareggiato. *Impostazione predefinita: DropLog.*

IPRF

Indica le operazioni che dovrà eseguire il firewall se i campi "riservati" delle intestazioni IP contengono informazioni. Generalmente, tali campi dovrebbero leggere 0. Utilizzato dal fingerprinting del sistema operativo. *Impostazione predefinita: DropLog.*

StripDFOnSmall

Sfoggia il flag Dont Fragment dei pacchetti che presentano una dimensione minore o uguale a quella specificata nell'impostazione. *Impostazione predefinita: 500 byte.*

7.3.2.2 Impostazioni di livello TCP

TCPOptionSizes

Verifica le dimensioni delle opzioni TCP. Questa funzione corrisponde all'opzione `IPOptionSizes` sopra descritta.

Impostazione predefinita: ValidateLogBad.

TCPMSSMin

Consente di specificare le dimensioni minime accettabili di TCP MSS. I pacchetti che contengono segmenti con dimensioni massime inferiori al valore limite specificato vengono gestiti secondo la seguente impostazione. *Impostazione predefinita: 100 byte.*

TCPMSSOnLow

Consente di stabilire l'azione intrapresa sui pacchetti la cui opzione TCP MSS presenta valori inferiori a quelli minimi stipulati. I valori troppo bassi potrebbero causare problemi negli stack TCP che includono pochi dati. *Impostazione predefinita: DropLog.*

TCPMSSMax

Consente di specificare la massima dimensione TCP MSS accettabile. I pacchetti che contengono segmenti le cui dimensioni massime superano questo limite vengono gestiti secondo la seguente impostazione. *Impostazione predefinita: 1460 byte.*

TCPMSSOnHigh

Consente di stabilire l'azione intrapresa sui pacchetti la cui opzione TCP MSS presenta valori superiori a quelli massimi stipulati. I valori troppo alti potrebbero creare problemi negli stack TCP che includono pochi dati, oppure potrebbero essere causa di numerose frammentazioni dei pacchetti a discapito delle prestazioni. *Impostazione predefinita: Adjust.*

TCPMSSLogLevel

Consente di stabilire quando effettuare la registrazione in caso di valori TCP MSS troppo alti non registrati da `TCPMSSOnHigh`. *Impostazione predefinita: 7000 byte.*

TCPZeroUnusedACK

Consente di comunicare al firewall se impostare su 0 il campo relativo al numero di sequenza ACK dei pacchetti TCP, se non utilizzato. Alcuni sistemi operativi riportano le informazioni sul numero di sequenza in questo modo e potrebbero quindi agevolare intrusioni indesiderate nelle connessioni protette.
Impostazione predefinita: ABILITATO.

TCPOPT_WSOPT

Consente di specificare le modalità di gestione delle opzioni relative alle proporzioni delle finestre da parte del firewall. Tali funzioni consentono di aumentare la dimensione delle finestre utilizzate dal protocollo TCP, ovvero la quantità di informazioni che è possibile inviare prima che il mittente riceva un messaggio ACK Utilizzati anche dal fingerprinting del sistema operativo. WSOPT rappresenta un'occorrenza comune nelle reti moderne. *Impostazione predefinita: ValidateLogBad.*

TCPOPT_SACK

Consente di definire le modalità di gestione delle opzioni di riconoscimento selettivo da parte del firewall. Tali opzioni vengono utilizzate nei singoli pacchetti ACK piuttosto che nelle serie complete per aumentare le prestazioni delle connessioni nelle quali si verifica una grande perdita di dati. Utilizzati anche dal fingerprinting del sistema operativo. SACK rappresenta un'occorrenza comune nelle reti moderne.
Impostazione predefinita: ValidateLogBad.

TCPOPT_TSOPT

Consente di definire le modalità di gestione delle opzioni relative all'indicatore della data e ora da parte del firewall. Come stabilito dal metodo PAWS (Protect Against Wrapped Sequence numbers), TSOPT viene utilizzato per evitare che i numeri di sequenza (cifre a 32 bit) superino il limite massimo senza che il destinatario ne sia a conoscenza. Normalmente questo non rappresenta un problema. Tramite TSOPT, alcuni stack TCP ottimizzano la loro connessione misurando il tempo impiegato da un pacchetto per arrivare a destinazione. Quindi, è possibile utilizzare queste informazioni per rinviare il pacchetto in modo più veloce. Utilizzato anche dal fingerprinting del sistema operativo. TSOPT rappresenta un'occorrenza comune nelle reti attuali. *Impostazione predefinita: ValidateLogBad.*

TCPOPT_ALTCHKREQ

Consente di definire le modalità di gestione delle opzioni relative alle richieste di checksum alternate da parte del firewall. Originariamente queste opzioni erano state progettate per garantire l'utilizzo di migliori checksum in TCP durante le fasi di negoziazione. Tuttavia, i sistemi standard attuali non sono in grado di comprendere queste funzioni. Nemmeno EnterNet FireWall sa riconoscere gli algoritmi checksum, ad eccezione di quelli standard. Pertanto, queste opzioni non vengono mai accettate. La funzione ALTCHKREQ è stata eliminata nelle reti odierne. *Impostazione predefinita: StripLog.*

TCPOPT_ALTCHKDATA

Consente di definire le modalità di gestione delle opzioni relative ai dati di checksum alternate da parte del firewall. Tali opzioni vengono utilizzate per trasportare le checksum alternate, se autorizzato dalla funzione ALTCHKREQ precedentemente descritta. In genere, questa funzione non è disponibile nelle reti. *Impostazione predefinita: StripLog.*

TCPOPT_CC

Consente di definire le modalità di gestione delle opzioni relative ai conteggi delle connessioni da parte del firewall. *Impostazione predefinita: StripLogBad.*

TCPOPT_OTHER

Consente di definire le modalità di gestione da parte del firewall delle opzioni TCP non incluse nelle impostazioni precedenti. In genere queste funzioni non sono disponibili nelle reti odierne. *Impostazione predefinita: StripLog.*

TCPSynUrg

Consente di definire le modalità di gestione da parte del firewall dei pacchetti TCP che includono flag SYN (Synchronize) e flag URG (Urgent data) attivati. La presenza di un flag SYN indica che sta per essere aperta una nuova connessione. Un flag URG, invece, si riferisce ad un pacchetto che contiene dati urgenti. Non è possibile attivare i due flag all'interno di un singolo pacchetto, poiché essi vengono utilizzati esclusivamente per arrestare i computer che includono stack TCP scarsamente implementati. *Impostazione predefinita: DropLog.*

TCPSynPsh

Consente di definire le modalità di gestione da parte del firewall dei pacchetti TCP che includono flag SYN e PSH (push) attivati. Il flag PSH indica che lo stack del destinatario dovrebbe immediatamente inviare le informazioni contenute nel pacchetto all'applicazione di destinazione nel computer. Non è possibile attivare contemporaneamente i due flag per evitare rischi di blocco negli stack TCP scarsamente implementati. Tuttavia, molti computer Macintosh non implementano correttamente gli stack TCP e pertanto inviano i pacchetti SYN *sempre* con il flag PSH attivato. Per questo motivo EnterNet FireWall generalmente elimina il flag PSH e consente il passaggio del pacchetto nonostante l'opzione sia impostata per rifiutarlo. *Impostazione predefinita: StripSilent.*

TCPFinUrg

Consente di definire le modalità di gestione da parte del firewall dei pacchetti TCP che includono flag FIN e (Finish, close connection) URG attivati. Questa eventualità non dovrebbe mai verificarsi, poiché generalmente non capita di chiudere una connessione durante l'invio di informazioni "importanti". Principalmente, questa combinazione di flag consente di bloccare gli stack TCP scarsamente implementati e viene anche utilizzata dal fingerprinting del sistema operativo. *Impostazione predefinita: DropLog.*

TCPUrg

Consente di definire le modalità di gestione da parte del firewall dei pacchetti TCP che includono flag URG attivati, indipendentemente dagli altri flag. Molte applicazioni e stack TCP gestiscono i flag urgenti nel modo sbagliato e possono pertanto smettere di funzionare nelle situazioni più critiche. Nonostante ciò, alcuni programmi, quali FTP e MS SQL Server, utilizzano quasi sempre il flag URG. *Impostazione predefinita: StripLog.*

TCPECN

Consente di definire le modalità di gestione da parte del firewall dei pacchetti TCP che includono flag Xmas o Ymas attivati. Tali flag sono molto utilizzati dal fingerprinting del sistema operativo.

Nota: uno standard di prossima uscita, denominato *Explicit Congestion Notification*, utilizzerà i flag TCP. Tuttavia, è consigliabile eliminare tali flag dal momento che pochi sistemi operativi li supportano. *Impostazione predefinita: StripLog.*

TCPRF

Consente di definire le modalità di gestione da parte del firewall delle informazioni incluse nel "campo riservato" dell'intestazione TCP, il cui valore generalmente corrisponde a 0. Questo campo non è uguale ai campi Xmas e Ymas. Utilizzato dal fingerprinting del sistema operativo. *Impostazione predefinita: DropLog.*

TCPNULL

Consente di definire le modalità di gestione da parte del firewall dei pacchetti TCP che non contengono flag SYN, ACK, FIN o RST attivati. Secondo lo standard TCP, tali pacchetti non sono validi e vengono utilizzati dal fingerprinting del sistema operativo e dagli scanner per porte clandestine. Infatti, alcuni firewall non sono in grado di rilevarli.
Impostazione predefinita: DropLog.

7.3.2.3 Impostazioni di livello ICMP

ICMPSendPerSecLimit

Definisce il numero massimo di messaggi ICMP che EnterNet FireWall può generare in un secondo. Sono incluse le risposte del protocollo ping, i messaggi di destinazione non raggiungibile e anche i pacchetti TCP RST. In sostanza, questa opzione limita il numero di rifiuti che possono essere creati in un secondo dalle regole Reject della sezione Rules
Impostazione predefinita: 20 al secondo.

SilentlyDropStateICMPErrors

Consente di stabilire se gli errori ICMP relativi alle connessioni aperte rilevate debbano essere rifiutati dal firewall. Gli errori non eliminati con questa impostazione verranno trasmessi alle regole per essere valutati, come avviene per gli altri pacchetti.
Impostazione predefinita: ABILITATO.

7.3.2.4 Impostazioni ARP

ARPMatchEnetSender

Consente di determinare se il firewall richiederà l'indirizzo del mittente a livello Ethernet per soddisfare l'indirizzo hardware riportato nei dati ARP. *Impostazione predefinita: DropLog.*

ARPQueryNoSenderIP

Gli indirizzi IP del mittente 0.0.0.0 nelle query ARP non sono mai validi per le risposte, ma le unità di rete che non sono ancora a conoscenza del proprio indirizzo IP eseguono talvolta delle richieste ad ARP con IP del mittente "non specificato".
Impostazione predefinita: DropLog.

ARPSenderIP

Consente di determinare se l'indirizzo IP del mittente soddisfa le regole della sezione Access. *Impostazione predefinita: Validate.*

UnsolicitedARPReplies

Consente di determinare in che modo il firewall gestirà le risposte ARP che non sono state richieste. In base alle specifiche ARP, il destinatario le dovrebbe accettare. Poiché questo potrebbe comunque facilitare il dirottamento delle connessioni locali, di regola non è consentito. *Impostazione predefinita: DropLog.*

ARPRequests

Consente di determinare se il firewall aggiungerà automaticamente i dati nelle richieste ARP alla relativa tabella ARP. Nelle specifiche ARP viene definito che l'operazione dovrebbe essere eseguita, ma poiché la procedura può facilitare il dirottamento delle connessioni locali, di regola questa non è consentita. Anche se il parametro ARPRequests è impostato su "Drop", vale a dire che il pacchetto viene scartato senza essere memorizzato, il firewall attiverà la risposta, purché le altre regole approvino la richiesta. *Impostazione predefinita: Drop.*

ARPChanges

Consente di determinare il comportamento del firewall nelle situazioni in cui una risposta o una richiesta ARP ricevuta modifichi un elemento esistente nella tabella ARP. Tale evento può facilitare il dirottamento delle connessioni locali. Tuttavia, se *non* si usa tale impostazione potrebbero verificarsi alcuni problemi quando, ad esempio, viene sostituita una scheda di rete, poiché il firewall non accetterà il nuovo indirizzo finché non è scaduta la voce della tabella ARP precedente.

Impostazione predefinita: AcceptLog.

StaticARPChanges

Consente di determinare il comportamento del firewall nelle situazioni in cui una risposta o una richiesta ARP ricevuta modifichi un elemento *statico* nella tabella ARP. Naturalmente, ciò non deve mai verificarsi. Tuttavia, tale impostazione non consente di specificare se tali eventi debbano essere registrati.

Impostazione predefinita: DropLog.

ARPExpire

Specifica la durata di conservazione di un elemento dinamico nella tabella ARP prima che venga rimosso. *Impostazione predefinita: 900 secondi (15 minuti).*

ARPExpireUnknown

Specifica il periodo di tempo in cui il firewall deve ricordare gli indirizzi che non possono essere raggiunti. Ciò consente di evitare che il firewall richieda in continuazione tali indirizzi.

Impostazione predefinita: 15 secondi.

ARPMulticast

Definisce la modalità in cui il firewall gestisce le richieste e le risposte ARP in cui sono presenti indirizzi multicast. Tali richieste non sono quasi mai corrette, con la sola eccezione di alcuni dispositivi di ridondanza e di bilanciamento del carico, che utilizzano gli indirizzi multicast a livello hardware.

Impostazione predefinita: DropLog.

ARPBroadcast

Definisce la modalità in cui il firewall gestisce le richieste e le risposte ARP in cui sono presenti indirizzi broadcast. Tali richieste non sono quasi mai corrette. *Impostazione predefinita: DropLog.*

7.3.2.5 Impostazioni Stateful Inspection

ConnReplace

Consente di aggiungere voci all'elenco delle connessioni del firewall, sostituendo le vecchie connessioni nel caso in cui non vi sia più spazio disponibile. *Impostazione predefinita: ReplaceLog.*

LogOpenFails

Nei casi in cui la sezione Rules determini che un pacchetto possa essere autorizzato a passare, il meccanismo di ispezione dello stato può decidere successivamente che il pacchetto non possa aprire una nuova connessione. Un chiaro esempio è il pacchetto TCP che, sebbene autorizzato dalla sezione Rules e non facendo parte di una connessione attiva, ha il flag SYN disabilitato. Tali pacchetti non possono mai aprire nuove connessioni. Inoltre, le nuove connessioni non possono mai essere aperte da messaggi ICMP diversi da ICMP ECHO (Ping). Questa impostazione determina se il firewall deve registrare l'occorrenza di tali pacchetti. *Impostazione predefinita: ABILITATO.*

LogReverseOpens

Determina se il firewall registrerà i pacchetti che tentano di riaprire una nuova connessione attraverso una già aperta. Nella versione 5.1, ciò si applica solo ai pacchetti TCP con il flag SYN abilitato e ai pacchetti ICMP ECHO. Per gli altri protocolli, come UDP, non è possibile determinare se il peer remoto stia tentando di aprire una nuova connessione. *Impostazione predefinita: ABILITATO.*

LogStateViolations

Determina se il firewall deve registrare i pacchetti che violano il diagramma di commutazione dello stato previsto per una connessione, ad esempio, accettare i pacchetti TCP FIN in risposta ai pacchetti TCP SYN. *Impostazione predefinita: ABILITATO.*

MaxConnections

Specifica il numero di connessioni che il firewall può tenere aperte contemporaneamente. Ciascuna connessione richiede circa 150 byte di RAM. *Impostazione predefinita: 4096 connessioni contemporanee.*

StrictIfaceMatching

Determina se il firewall riceverà le risposte sulla stessa interfaccia da cui è stata inviata la richiesta originale. In genere, tale funzione non influenza il sistema purché l'elenco di accesso sia configurato in modo tale che solo un dato indirizzo IP venga autorizzato come mittente su un'interfaccia specifica. *Impostazione predefinita: ABILITATO.*

DynamicNATBasePort

Specifica la prima porta di origine che il firewall deve utilizzare durante il NAT dinamico NAT (NAT Hide). Le porte utilizzate iniziano con questo valore e continuano con numeri crescenti finché non viene raggiunto il valore impostato dall'opzione *MaxConnections*. *Impostazione predefinita: 32768.*

LogConnections

Specifica la modalità in cui il firewall registra le connessioni:

- **NoLog** – Le connessioni non vengono registrate; ne consegue che non è importante se la registrazione è attiva per le regole Allow o NAT nella sezione Rules. Le connessioni non verranno comunque registrate. Tuttavia, le regole FwdFast, Drop e Reject saranno registrate in base alle impostazioni della sezione Rules.

- **Log** – Registra le connessioni in formato ridotto; fornisce una breve descrizione della connessione, della regola con cui è stata autorizzata e le regole SAT applicabili. Le connessioni saranno registrate anche quando sono chiuse.
- **LogOC** – Simile all'opzione Log, ma include anche le informazioni sui due pacchetti che aprono e chiudono la connessione. Se la connessione viene chiusa perché scaduta, non verrà registrato il pacchetto finale.
- **LogOCAll** – Registra tutti i pacchetti coinvolti nell'apertura e nella chiusura della connessione. Nel caso del protocollo TCP, tale opzione interessa tutti i pacchetti con i flag SYN, FIN o RST attivi.
- **LogAll** – Registra tutti i pacchetti della connessione.

Impostazione predefinita: Log

LogDisallowedReturnData

Specifica se saranno registrati i tentativi per l'invio dei dati di ritorno sulle connessioni unidirezionali. Tali pacchetti vengono eliminati a prescindere dal fatto che siano o non siano registrati.

Impostazione predefinita: ABILITATO.

7.3.2.6 Timeout di una connessione

Le impostazioni incluse in questa sezione specificano la durata di inattività di una connessione, ad esempio quando non esiste più traffico di dati, prima che questa venga chiusa automaticamente. Notare che ciascuna connessione ha due valori di timeout: uno per ciascuna direzione. Una connessione viene terminata se entrambi i valori sono uguali a 0.

ConnLife_TCP_SYN

Specifica la durata di inattività di una connessione TCP non ancora completamente stabilita prima che venga terminata.

Impostazione predefinita: 60 secondi.

ConnLife_TCP

Specifica la durata di inattività di una connessione TCP completamente stabilita prima che venga terminata. Le connessioni diventano completamente stabilite non appena i pacchetti, con i rispettivi flag SYN disattivati, viaggiano in entrambe le direzioni. *Impostazione predefinita: 3600 secondi (60 minuti).*

ConnLife_TCP_FIN

Specifica la durata di inattività di una connessione TCP in procinto di essere chiusa prima che venga terminata. Le connessioni raggiungono questo stato quando un pacchetto con il flag FIN attivo è passato in entrambe le direzioni. *Impostazione predefinita: 80 secondi.*

ConnLife_UDP

Specifica la durata di inattività di una connessione con il protocollo UDP prima che venga terminata. Il valore di timeout è generalmente basso, in quanto il protocollo UDP non ha modo di segnalare quando la connessione sta per terminare. *Impostazione predefinita: 130 secondi.*

ConnLife_Ping

Specifica la durata di inattività di una connessione Ping (ICMP ECHO) prima che venga terminata. *Impostazione predefinita: 8 secondi.*

ConnLife_Other

Specifica la durata di inattività di una connessione che utilizza un protocollo sconosciuto prima che venga terminata. *Impostazione predefinita: 130 secondi.*

7.3.2.7 Limiti di dimensioni in base al protocollo

Questa sezione contiene informazioni sui limiti delle dimensioni imposti ai protocolli direttamente sotto il livello IP, ad esempio TCP, ICMP, UDP e così via.

I valori indicati di seguito riguardano i dati IP contenuti nei pacchetti. Nel caso di una rete Ethernet, un singolo pacchetto può contenere fino a 1480 byte di dati IP senza frammentazione. Inoltre, esistono altri 20 byte di intestazione IP e 14 byte di intestazione Ethernet, che corrispondono all'unità di trasmissione massima del supporto sulle reti Ethernet pari a 1514 byte.

MaxTCPLen

Specifica la dimensione massima di un pacchetto TCP inclusa l'intestazione. Questo valore si riferisce spesso al totale dei dati IP che possono essere inseriti in un pacchetto non frammentato, dal momento che il protocollo TCP adatta generalmente i segmenti inviati in base alla dimensione massima del pacchetto. Tuttavia, questo valore deve essere aumentato di 20-50 byte su alcuni sistemi VPN meno comuni. *Impostazione predefinita: 1480 byte.*

MaxUDPLen

Specifica la dimensione massima dei pacchetti per il protocollo UDP, inclusa l'intestazione. Il valore richiesto potrebbe essere alto, visto che molte applicazioni in tempo reale utilizzano pacchetti UDP di grandi dimensioni. Se non vengono utilizzati tali protocolli, il limite delle dimensioni imposto sui pacchetti UDP può essere ridotto a 1480 byte. *Impostazione predefinita: 60000 byte.*

MaxICMPLen

Specifica la dimensione massima dei pacchetti ICMP. I messaggi di errore ICMP non devono mai superare i 600 byte, sebbene i pacchetti Ping possano essere più grandi se richiesto. Tale valore può essere ridotto a 1000 byte se non si desidera utilizzare i pacchetti Ping. *Impostazione predefinita: 10000 byte.*

MaxGRELen

Specifica la dimensione massima di un pacchetto GRE. Il pacchetto GRE (Generic Routing Encapsulation) consente vari utilizzi, inclusi il trasporto dei dati PPTP (Point to Point Tunneling Protocol). Il valore dovrebbe essere impostato in base alle dimensioni del pacchetto più grande cui è consentito il passaggio nelle connessioni VPN, indipendentemente dal protocollo originale, aggiungendo circa 50 byte. *Impostazione predefinita: 2000 byte.*

MaxESPLen

Specifica la dimensione massima di un pacchetto ESP. Il pacchetto ESP (Encapsulation Security Payload) viene utilizzato da IPsec quando è richiesta la funzione di crittografia. Il valore dovrebbe essere impostato in base alle dimensioni del pacchetto più grande cui è consentito il passaggio nelle connessioni VPN, indipendentemente dal protocollo originale, aggiungendo circa 50 byte. *Impostazione predefinita: 2000 byte.*

MaxAHLen

Specifica la dimensione massima di un pacchetto AH. Il pacchetto AH (Authentication Header) viene utilizzato da IPsec quando è richiesta solo la funzione di autenticazione. Il valore dovrebbe essere impostato in base alle dimensioni del pacchetto più grande cui è consentito il passaggio nelle connessioni VPN, indipendentemente dal protocollo originale, aggiungendo circa 50 byte. *Impostazione predefinita: 2000 byte.*

MaxSKIPLen

Specifica la dimensione massima di un pacchetto SKIP.
Impostazione predefinita: 2000 byte.

MaxOSPFLen

Specifica la dimensione massima di un pacchetto OSPF. L'OSPF è un protocollo di instradamento utilizzato principalmente in reti LAN di grandi dimensioni. *Impostazione predefinita: 1480.*

MaxIPIPLen

Specifica la dimensione massima di un pacchetto IP-in-IP. Questo pacchetto viene utilizzato dalle connessioni VPN di tipo Checkpoint Firewall-1 quando non è adottato il protocollo IPsec. Il valore dovrebbe essere impostato in base alle dimensioni del pacchetto più grande cui è consentito il passaggio nelle connessioni VPN, indipendentemente dal protocollo originale, aggiungendo circa 50 byte. *Impostazione predefinita: 2000 byte.*

MaxIPCompLen

Specifica la dimensione massima di un pacchetto IPComp. *Impostazione predefinita: 2000 byte.*

MaxL2TPLen

Specifica la dimensione massima di un pacchetto Layer 2 Tunneling Protocol. *Impostazione predefinita: 2000 byte.*

MaxOtherSubIPLen

Specifica la dimensione massima dei pacchetti con protocolli non specificati precedentemente. *Impostazione predefinita: 1480 byte.*

LogOversizedPackets

Specifica se il firewall deve registrare i pacchetti che superano le dimensioni consentite. *Impostazione predefinita: ABILITATO.*

7.3.2.8 Impostazioni di frammentazione

Il protocollo IP è in grado di trasportare fino a 65536 byte di dati. Tuttavia, la maggior parte dei supporti, come ad esempio la rete Ethernet, non può trasferire pacchetti così grandi. In compenso, lo stack IP *frammenta* i dati da inviare in pacchetti separati, ciascuno dei quali con la propria intestazione IP e le relative informazioni che consentiranno al destinatario di *riassemblare* correttamente il pacchetto originale.

Tuttavia, molti stack IP non sono in grado di gestire correttamente i pacchetti frammentati, cosa che può essere sfruttata da intrusi indesiderati per bloccare tali sistemi. Il sistema EnterNet FireWall fornisce vari di tipi di protezione contro gli attacchi compiuti sulla frammentazione dei pacchetti.

IllegalFrag

Determina la modalità in cui il firewall gestisce i frammenti ricostruiti in modo non corretto. Il termine "ricostruiti in modo non corretto" si riferisce ai frammenti sovrapposti, duplicati con dati diversi, con dimensioni di frammentazioni non corrette e così via. Le impostazioni possibili sono le seguenti:

- **Drop** – Elimina il frammento non valido senza registrarlo. Consente inoltre di ricordare che il pacchetto da riassembleare è sospetto e questa informazione può essere utilizzata per una registrazione successiva.
- **DropLog** – Elimina e registra il frammento non valido. Consente inoltre di ricordare che il pacchetto da riassembleare è sospetto e questa informazione può essere utilizzata per una registrazione successiva.
- **DropPacket** – Elimina il frammento non valido e tutti i frammenti memorizzati in precedenza. Ciò non consente ad altri frammenti del pacchetto di passare durante i secondi *ReassIllegalLinger*.
- **DropLogPacket** – Simile all'opzione DropPacket, ma consente anche di registrare l'evento.
- **DropLogAll** – Simile all'opzione DropLogPacket, ma registra anche gli altri frammenti appartenenti a questo pacchetto che arrivano durante i secondi *ReassIllegalLinger*.

La scelta di eliminare i singoli frammenti o bloccare l'intero pacchetto dipende da due fattori:

- È più sicuro eliminare l'intero pacchetto.

- Se, in seguito al ricevimento di un frammento non valido, si sceglie di eliminare l'intero pacchetto, i pirati informatici potranno bloccare la comunicazione inviando frammenti non validi durante un riassettaggio, interrompendo quasi tutte le comunicazioni.

Impostazione predefinita: DropLog – elimina i frammenti e ricorda che il tentativo di riassettaggio è "sospetto".

DuplicateFragData

Se viene ricevuto più di una volta lo stesso frammento, è possibile che questo sia stato duplicato in un punto qualsiasi del tragitto verso il destinatario *oppure* che un pirata informatico stia cercando di sabotare il riassettaggio del pacchetto. Per determinare quale situazione sia la più probabile, EnterNet FireWall confronta i componenti dei dati del frammento. Tale confronto avviene su un numero di posizioni casuali all'interno del frammento che può oscillare da 2 a 512, verificando quattro byte per ciascuna posizione. Se il confronto viene eseguito su un numero di campioni maggiore, è probabile che vengano individuati alcuni duplicati non compatibili. Tuttavia, notare che più aumenta il numero di confronti e maggiore sarà il carico della CPU. *Impostazione predefinita: Check8 – confronta 8 posizioni casuali, un totale di 32 byte.*

FragReassemblyFail

Il riassettaggio potrebbe non riuscire a causa di una dei seguenti problemi:

- Alcuni frammenti non sono arrivati nel tempo stabilito dalle impostazioni ReassTimeout o ReassTimeLimit. Ciò significa che uno o più frammenti sono andati persi nel loro percorso in Internet, un evento abbastanza frequente.
- Il firewall ha interrotto la procedura di riassettaggio a causa dell'arrivo di nuovi pacchetti frammentati che hanno temporaneamente assorbito tutte le risorse. In tali situazioni, i tentativi di riassettaggio precedenti vengono interrotti o contrassegnati come "non riuscito".
- Un pirata informatico ha tentato di inviare un pacchetto frammentato in modo non corretto.

In normali circostanze, non è necessario registrare gli errori visto che questi si verificano di frequente. Tuttavia, potrebbe essere utile registrare gli errori relativi ai frammenti "sospetti". Tali errori possono verificarsi se, ad esempio, l'impostazione `IllegalFragments` è stata impostata su `Drop` piuttosto che su `DropPacket`.

Le seguenti impostazioni sono disponibili per l'opzione `FragmentsReassemblyFail`:

- **NoLog** – Non viene eseguita alcuna registrazione quando un tentativo di riassettaggio non riesce.
- **LogSuspect** – Registra i tentativi di riassettaggio non riusciti solo nel caso in cui sono stati individuati frammenti "sospetti".
- **LogSuspectSubseq** – Simile all'opzione `LogSuspect`, ma registra anche i frammenti successivi del pacchetto non appena arrivano.
- **LogAll** – Registra tutti i tentativi di riassettaggio non riusciti.
- **LogAllSubseq** – Simile all'opzione `LogAll`, ma registra anche i frammenti successivi del pacchetto non appena arrivano.

Impostazione predefinita: `LogSuspectSubseq`.

DroppedFragments

Se un pacchetto non viene autorizzato ad entrare nel sistema in base alle impostazioni della sezione `Rules`, potrebbe essere utile registrare i singoli frammenti del pacchetto. L'impostazione `DroppedFragments` specifica il comportamento del firewall. Le impostazioni possibili per questa regola sono le seguenti:

- **NoLog** – Non viene eseguita alcuna registrazione su ciò che è definito nel set di regole.
- **LogSuspect** – Registra i singoli frammenti identificati nei tentativi di riassettaggio come frammenti "sospetti".
- **LogAll** – Registra sempre i singoli frammenti.

Impostazione predefinita: `LogSuspect`.

DuplicateFrag

Se viene ricevuto più di una volta lo stesso frammento, è possibile che questo sia stato duplicato in un punto qualsiasi del tragitto verso il destinatario *oppure* che un pirata informatico stia cercando di sabotare il riassettaggio del pacchetto. L'opzione DuplicateFrag determina se tale frammento sarà registrato. Notare che l'impostazione DuplicateFragData può registrare tali frammenti se i dati contenuti in essi non corrispondono. Le impostazioni possibili sono le seguenti:

- **NoLog** – In normali circostanze, non viene eseguita alcuna registrazione.
- **LogSuspect** – Registra i frammenti duplicati se nella procedura di riassettaggio sono stati identificati frammenti "sospetti".
- **LogAll** – Registra sempre i frammenti duplicati.

Impostazione predefinita: LogSuspect.

FragmentedICMP

Diversi dal protocollo ICMP ECHO (Ping), i messaggi ICMP generalmente non devono essere frammentati, in quanto contengono pochi dati e la frammentazione non si rende necessaria. L'impostazione FragmentedICMP determina il comportamento del firewall quando riceve i messaggi ICMP frammentati che non sono né ICMP ECHO né ECHOREPLY.

Impostazione predefinita: DropLog.

MinimumFragLength

L'opzione MinimumFragLength determina la dimensione minima di tutti i frammenti, con la sola eccezione del frammento finale. Sebbene l'arrivo di troppi frammenti di dimensioni molto piccole possa causare problemi per gli stack IP, spesso non è possibile impostare questo limite troppo alto. È tuttavia raro che i mittenti creino frammenti molto piccoli. Quando un mittente invia frammenti di 1480 byte, un router o tunnel VPN sul percorso verso il destinatario può ridurre successivamente il valore effettivo dell'unità MTU a 1440 byte. Ciò crea svariati frammenti di 1440 byte e un numero uguale di frammenti di 40 byte. Visti i problemi che potrebbero verificarsi, in EnterNet FireWall è stata studiata un'impostazione predefinita che permette di far passare i frammenti più piccoli possibili, vale a dire fino a 8 byte. Per uso interno, dove si conoscono le dimensioni di tutti i supporti, questo valore può essere aumentato fino a 200 byte o superiore.

Impostazione predefinita: 8 byte. ReassTimeout

Un tentativo di riassemblaggio verrà interrotto se non arrivano altri frammenti nel limite di tempo in secondi definito dall'opzione *ReassTimeout* a partire dal momento della ricezione dell'ultimo frammento. *Impostazione predefinita: 65 secondi.*

ReassTimeLimit

Un tentativo di riassemblaggio verrà sempre interrotto se è stato superato il limite di tempo in secondi definito dall'opzione *ReassTimeLimit* dopo l'arrivo del primo frammento ricevuto. *Impostazione predefinita: 90 secondi.*

ReassDoneLinger

Una volta riassemblato un pacchetto, il firewall è in grado di ricordarlo per un breve periodo di tempo in modo da evitare che arrivino altri frammenti di quel pacchetto quali, ad esempio, vecchi frammenti duplicati. *Impostazione predefinita: 20 secondi.*

ReassIllegalLinger

Una volta contrassegnato l'intero pacchetto come non valido, il firewall è in grado di conservarlo in memoria per impedire l'arrivo di altri frammenti di quel pacchetto. *Impostazione predefinita: 60 secondi.*

7.3.2.9 Impostazioni di auditing**LogSendPerSecLimit**

Questa impostazione limita il numero di pacchetti registrati che il sistema EnterNet FireWall può inviare ogni secondo. Il valore non dovrebbe mai essere troppo basso, poiché potrebbero verificarsi eventi importanti che non vengono registrati. Un valore troppo alto invece potrebbe causare problemi quando il firewall invia un messaggio di log al server in cui la funzione di ricezione del log non è attiva. Il server risponde con un messaggio ICMP UNREACHABLE che potrebbe portare il firewall ad inviare un altro messaggio di log, che a sua volta genererà un altro messaggio ICMP UNREACHABLE e così via. Ponendo un limite al numero di messaggi di log che il firewall invia ogni secondo, si evita di incorrere in tali situazioni in cui vi è un enorme consumo della larghezza di banda. *Impostazione predefinita: 100 messaggi al secondo.*

UsageLogInterval

EnterNet FireWall invia periodicamente le informazioni sulle connessioni aperte e il carico di rete ai destinatari dei log. L'opzione UsageLogInterval ne specifica la frequenza. *Impostazione predefinita: 3600 secondi, ogni ora.*

7.3.2.10 Impostazioni varie

NetConBiDirTimeout

Quando si carica una nuova configurazione, il firewall prova a ristabilire una comunicazione bidirezionale con Firewall Manager in modo da garantire la raggiungibilità del firewall. Questa impostazione specifica la durata di attesa prima che il firewall ritorni alla configurazione precedente. *Impostazione predefinita: 30 secondi.*

BuffFloodRebootTime

Il firewall si riavvia automaticamente se i buffer sono stati ridondanti per lungo tempo. Questa impostazione definisce il periodo di tempo necessario. *Impostazione predefinita: 3600 secondi.*

ScrSaveTime

Il tempo in secondi prima che il firewall attivi automaticamente un salvaschermo. Il salvaschermo adatterà automaticamente la propria attività al carico corrente della CPU del sistema. In caso di carichi elevati, si aggiornerà una volta al secondo, consumando una percentuale minima del carico della CPU. *Impostazione predefinita: 300 secondi (5 minuti).*

HighBuffers

Il numero di buffer da allocare alla RAM superiore al limite di 1 MB. Nota: dal momento che i driver ODI non possono accedere alla RAM superiore a 1 MB, non verranno allocati buffer più elevati quando si utilizzano questi driver. Nella RAM bassa, esiste in genere spazio sufficiente per 200 buffer, in base al numero di driver ODI caricati. *Impostazione predefinita: 1024 buffer*

BOOTPRelay

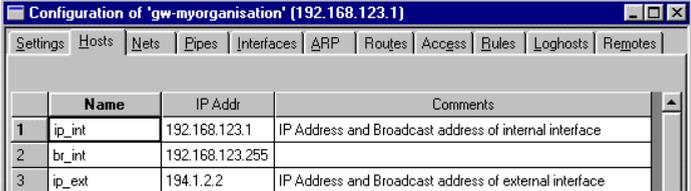
Attiva o disattiva un semplice relay BOOTP/DHCP nel software del firewall. Si tratta di una funzione abbastanza semplice e senza concetto di stato. Questa opzione può essere considerata una funzionalità "precedente al rilascio" e non dovrebbe essere attivata se non si conoscono bene le conseguenze che potrebbero derivarne. Rivolgersi al personale di supporto tecnico di EnterNet per una descrizione completa e aggiornata dei relativi effetti prima di attivare tale funzione.

Impostazione predefinita: OFF

MaxPipeUsers

Il numero massimo di utenti pipe da allocare. Poiché gli utenti pipe vengono identificati per un ventesimo di secondo, non è necessario che tale numero sia prossimo al numero degli utenti effettivi oppure a quello delle connessioni di stato identificate. Se i pipe non sono stati configurati, è impossibile allocare utenti pipe, a prescindere da questa impostazione. Per ulteriori informazioni sui pipe e sui relativi utenti, consultare il capitolo 10, Configurazione del traffico. Impostazione predefinita: 512.

7.3.3 Scheda Hosts



	Name	IP Addr	Comments
1	ip_int	192.168.123.1	IP Address and Broadcast address of internal interface
2	br_int	192.168.123.255	
3	ip_ext	194.1.2.2	IP Address and Broadcast address of external interface

La scheda Hosts consente di specificare le coppie di nomi simbolici e di indirizzi IP numerici. Ciò consente di semplificare l'amministrazione del firewall, poiché i nomi simbolici possono essere utilizzati al posto degli indirizzi IP numerici laddove vengono richieste tali informazioni. Gli elementi aggiunti qui sono visualizzati anche automaticamente in elenchi a discesa dove è possibile specificare indirizzi IP e/o nomi host.

L'utilizzo di nomi simbolici fornisce all'utente i seguenti tre vantaggi: aumenta la leggibilità, riduce il rischio di immettere indirizzi IP numerici non corretti e consente di modificare gli indirizzi IP in modo più facile, nel caso in cui l'indirizzo di un server, ad esempio, fosse cambiato. Utilizzando i nomi simbolici invece di indirizzi IP numerici, è necessario eseguire le modifiche in una singola posizione, nella scheda Hosts, invece che in ciascuna sezione di configurazione in cui appaiono tali indirizzi.



Non è necessario utilizzare i nomi simbolici in tutta la configurazione. Se è più semplice immettere l'indirizzo IP numerico, utilizzare quindi tale soluzione. In questo modo non è necessario impostare una voce host e poi utilizzare il nome simbolico.

7.3.4 Scheda Nets

	Name	Net Addr	Comments
1	intnet	192.168.123.0/24	Internal network - the one that is protected
2	extnet	194.1.2.0/24	External network - the one connected directly to the external...
3	all-nets	0.0.0.0/0	All possible networks, including intnet and extnet

La scheda Nets consente di specificare le coppie di nomi simbolici e di indirizzi IP numerici con le maschere di rete. Ciò consente di semplificare l'amministrazione del firewall, poiché i nomi simbolici possono essere utilizzati al posto degli indirizzi di rete numerici laddove vengono richieste tali informazioni. Gli elementi aggiunti qui sono visualizzati anche automaticamente in elenchi a discesa in cui è possibile specificare gli indirizzi di rete.



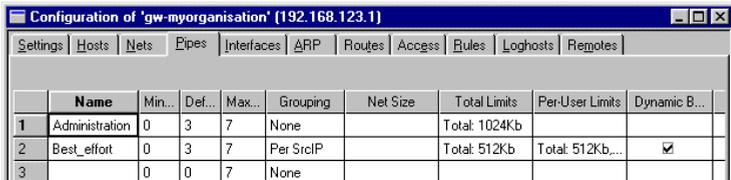
Notare che gli indirizzi di rete vengono specificati in relazione all'indirizzo di base della rete, e *non* con un indirizzo appartenente alla rete quale l'indirizzo IP del firewall. Se non si conosce il significato del termine indirizzo di rete, contattare il service provider di Internet (ISP).

L'utilizzo di nomi di rete simbolici fornisce all'utente i seguenti tre vantaggi: aumenta la leggibilità, riduce il rischio di immettere indirizzi di rete non corretti e consente di modificare gli indirizzi di rete in modo più facile, nel caso in cui l'indirizzo di rete, ad esempio, fosse stato cambiato. Utilizzando i nomi simbolici invece di indirizzi numerici, è necessario eseguire le modifiche in una singola posizione, nella scheda Nets, piuttosto che in ciascuna sezione di configurazione in cui appaiono gli indirizzi.



Non è necessario utilizzare i nomi simbolici in tutta la configurazione. Se è più semplice immettere l'indirizzo numerico di rete, utilizzare quindi tale soluzione. In questo modo non è necessario impostare una nuova voce di rete e poi utilizzare il nome simbolico.

7.3.5 Scheda Pipes



	Name	Min...	Def...	Max...	Grouping	Net Size	Total Limits	Per-User Limits	Dynamic B...
1	Administration	0	3	7	None		Total: 1024Kb		
2	Best_effort	0	3	7	Per SrcIP		Total: 512Kb	Total: 512Kb...	<input checked="" type="checkbox"/>
3		0	0	7	None				

La scheda Pipes consente di specificare i *pipe* da utilizzare per la configurazione del traffico. Utilizzando i pipe in una configurazione appropriata, il firewall è in grado di garantire la larghezza di banda della rete nonché di limitarne l'utilizzo in base alle diverse reti e ai tipi servizi. I pipe definiti nella tabella seguente saranno utilizzati in seguito nella colonna Pipes della scheda Rules.



La configurazione del traffico rientra nelle funzionalità avanzate di EnterNet FireWall e non è consigliabile ad utenti principianti.

Per una descrizione dettagliata sulla configurazione del traffico e dei pipe per i diversi usi, consultare il capitolo 10, Configurazione del traffico.

- **Name** – Specifica un nome simbolico per il pipe. Questo nome viene utilizzato nelle impostazioni dei pipe della scheda Rules.
- **Min Prec** – Ciascun pipe è composto da 8 differenti precedenze, numerate da 0 a 7. Questa impostazione specifica la precedenza *più bassa consentita* per il traffico in questo pipe. Se entra un pacchetto con una precedenza inferiore, questa viene aumentata al valore contenuto in questo campo. Il valore può variare da 0 a 7.
- **Def Prec** – Specifica la precedenza *predefinita* per il pipe. Se un pacchetto entra in questo pipe senza una precedenza già impostata, gli viene assegnata la precedenza predefinita. Il valore può variare da 0 a 7, ma deve essere maggiore o uguale alla precedenza minima.

- **Max Prec** – Specifica la precedenza più alta consentita per il traffico in questo pipe. Se entra un pacchetto con una precedenza superiore, questa viene ridotta al valore contenuto in questo campo. Il valore può variare da 0 a 7, ma deve essere superiore o uguale alla precedenza predefinita.
- **Grouping** – La limitazione e la prenotazione del traffico possono applicarsi anche ai singoli utenti di un pipe; allo stesso modo in cui vengono applicati globalmente a un pipe. Gli utenti possono essere raggruppati in base alla rete di destinazione, all'indirizzo IP di destinazione, alla porta di destinazione, alla rete di origine, all'indirizzo IP di origine e alla porta di origine. Nota: il raggruppamento per *porta* significa implicitamente raggruppamento per *IP*; la porta 1025 su un computer *non* è uguale alla porta 1025 di un altro computer.
- **Net Size** – Se gli utenti sono raggruppati in base alla rete di origine e di destinazione, la dimensione della rete deve essere specificata in questa impostazione.
- **Total Limit** – Mostra una breve panoramica dei limiti del traffico di rete per questo pipe. Facendo clic su questa colonna si apre una finestra di dialogo che contiene informazioni dettagliate. Consultare la sezione 7.3.5.1, Finestra di dialogo Total Limit, più avanti.
- **Per-user Limit** – Mostra una breve panoramica dei limiti del traffico di rete relativo a ciascun utente per questo pipe. Facendo clic su questa colonna si apre una finestra di dialogo che contiene informazioni dettagliate. Consultare la sezione 7.3.5.2, Finestra di dialogo User Limit, più avanti.
- **Dynamic Balancing** – Determina se il bilanciamento dinamico della larghezza di banda debba essere applicato agli utenti di questo pipe.

7.3.5.1 Finestra di dialogo Total Limit

Questa finestra di dialogo consente di specificare i limiti della larghezza di banda e del numero di pacchetti al secondo per ciascuna precedenza nel pipe, nonché per il totale del pipe. Le limitazioni della larghezza di banda sono definite in Kbps (kilobit per secondo).

Un campo vuoto rappresenta un valore illimitato.

The 'Limits' dialog box has a title bar with 'Limits' and a close button. The main area is titled 'Set Total Limits' and contains a table with three columns: 'Prec', 'Kbps', and 'Pps'. The rows are numbered 7 down to 0, plus a 'Total' row at the bottom. The 'Kbps' and 'Pps' columns have input fields. In row 4, 'Kbps' is 512 and 'Pps' is 1024. In row 3, 'Kbps' is 256 and 'Pps' is 512. The 'Total' row has 'Kbps' as 1024 and 'Pps' as 1024. There are 'OK' and 'Cancel' buttons at the bottom.

Prec	Kbps	Pps
7:		
6:		
5:		
4:	512	1024
3:	256	512
2:		
1:		
0:		
Total:	1024	1024

7.3.5.2 Finestra di dialogo User Limit

The 'Limits' dialog box has a title bar with 'Limits' and a close button. The main area is titled 'Set Per-User Limits' and contains a table with three columns: 'Prec', 'Kbps', and 'Pps'. The rows are numbered 7 down to 0, plus a 'Total' row at the bottom. The 'Kbps' and 'Pps' columns have input fields. In row 3, 'Kbps' is 64. The 'Total' row has 'Kbps' as 512 and 'Pps' as an empty field. There are 'OK' and 'Cancel' buttons at the bottom.

Prec	Kbps	Pps
7:		
6:		
5:		
4:		
3:	64	
2:		
1:		
0:		
Total:	512	

Questa finestra di dialogo consente di specificare i limiti della larghezza di banda di ciascun utente e del numero di pacchetti al secondo per ciascuna precedenza dell'utente, nonché per il totale della banda allocata all'utente. Le limitazioni della larghezza di banda sono definite in Kbps (kilobit per secondo).

Un campo vuoto rappresenta un valore illimitato.

Il valore 'user' viene controllato dalla colonna di raggruppamento.

7.3.6 Scheda Interfaces

	Name	Connect	IP Addr	Broadcast Addr	Comments
1	int	PCI SLOT 9 BUS 0	ip_int	br_int	Internal interface
2	ext	PCI SLOT 10 BUS 0	ip_ext	br_ext	External interface

La scheda Interfaces specifica le *interfacce* (schede di rete) installate nel firewall. Consente di configurare gli IRQ della scheda, i numeri degli slot e così via.



Se si utilizzano i driver ODI, invece di quelli integrati, e si modificano le impostazioni hardware di una o più schede di rete, le modifiche apportate non saranno effettive se si invia la configurazione al firewall tramite la rete. È necessario utilizzare i comandi **Create Boot Media** o **Save To Disk** del menu **FireWall**. Consultare il paragrafo 7.2.3.1, Menu FireWall/Advanced Menu FireWall/Advanced.

- **Name** – Specifica un nome simbolico per l'interfaccia. Questo nome è limitato a sette lettere e sarà utilizzato in molti altri punti della configurazione.
- **Connect** – Mostra un breve riepilogo della configurazione hardware relativa alla scheda di rete. Facendo clic su questa colonna si apre una finestra di dialogo che contiene le impostazioni sull'hardware. Consultare il paragrafo 6.4.4, Configurazione dell'interfaccia Configurazione dell'interfaccia.
- **IP Addr** – Indirizzo IP dell'interfaccia. Si tratta di indirizzi che possono essere utilizzati per eseguire il ping sul firewall e controllarlo da una postazione remota. Inoltre, vengono utilizzati come indirizzo di origine per le connessioni tradotte dinamicamente. Per simulare l'effetto di un'interfaccia che dispone di uno o più indirizzi IP, è possibile pubblicare tali indirizzi sull'interfaccia mediante ARP. Consultare il paragrafo 7.3.7, Scheda ARP.

- **Broadcast** – Gli indirizzi di broadcast della rete connessa. Questo è l'indirizzo più alto disponibile nella rete. Nel caso di una rete con 32 indirizzi, l'indirizzo di broadcast è l'indirizzo di rete +31; ad esempio, se la rete ha un indirizzo 192.168.123.64 255.255.255.224, il relativo broadcast è 192.168.123.95. All'indirizzo di broadcast vengono inviate le informazioni che devono raggiungere tutti i computer collegati alla rete.

7.3.7 Scheda ARP

	Mode	Iface	IP Address	Hw Address	Comments
1	Publish	ext	mailsrv-pub		
2	PUBLISH	ext	wwwsrv-pub		

La scheda ARP contiene gli indirizzi hardware per IP specifici su ciascuna interfaccia. Consente il binding statico di indirizzi IP verso indirizzi hardware e la pubblicazione di indirizzi IP con indirizzi hardware specifici.

- **Mode** – Static, Publish o XPublish.
- **Interface** – Indica l'interfaccia a cui si applica la voce ARP; ad esempio, l'interfaccia su cui deve essere pubblicato l'indirizzo.
- **IP Address** – L'indirizzo IP che deve essere pubblicato oppure connesso staticamente all'indirizzo hardware.
- **Hw Address** – L'indirizzo hardware associato all'indirizzo IP. Se si omette questo campo, viene utilizzato automaticamente l'indirizzo locale della scheda di rete.

7.3.7.1 Elementi ARP statici

Gli elementi ARP statici possono essere utili in situazioni in cui viene segnalato un indirizzo hardware per un dispositivo non valido in risposta a richieste ARP. Nei bridge delle workstation, quali modem via radio, si verificano tali problemi. Inoltre può essere utilizzato per bloccare un indirizzo IP verso un indirizzo hardware specifico in modo da aumentare la sicurezza o evitare effetti di negazione del servizio se vi sono utenti malintenzionati nella rete. Tuttavia, tale protezione si applica solo ai pacchetti che vengono inviati *a* quell'indirizzo IP, mentre non è valida per i pacchetti inviati *da* quell'indirizzo IP.

7.3.7.2 Elementi ARP pubblicati

La pubblicazione di un indirizzo IP mediante ARP può essere utile per due ragioni:

- Aiutare le apparecchiature di rete vicine che rispondono a richieste ARP in modo non corretto. Questo utilizzo è poco comune.
- Fornire l'impressione che ciascuna interfaccia del firewall abbia più di un indirizzo IP.

Per questo, il firewall fornisce le risposte alle richieste ARP relative agli indirizzi IP in elementi ARP pubblicati.

L'ultimo utilizzo risulta utile se esistono varie estensioni IP separate su una singola rete LAN. I computer presenti su ciascuna estensione IP possono quindi utilizzare un gateway nella propria estensione pubblicandolo sull'interfaccia del firewall.

Un altro campo di utilizzo è la pubblicazione di indirizzi multipli su un'interfaccia esterna, consentendo al firewall di inviare staticamente la comunicazione tradotta a tali indirizzi e poi inoltrarla ai server interni con indirizzi IP privati.

La differenza tra l'opzione XPublish e Publish è che la prima "mente" circa l'indirizzo del mittente nell'intestazione Ethernet; questa viene impostata per essere uguale all'indirizzo hardware pubblicato invece che all'indirizzo hardware effettivo della scheda di rete.



Se l'indirizzo hardware pubblicato è uguale a quello della scheda di rete, la scelta dell'opzione Publish o Xpublish è del tutto indifferente; i risultati saranno gli stessi.



Nella sezione ARP, gli indirizzi possono essere pubblicati solo uno alla volta. La sezione Routes dall'altra parte può gestire la pubblicazione di intere reti mediante Proxy ARP.

È possibile trovare esempi di elementi ARP pubblicati nella sezione 8.5, Esempi di configurazione.

7.3.8 Scheda Routes

	Iface	Net	Gateway	Local IP	ProxyARP	Comments
1	int	intnet				No gateway means that the network...
2	ext	extnet				firewall; interface addresses are ND...
3	ext	all-nets	gw-world			

La scheda Routes descrive la tabella di instradamento del firewall. EnterNet FireWall utilizza un modo diverso di descrivere i percorsi se paragonato ad altri sistemi. Tuttavia, si ritiene che tale modo di descrivere i percorsi sia più semplice da comprendere, evitando agli utenti di causare danni o violazioni della sicurezza.

- **Iface** – Specifica i pacchetti di interfaccia destinati a quel percorso che devono essere inviati.
- **Net** – Specifica l'indirizzo di rete per quel percorso. Come descritto in precedenza, è possibile utilizzare sia gli indirizzi numerici che i nomi di rete simbolici.
- **Gateway** – Specifica l'indirizzo IP dell'hop successivo del router utilizzato per raggiungere la rete di destinazione. Se la rete è connessa direttamente all'interfaccia del firewall, non viene specificato alcun indirizzo gateway.
- **Local IP** – L'indirizzo IP specificato qui sarà automaticamente pubblicato nell'interfaccia corrispondente. Questo indirizzo sarà utilizzato anche come indirizzo del mittente nelle richieste ARP. Se non viene specificato alcun indirizzo, sarà utilizzato l'indirizzo IP dell'interfaccia del firewall.

- **Proxy ARP** – Specifica l'interfaccia o le interfacce su cui il firewall deve pubblicare questo percorso mediante Proxy ARP.

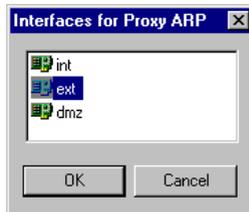
Uno dei vantaggi che si può ottenere con questa forma di annotazione consiste nel poter specificare un gateway per un particolare percorso, senza che un percorso copra necessariamente l'indirizzo IP del gateway oppure nonostante il percorso che copre l'indirizzo IP del gateway venga normalmente instradato mediante un'altra interfaccia.



La differenza tra questa forma di annotazione e quella più comunemente in uso sta nel fatto che non viene specificato il nome dell'interfaccia in una colonna separata. Al contrario, si specifica l'indirizzo IP di ciascuna interfaccia come un gateway.

7.3.8.1 Finestra di dialogo Proxy ARP

Questa finestra di dialogo specifica su quali interfacce sarà pubblicato il percorso corrente mediante Proxy ARP. Per selezionare più di un'interfaccia, tenere premuto il tasto Ctrl e fare clic sugli elementi inclusi nell'elenco.

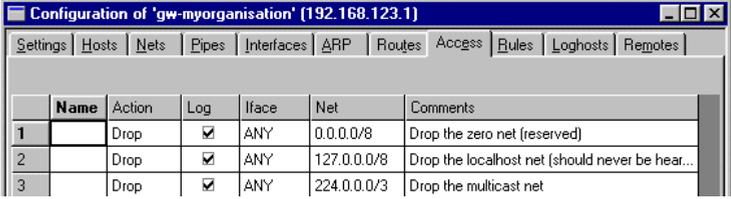


In breve, la funzione Proxy ARP ha le stesse funzionalità della pubblicazione di elementi ARP, che può essere eseguita nella sezione ARP.

La grande differenza consiste nel fatto che è possibile, in modo semplice e rapido, pubblicare contemporaneamente intere reti su una o più interfacce. Un'altra differenza, meno importante, è che il firewall pubblica sempre gli indirizzi come appartenenti al firewall stesso; perciò non è possibile pubblicare indirizzi che appartengono ad altri indirizzi hardware.

Per ulteriori informazioni sui casi in cui possono risultare utili le funzioni di pubblicazione Proxy ARP e ARP nonché sul loro funzionamento, consultare gli esempi di configurazione mediante Proxy ARP nella sezione 8.5, Esempi di configurazione.

7.3.9 Scheda Access



	Name	Action	Log	Iface	Net	Comments
1		Drop	<input checked="" type="checkbox"/>	ANY	0.0.0.0/8	Drop the zero net (reserved)
2		Drop	<input checked="" type="checkbox"/>	ANY	127.0.0.0/8	Drop the localhost net (should never be hear...
3		Drop	<input checked="" type="checkbox"/>	ANY	224.0.0.0/3	Drop the multicast net

Da un punto di vista teorico, le funzionalità della scheda Access possono essere utilizzate solo mediante la scheda Rules. Tuttavia, per semplificare l'amministrazione e ridurre il rischio di improvvise violazioni della sicurezza, EnterNet FireWall divide il set di regole in sue sezioni distinte.

La sezione Access controlla quali indirizzi IP che il firewall accetterà come indirizzi del mittente su ciascuna interfaccia. In altre parole, si tratta di una protezione contro lo spoofing IP.



La sezione Access *non* decide quali indirizzi del mittente saranno autorizzati a comunicare *attraverso* il firewall né tantomeno in quale modo potranno comunicare. Decide esclusivamente quali indirizzi del mittente sono validi per un'interfaccia specifica.

Il vantaggio di utilizzare la sezione Access consiste nel fatto che gli indirizzi ricevuti su un'interfaccia specifica della sezione Rules sono sempre corretti, a condizione che la sezione Access sia configurata correttamente.

Il set di regole della sezione Access confronta ciascun pacchetto ricevuto con le proprie regole, riga dopo riga, finché i valori non corrispondono ai parametri Iface e Net. Dopo aver trovato una regola corrispondente, viene eseguita l'azione.

- **Name** – Specifica un nome simbolico per la regola. Utilizzato principalmente come riferimento nei dati di log.
- **Action** – Accept, Expect o Drop. Vedere di seguito.
- **Log** – Specifica se e come viene eseguita la registrazione su una corrispondenza di regole.

- **Iface** – L'interfaccia che il pacchetto deve raggiungere affinché venga soddisfatta la regola. *Eccezione: la regola Expect, vedere di seguito.*
- **Iface** – L'estensione IP a cui deve appartenere il mittente affinché venga rispettata la regola.

Le seguenti regole si applicano a diversi tipi di azioni inclusi nella sezione Access:

- **Drop** – Se l'indirizzo del mittente del pacchetto corrisponde all'estensione IP specificata da questa regola e se l'interfaccia ricevente corrisponde a quella specificata da questa regola, il pacchetto viene scartato. La registrazione viene eseguita se è attivata nella colonna Log.
- **Accept** – Se l'indirizzo del mittente del pacchetto corrisponde all'estensione IP specificata da questa regola e se l'interfaccia ricevente corrisponde a quella specificata da questa regola, il pacchetto viene accettato per ulteriori ispezioni, ad esempio nella sezione Rules. La registrazione viene eseguita se è attivata nella colonna Log.
- **Expect** – Se l'indirizzo del mittente del pacchetto corrisponde all'estensione IP specificata da questa regola, l'interfaccia ricevente viene confrontata a quella specificata nella regola. Se l'interfaccia corrisponde, il pacchetto viene accettato in un modo simile all'azione Accept. Non viene eseguita alcuna registrazione. Se l'interfaccia *non* corrisponde, il pacchetto viene rilasciato nello stesso modo dell'azione Drop. La registrazione viene eseguita se è attivata nella colonna Log.

Per ulteriori informazioni sull'ordine in cui vengono esaminate le diverse regole e impostazioni, consultare il diagramma di flusso di EnterNet FireWall alla fine del capitolo 8.

7.3.10 Scheda Rules

	Name	Action	Pipes	Log	Src Iface	Source Net	Dest Iface	Dest Net	Proto	Ports/Params	Comments
1		Drop		<input type="checkbox"/>	ANY	all-nets	ANY	all-nets	UDP	ALL -> 137	Drop NetBIOS name
2		Drop		<input checked="" type="checkbox"/>	ANY	all-nets	ANY	all-nets	Ports	ALL -> 135-139	Drop and log all othe
3		Drop		<input checked="" type="checkbox"/>	ANY	all-nets	ANY	all-nets	Ports	ALL -> 445	Drop and log all NetE

La scheda Rules contiene la parte centrale di EnterNet FireWall: il set di regole.

In questa sezione, ciascun pacchetto ricevuto viene confrontato con le regole, riga dopo riga, finché i valori non trovano corrispondenza nei parametri Source Net, Dest Net, Protocol e Ports/Params. Dopo aver trovato una regola corrispondente, viene eseguita l'azione. *Eccezione: regole SAT. Vedere di seguito.*

- **Name** – Specifica un nome simbolico per la regola. Questo nome è utilizzato principalmente come riferimento nei dati di log e nelle statistiche.
- **Action** – Reject, Drop, FwdFast, Allow, NAT o SAT. Vedere di seguito per una descrizione dettagliata di ciascuna azione.
- **Pipes** – Specifica la catena di pipe per il passaggio del pacchetto e le precedenze da applicare al pacchetto stesso. Se non è specificato alcun pipe, il pacchetto viene semplicemente inviato a destinazione. Per le regole NAT e Allow, le catene di pipe possono essere specificate in entrambe le direzioni di invio e di ritorno. Per le regole FwdFast, può essere definita solo una catena di pipe nella direzione di invio.
- **Log** – Specifica se e come viene eseguita la registrazione su una corrispondenza di regole.
- **Src Iface** – Specifica il nome dell'interfaccia ricevente che deve essere confrontata con il pacchetto ricevuto. Perché venga eseguita la regola, i pacchetti da esaminare devono corrispondere a questo e a tutti gli altri filtri

- **Src Net** – Specifica il range di indirizzi IP del mittente che deve essere confrontato con il pacchetto ricevuto. I pacchetti da esaminare devono corrispondere a questo filtro e a tutti gli altri filtri perché sia avviata la regola.
- **Dest Iface** – Specifica il nome dell'interfaccia che deve essere confrontata con l'interfaccia di destinazione per l'IP di destinazione del pacchetto ricevuto. L'interfaccia di destinazione viene calcolata con una ricerca nel percorso prima dell'analisi del set di regole. Perché venga eseguita la regola, i pacchetti da esaminare devono corrispondere a questo e a tutti gli altri filtri.



Nota: poiché l'interfaccia di destinazione viene calcolata mediante una ricerca sul percorso *prima* che inizi il confronto con regole, questa *non* verrà influenzata dalle regole SAT o altre traduzioni di indirizzi.

- **Dest Net** – Specifica l'estensione il range di indirizzi IP che deve essere confrontato con l'IP di destinazione del pacchetto ricevuto. Perché venga eseguita la regola, i pacchetti da esaminare devono corrispondere a questo e a tutti gli altri filtri.
- **Proto** – Specifica il protocollo IP che deve essere confrontato con il pacchetto ricevuto. Esistono diversi nomi di protocollo predefiniti (vedere l'elenco di protocolli riportato di seguito), alcuni dei quali dispongono di ulteriori parametri di filtro nella colonna Ports/Params. I tipi di protocollo IP non elencati possono essere filtrati mediante il numero di protocollo numerico. Perché venga eseguita la regola, i pacchetti da esaminare devono corrispondere a questo e a tutti gli altri filtri.
- **Ports/Params** – Specifica i parametri aggiuntivi da confrontare con il pacchetto ricevuto. I parametri effettivi disponibili dipendono dal protocollo IP selezionato (vedere più avanti). Perché venga eseguita la regola, i pacchetti da esaminare devono corrispondere a questo e a tutti gli altri filtri.

7.3.10.1 Tipi di azione della sezione Rules

Drop

I pacchetti che soddisfano la regola Drop vengono scartati immediatamente. Tali pacchetti saranno registrati se la relativa funzione è stata attivata nella colonna Log.

Reject

Rifiuta i pacchetti allo stesso modo della funzione Drop. In aggiunta, il firewall invia un messaggio ICMP UNREACHABLE al mittente oppure, se il pacchetto rifiutato era di tipo TCP, un messaggio TCP RST.

FwdFast

I pacchetti che soddisfano le regole FwdFast vengono autorizzati immediatamente. Con queste regole, il firewall non ricorda le connessioni aperte e, di conseguenza, non *ispeziona lo stato* del traffico lasciato passare secondo le regole FwdFast. Ciò significa che deve essere attiva una regola corrispondente che consenta al traffico di ritorno, se richiesto, di passare attraverso il firewall. Se è stata attivata la funzione di registrazione nella colonna Log, verrà eseguito il log di tutti i pacchetti che passano in base alle regole FwdFast.

Le regole FwdFast sono influenzate anche dalla traduzione statica degli indirizzi specificata nelle regole SAT. Tuttavia, si tenga presente che in questo caso, devono essere attive le regole SAT per il ritorno del traffico, se richiesto.

Allow

I pacchetti che soddisfano le regole Allow vengono lasciati passare al motore di ricerca di ispezione dello stato, il quale ricorderà che una connessione è stata aperta. Quindi le regole per il ritorno del traffico non saranno richieste in quanto il traffico appartenente alle connessioni aperte viene automaticamente gestito prima che raggiunga il set di regole.

La registrazione viene eseguita se è stata attivata nella colonna Log. Ciò che viene registrato dipende dalle impostazioni **LogConnections** contenute nella sezione Settings. Consultare il paragrafo 7.3.2.5, , impostazioni stateful inspection.

NAT

Le regole NAT sono simili alle regole Allow. Queste regole eseguono una traduzione dinamica dell'indirizzo, NAT hide, relativa all'indirizzo del mittente.

L'utilizzo più comune della funzione NAT hide è quella di portare tutte le macchine presenti su una rete protetta ad essere visualizzate al mondo esterno come se utilizzassero un singolo indirizzo IP. Ciò può essere utile per ragioni di sicurezza, nascondendo la struttura interna della rete, oppure per motivi pratici, quali la possibilità di comunicare con le reti pubbliche per macchine con indirizzi privati.

SAT

Quando un pacchetto soddisfa una regola SAT, in realtà non succede nulla. Il firewall invece ricorda che la traduzione statica di un indirizzo sarà eseguita in fase successiva e continuerà a cercare una regola corrispondente che consenta il passaggio del pacchetto. Se il pacchetto soddisfa quindi una delle regole FwdFast, Allow o NAT, allora viene autorizzato a passare. Al contrario, se il pacchetto soddisfa una regola Drop o Reject, questo viene eliminato.

Il vantaggio consiste nel fatto che se, ad esempio, viene utilizzata una regola SAT per consentire il traffico verso un server in una zona demilitarizzata con un indirizzo privato, sarà ancora necessario effettuare una distinzione tra le connessioni originate internamente ed esternamente. Le connessioni originate esternamente vengono generalmente autorizzate da una regola Allow, mentre quelle originate internamente sono spesso autorizzate dalle regole NAT, in modo da nascondere la struttura interna della rete ai server nella zona demilitarizzata.

La registrazione della regola SAT viene eseguita solo se è stata attivata nella regola finale FwdFast, Allow o NAT.

7.3.10.2 Colonna Protocol

La colonna Protocol nella sezione Rules specifica a quale protocollo IP si applica la regola. Il protocollo scelto influisce sull'aspetto della finestra di dialogo Ports/Params che viene attivata facendo clic nella colonna accanto alla colonna Protocol.

Vengono definiti i seguenti protocolli IP:

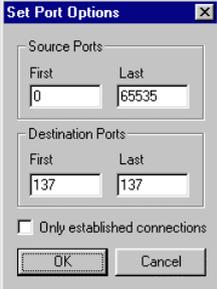
- **TCP** – Transmission Control Protocol. Consente il filtro sulle porte del mittente e della destinazione da 0 a 65535.
- **UDP** – User Datagram Protocol. Consente il filtro sulle porte del mittente e della destinazione da 0 a 65535.
- **ICMP** – Internet Control Message Protocol. Consente di filtrare i tipi di messaggio ICMP.
- **Standard** – TCP, UDP e ICMP. Non consente il filtro del tipo di porta o di messaggio; si applica a tutte le porte e tipi di messaggio.
- **GRE** – Generic Router Encapsulation. Non consente ulteriore filtro. GRE viene utilizzato dal protocollo PPTP per trasferire i dati nella propria connessione VPN.
- **IPIP** – IP-in-IP. Non consente ulteriore filtro. Utilizzato da CheckPoint VPN-1.
- **ESP** – IPsec Encapsulation Security Payload. Non consente ulteriore filtro. Utilizzato dal protocollo IPsec nei casi in cui sono crittografate le connessioni VPN.
- **AH** – IPsec Authentication Header. Non consente ulteriore filtro. Utilizzato dal protocollo IPsec nei casi in cui sono autenticate le connessioni VPN.
- **IPComp** – IPsec Data Compression. Non consente ulteriore filtro. Utilizzato dal protocollo IPsec quando le connessioni VPN sono compresse.
- **IPsec** – ESP e / o AH. Non consente ulteriore filtro.
- **SKIP** – Simple Key Management Protocol for Internet Protocols. Non consente ulteriore filtro. Il protocollo VPN è stato sviluppato originariamente da Sun Microsystems.

- **L2TP** – Layer 2 Tunneling Protocol. Non consente ulteriore filtro. Utilizzato da Microsoft Windows per forzare il tunneling di tutto il traffico attraverso il protocollo IPsec.
- **OSPF** – Open Shortest Path First. Non consente ulteriore filtro. Protocollo di instradamento utilizzato da vari router. Sostituisce il RIP.
- **IPProto**. Permette all'utente di definire il protocollo IP da utilizzare. Per un elenco dei protocolli IP definiti, consultare la sezione 11.1, Numeri di protocollo IP.
- **ALL** – Tutti i protocolli IP possibili da 0 a 255.

7.3.10.3 Finestra Port/Params - TCP, UDP e Ports

Se si sceglie l'opzione TCP, UDP o Ports viene visualizzata questa finestra di dialogo quando si fa clic sulla colonna Ports/Params.

Questa finestra di dialogo permette di impostare un intervallo di valori per le porte di origine e di destinazione. Notare che gli intervalli sono *complessivi*, nel senso che l'intervallo 137-139 copre le porte 137, 138 e 139.



Source Ports	
First	Last
0	65535

Destination Ports	
First	Last
137	137

Only established connections

OK Cancel

Affinché vi sia corrispondenza tra le porte esistenti, utilizzare i valori compresi tra 0 e 65535. Per garantire la compatibilità tra porte *assegnate dinamicamente*, utilizzare i valori compresi tra 1024 e 65535. Le porte dinamiche sono porte di origine normalmente utilizzate da un host client quando si apre una connessione verso un server.

Impostazione delle porte nelle regole FwdFast

La finestra di dialogo contiene anche una casella di controllo chiamata "Only established connesctions" per il protocollo TCP e le porte nelle regole FwdFast. Questa casella di controllo ha la stessa funzione del flag ESTABLISHED, presente in molti router con gli elenchi ACL (Access Control List). Se la casella è selezionata, il pacchetto TCP deve avere il flag SYN inattivo oppure, se questo è attivo, anche il flag ACK deve essere abilitato. Ciò significa che tale regola non si applica ai nuovi collegamenti effettuati mediante TCP. Non esiste alcuna protezione equivalente per pacchetti UDP o ICMP.

Impostazione delle porte nelle regole NAT e Allow

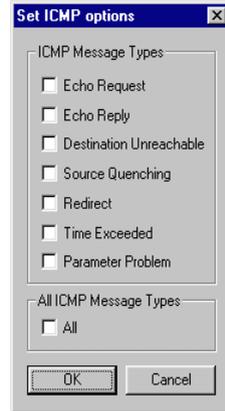
Per le impostazioni relative al protocollo TCP o alle porte nelle regole NAT e Allow, la finestra di dialogo mostrerà una casella di controllo "SYN flood protection". L'attivazione di questa funzione protegge gli *indirizzi di destinazione* dalla ridondanza SYN mediante un meccanismo chiamato "SYN Relay".

7.3.10.4 Finestra Ports/Params - ICMP

Se si sceglie il protocollo ICMP viene visualizzata questa finestra di dialogo quando si fa clic sulla colonna Ports/Params.

Questa finestra di dialogo permette di impostare i tipi di messaggi ICMP che un pacchetto può contenere per soddisfare una determinata regola.

Questo non vuole essere in alcun modo un elenco completo dei tipi di messaggi in ICMP. Selezionare la casella **All** significa applicare la regola a tutti i 256 tipi di messaggi possibili, cosa che naturalmente è ben diversa dal selezionare tutti i tipi di messaggi contenuti nell'elenco, uno alla volta.



ICMP Echo Request

Viene inviata una richiesta di eco quando si utilizza il comando Ping.

ICMP Echo Reply

Viene generalmente ricevuta una risposta di eco in seguito all'invio di un comando Ping.

ICMP Destination Unreachable

Tale messaggio può essere ricevuto in risposta all'invio di un comando Ping se il messaggio di richiesta di eco non ha raggiunto la destinazione stabilita; inoltre, può indicare che un collegamento TCP o UDP è stato interrotto oppure che non può essere stabilito.

ICMP Source Quenching

Questo messaggio segnala all'host che il peer ha incontrato problemi nel ricevere i dati alla velocità con cui l'host li ha trasmessi.

Molte implementazioni IP limitano le velocità di trasmissione per un periodo breve di tempo dopo avere ricevuto questo messaggio. Tuttavia, la funzione di avviso di congestione del traffico può essere utilizzata dai pirati informatici per diminuire la velocità di collegamento fra due parti. Per questo, il pirata informatico deve conoscere gli indirizzi IP di entrambe le parti. I messaggi di congestione del traffico sono utilizzati spesso da gruppi di modem per comunicare ai server su Internet di "rallentare" la trasmissione, quando il collegamento ai modem non riesce a supportare velocità molto elevate.

EnterNet FireWall ignora i messaggi Source Quenching se questi vengono inviati direttamente al firewall.

ICMP Redirect

Il reindirizzamento dei messaggi avviene quando una macchina sulla rete si accorge che il traffico verso un indirizzo dovrebbe invece essere diretto ad un altro. Questi messaggi non hanno alcun uso pratico oggi se non quello di permettere agli intrusi indesiderati di reindirizzare a sé stessi il traffico tra due parti. Questo tipo di messaggio non dovrebbe essere mai autorizzato all'interno di una rete protetta.

Poiché EnterNet FireWall non utilizza protocolli di instradamento quali RIP o OSPF, i messaggi di reindirizzamento possono rappresentare, in alcuni casi, un'indicazione che deve essere aggiunto un percorso alla tabella di instradamento. Può rivelarsi quindi utile la registrazione dei messaggi di reindirizzamento.



Nota: è sconsigliabile autorizzare il passaggio di messaggi ICMP Redirect su reti protette.

ICMP Time Exceeded

Questo messaggio segnala in genere che il contatore TTL (Time To Live) del pacchetto IP ha raggiunto il valore 0 e che quindi non sarà in grado di raggiungere la destinazione. Ciò può essere dovuto al fatto che l'impostazione della macchina relativa alla trasmissione del TTL sui pacchetti è troppo bassa; in Windows 95, i pacchetti vengono inviati con il TTL impostato in modo predefinito su 32, un valore medio che consente di raggiungere tutti i punti presenti in Internet.

Tuttavia, l'uso più comune del messaggio Time Exceeded è con il comando Traceroute. Questo comando invia un numero di pacchetti con vari TTL e registra gli indirizzi IP che rispondono con un messaggio Time Exceeded per ogni TTL. Ciò fornisce una panoramica generale del percorso effettuato da un pacchetto per raggiungere l'indirizzo di destinazione specifico.

ICMP Parameter Problem

Questi messaggi vengono inviati, benché molto raramente, in risposta ad alcuni pacchetti in cui, ad esempio, il destinatario ha avuto difficoltà nella comprensione di quello che il mittente desidera comunicare. Raramente questo messaggio adempie a qualche funzione e non dovrebbe rappresentare alcun pericolo per la sicurezza, considerando che la struttura esegue un test su ciascun pacchetto non appena passa attraverso EnterNet FireWall.

All

Selezionando la casella di controllo "All" nella finestra di dialogo vengono inclusi tutti i tipi di messaggi sopra elencati, compreso il messaggio Redirect, definito "pericoloso", e tutti i tipi di messaggio *sconosciuti*. Si sconsiglia di utilizzare l'impostazione All nelle regole FwdFast, NAT o Allow. Tuttavia, è una funzione molto utilizzata dalle regole Drop.

7.3.10.5 Finestra Ports/Params - IPProto

Se si seleziona l'opzione IPProto, viene visualizzata questa finestra di dialogo quando si fa clic sulla colonna Ports/Params.



Questa finestra di dialogo consente di scegliere il numero del protocollo IP che un pacchetto deve contenere per soddisfare una determinata regola.

Molti protocolli comuni vengono predefiniti nella colonna Protocol della scheda Rules, ma questa impostazione permette anche di filtrare i pacchetti con numeri di protocollo diversi.

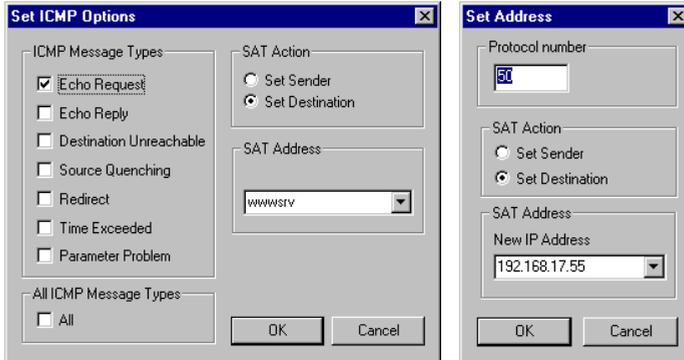
Per un elenco di numeri di protocolli predefiniti, consultare la sezione 11.1, Numeri di protocollo IP.



Se, ad esempio, si sceglie il protocollo IP numero 6, che corrisponde al TCP, la regola verrà applicata a *tutti* i pacchetti TCP, indipendentemente dal numero della porta. Sebbene non sia possibile applicare filtri più specifici al protocollo in questione, il firewall gestirà il protocollo proprio come se venisse filtrato da una normale regola TCP o Ports. In altre parole, tutti test di coerenza relativi a flag, opzioni, frammentazione e così via continueranno a funzionare.

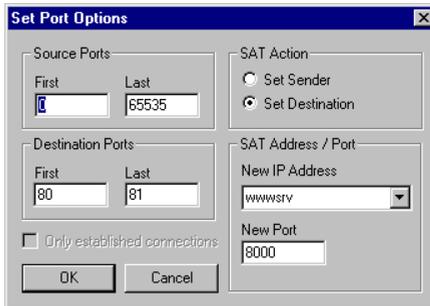
7.3.10.6 Finestra Ports/Params - Regole NAT/SAT

Le normali finestre di dialogo Ports/Params includono anche le impostazioni di traduzione dell'indirizzo, NAT e SAT.



ICMP con impostazioni per la traduzione statica dell'indirizzo.

IPProto con la traduzione statica dell'indirizzo.



TCP, UDP e Ports con impostazioni per la traduzione statica dell'indirizzo.

Le regole di traduzione statica dell'indirizzo includono sia gli indirizzi IP che le porte. L'esempio TCP illustrato sopra porterebbe la porta 80 ad essere mappata sulla porta 8000 come "wwwsrv" e la porta 81 a 8001.

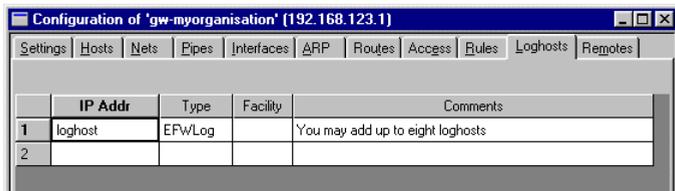
Per ulteriori informazioni consultare la sezione 8.1, Traduzione degli indirizzi.

Le regole per la traduzione degli indirizzi dinamici, NAT hide, sono leggermente diverse dalle regole SAT, nel fatto che la traduzione viene applicata solo all'indirizzo IP del mittente.



In genere EnterNet FireWall utilizza l'indirizzo dell'interfaccia che invia il pacchetto come indirizzo del mittente per collegamenti tradotti in modo dinamico, mediante l'opzione **Use Interface Address**. Tuttavia, è possibile anche specificare l'indirizzo del mittente scegliendo l'opzione **Specify Sender Address** e immettendo l'indirizzo del mittente richiesto.

7.3.11 Scheda Loghosts



	IP Addr	Type	Facility	Comments
1	loghost	EPWLog		You may add up to eight loghosts
2				

La scheda Loghosts contiene un elenco degli indirizzi IP in cui sono installati i destinatari della registrazione.

EnterNet FireWall v6.0 è in grado di inviare dati di log sia a EnterNet Firewall Loggers che ai destinatari di syslog. Possono essere specificati fino a otto loghost per ciascun firewall.

La registrazione avviene non appena si rileva una qualsiasi attività per tutti i destinatari specificati.

La procedura per la lettura dei file di log dipende dal tipo di loghost utilizzato. Per il FireWall Logger, vedere la sezione 9.2, EnterNet FireWall Logger. Lo stesso è valido anche per la lettura dei file syslog, in cui tutto dipende dal daemon syslog utilizzato: vedere la documentazione per il daemon syslog.

FireWall Manager fornisce anche un visualizzatore per i file di log in tempo reale. Questo visualizzatore mostra solo ciò che si è verificato dal momento che è stato attivato. EnterNet FireWall v5.1 e superiore consente di presentare molte più informazioni utilizzando questo visualizzatore rispetto alle versioni precedenti.



Il visualizzatore del file di log in tempo reale di FireWall Manager utilizza lo stesso collegamento remoto della console remota e la visualizzazione delle statistiche; di conseguenza, le workstation che utilizzano questo visualizzatore *non* necessitano di essere specificate nella sezione Loghosts.

7.3.12 Scheda Remotes

	Mode	Iface	Net	Comments
1	NetCon	int	intnet	Allow NetCon remote control access to all hosts on the inter...
2	Xfer	int	intnet	Also allow file transfer access...
3				

La scheda Remotes contiene un elenco di indirizzi IP a cui sono stati concessi i diritti per amministrare il firewall in modalità remota. Inoltre determina quali aspetti del firewall possono essere amministrati.

Notare che per amministrare il firewall in modalità remota non è sufficiente essere inclusi nell'elenco di indirizzi IP autorizzati. L'amministratore deve conoscere anche la chiave di crittografia a 128 bit memorizzata nel database di amministrazione.

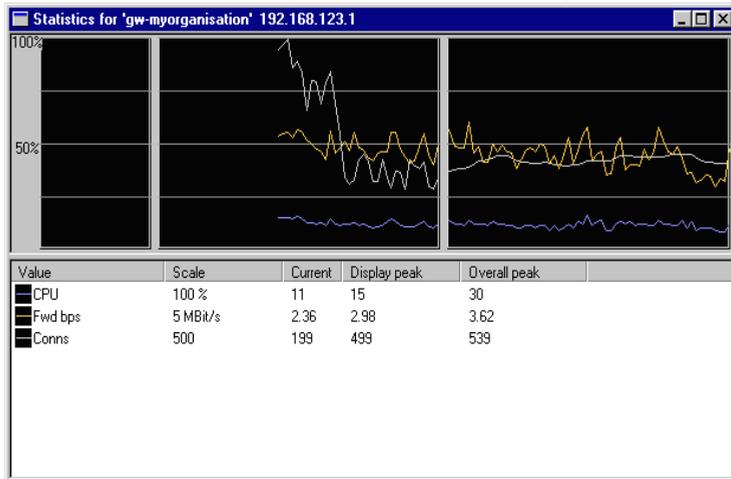


La scheda Remotes non consente di stabilire automaticamente una connessione tra la porta 999 TCP/UDP e il firewall. Tale comunicazione deve essere autorizzata anche dal set di regole.

- **Mode** - Determina le funzioni del firewall che possono essere amministrate. **NetCon** indica che è possibile collegarsi alla console del firewall tramite la rete. **Xfer** indica che è possibile trasferire i file di configurazione e aggiornare il software di EnterNet FireWall.
- **Interface** - Specifica l'interfaccia su cui devono essere ricevute le connessioni affinché vengano concessi i diritti di amministrazione remota.
- **Net** - Specifica un insieme di indirizzi IP a cui devono essere concessi i diritti di amministrazione remota per il firewall.

7.4 Visualizzazione delle statistiche

Scegliendo **Statistics** dal menu **FireWall** si accede alla visualizzazione delle statistiche, che mostra i vari aspetti del



La finestra mostra tre diagrammi uno accanto all'altro.

Il diagramma di destra visualizza le statistiche ogni secondo.

Il diagramma centrale mostra i valori medi ogni minuto.

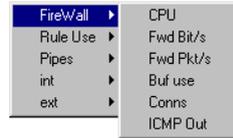
Il diagramma di sinistra mostra i valori medi ogni ora.

I grafici possono essere aggiunti alla visualizzazione delle statistiche selezionando il menu **Plot** oppure facendo clic con il pulsante destro sulla visualizzazione stessa che aprirà lo stesso menu.

Il menu **Plot** contiene il sottomenu **FireWall**, da cui è possibile accedere alle statistiche globali del firewall. Inoltre include altri sottomenu, i cui nomi variano in base alle interfacce del firewall, che contengono informazioni su ciascuna interfaccia specifica.

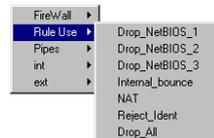
7.4.1 Statistiche relative al firewall

- **CPU** - Il carico percentuale sulla CPU del firewall.
- **Fwd Bit/s** - Numero di bit al secondo inviati attraverso il firewall.
- **Fwd Pkt/s** - Numero di pacchetti al secondo inviati attraverso il firewall.
- **Buf use** - Percentuale utilizzata dei buffer relativi al pacchetto del firewall.
- **Conns** - Numero di connessioni aperte mediante regole Allow o NAT. Nessun collegamento è aperto per il traffico autorizzato mediante le regole FwdFast; tale traffico non è incluso in questo grafico.
- **ICMP out** - Numero di pacchetti ICMP inviati dal firewall. Queste possono essere risposte Ping o pacchetti Destination Unreachable generati dal firewall in risposta a pacchetti a cui è stato negato l'accesso.



7.4.2 Statistiche di utilizzo per le regole

Il contatore sull'utilizzo di una regola specifica nella configurazione può essere attivato scegliendo la regola nel menu Rule Use.

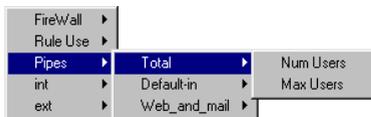


Per questo si consiglia di assegnare alle regole nomi simbolici descrittivi.

7.4.3 Statistiche sui pipe

Il sottomenu *Pipes* fornisce accesso a vari contatori per le statistiche relative alle funzioni di modellazione del traffico in EnterNet FireWall.

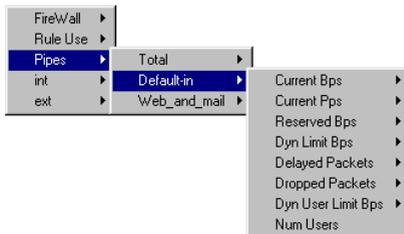
7.4.3.1 Statistiche globali sui pipe



- **Num Users** - Numero corrente di utenti, come definito dalle impostazioni di raggruppamento di ogni pipe, rilevato nei pipe. Notare che questo valore corrisponde al numero di utenti attivo per ogni porzione di tempo pari a 1/20° di secondo e non al numero di utenti che dispongono di connessioni "aperte".

7.4.3.2 Statistiche per pipe

- **Current Bps** - Velocità di trasmissione corrente del pipe, misurata in bit al secondo, per precedenza e come totale delle precedenze.



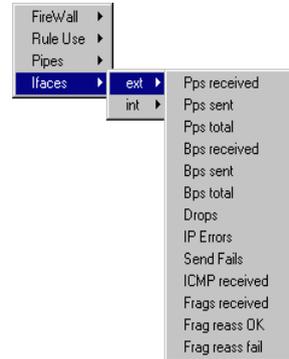
- **Current Pps** – Velocità di trasmissione corrente del pipe, misurata in bit al secondo, per precedenza e come totale delle precedenze.

- **Reserved Bps** - Larghezza di banda corrente assegnata ad ogni precedenza; alle precedenze inferiori non è permesso di utilizzare questa larghezza di banda. Notare che la larghezza di banda non viene riservata per precedenze con valore 0, alle quali è assegnato ciò che rimane del limite totale dopo aver sottratto tutte le prenotazioni di banda destinate alle precedenze più alte.

- **Dyn Limit Bps** - Limite corrente della larghezza di banda applicato alle rispettive precedenze. Si riferisce al grafico Reserved Bps, ma di solito è più alto, poiché mostra la larghezza di banda rimasta dopo aver sottratto le prenotazioni di banda per le precedenze più alte dal limite totale.
- **Delayed Packets** - Frequenza con cui i pacchetti sono stati ritardati a seguito dell'esaurimento della larghezza di banda assegnata da parte di un pipe, di una precedenza o di un utente di pipe. Notare che un singolo pacchetto può essere ritardato più volte; se un pipe è *realmente* pieno, il conteggio può superare il numero di pacchetti che attraversano effettivamente il pipe.
- **Dropped Packets** - Numero di pacchetti non elaborati. I pacchetti vengono scartati quando il software esaurisce i buffer dei pacchetti, evento che si verifica quando una quantità eccessiva di pacchetti vengono messi in coda per un invio successivo. Il pacchetto scartato è sempre quello che si trova in coda da più tempo; ciò significa che il collegamento in cui si verifica la perdita del pacchetto sarà quello che sovraccaricherà di più il sistema.
- **Dyn User Limit Bps** - Limite corrente della larghezza di banda per utente del pipe. Se il bilanciamento dinamico della larghezza è abilitato, questo valore può essere inferiore rispetto ai limiti configurati per ciascun utente.

7.4.4 Statistiche per ciascuna interfaccia

- **Counters Pps** - Numero di pacchetti ricevuti, inviati e sommati insieme.
- **Bps counters** - Numero di bit ricevuti, inviati e sommati insieme.
- **Drops** - Numero di pacchetti ricevuti da questa interfaccia che sono stati rilasciati su intervento del set di regole oppure in seguito a verifiche di coerenza dei pacchetti non riuscite.
- **IP Errors** - Numero di pacchetti ricevuti da questa interfaccia che sono stati così mutilati che avrebbero potuto difficilmente attraversare un router per arrivare al firewall, pur *non* essendo il risultato di un attacco.
- **Send Fails** - Numero di pacchetti non inviati, a causa di insufficienza di risorse interne dovuta ad un aumento del carico, a problemi hardware oppure a collegamenti half-duplex congestionati.
- **ICMP received** - Numero di datagrammi ICMP (ping, messaggi di errore) destinati all'indirizzo IP di questa interfaccia.
- **Fragrs received** - Numero di frammenti di pacchetto IP ricevuti da questa interfaccia.
- **Frag reass OK** - Numero di pacchetti completi che sono stati riassemblati dai frammenti ricevuti.
- **Frag reass fail** - Numero di pacchetti che non è stato possibile riassemblare a causa di insufficienza delle risorse, di frammentazione non corretta o di perdita del pacchetto.



8. EnterNet FireWall

Il presente capitolo fornisce una descrizione dettagliata sul funzionamento di EnterNet FireWall. Contiene esempi di configurazione da utilizzare per risolvere problemi e fornisce assistenza in situazioni più complesse.

Questo capitolo include inoltre una sezione di riferimento sui comandi per la console del firewall e un elenco del contenuto relativo ai supporti di avvio di EnterNet FireWall.

8.1 Traduzione degli indirizzi

EnterNet FireWall supporta due tipi di traduzione degli indirizzi: dinamica, "NAT hide"; statica, "NAT static". Questi due tipi sono rappresentati rispettivamente dalle regole NAT e SAT.

Esistono due ragioni principali per l'utilizzo della funzione di traduzione degli indirizzi:

- **Funzionalità.** Se si utilizzano indirizzi IP privati sulla rete protetta e gli host protetti hanno accesso a Internet, viene utilizzata la traduzione dinamica dell'indirizzo. Se si dispone di server con indirizzi IP privati che hanno bisogno di essere accessibili pubblicamente: viene utilizzata la traduzione statica dell'indirizzo.
 - **Sicurezza.** La traduzione degli indirizzi in sé non fornisce un livello maggiore di sicurezza, ma può rendere più difficile la comprensione dell'esatta disposizione della rete protetta e delle macchine che possono diventare bersaglio di un eventuale attacco da parte di intrusi indesiderati. Nel peggiore dei casi, l'uso della traduzione degli indirizzi rallenterà l'operato dell'intruso indesiderato, il quale sarà anche più visibile nei file di log del firewall. Nella migliore delle ipotesi, l'intruso si arrenderà.

In questa sezione viene descritta la traduzione degli indirizzi statica e dinamica nonché il funzionamento e le relative opzioni. Vengono inoltre forniti esempi relativi alle regole NAT e SAT.

8.1.1 Traduzione dinamica degli indirizzi di rete

Il processo di traduzione dinamica dell'indirizzo implica la traduzione di più indirizzi del mittente in un altro o altri indirizzi del mittente. Il funzionamento del processo viene descritto di seguito:

- Il mittente, ad esempio 192.168.1.5, invia un pacchetto da una porta assegnata dinamicamente, supponiamo la porta 1038, ad un server, ad esempio 195.55.66.77 su porta 80.
192.168.1.5:1038 → 195.55.66.77:80
- In genere, il firewall traduce l'indirizzo del mittente nell'indirizzo l'interfaccia più vicina all'indirizzo di destinazione. In questo esempio si utilizzerà 195.11.22.33. Inoltre, la porta di origine viene cambiata in una porta libera sul firewall, di solito un valore superiore a 32768. In questo esempio si utilizzerà la porta 32789. Il pacchetto è quindi inviato alla relativa destinazione.
195.11.22.33:32789 → 195.55.66.77:80
- Il server del destinatario elabora quindi il pacchetto e invia la risposta.
195.55.66.77:80 → 195.11.22.33:32789
- Il firewall riceve il pacchetto e lo confronta con l'elenco delle connessioni aperte. Una volta trovata la connessione in questione, il firewall *ripristina* l'indirizzo originale e invia il pacchetto.
195.55.66.77:80 → 192.168.1.5:1038
- Il mittente originale riceve la risposta.

8.1.2 Quali protocolli può elaborare la regola NAT Hide?

La traduzione dinamica dell'indirizzo è in grado di elaborare i protocolli TCP, UDP e ICMP con un buon livello di funzionalità poiché l'algoritmo conosce i valori che possono essere adattati per diventare univoci nei tre protocolli.

Per altri protocolli IP, le connessioni univoche vengono identificate dagli indirizzi del mittente, dagli indirizzi di destinazione e dai numeri di protocollo. Ciò significa che:

- Una macchina interna può comunicare con vari server esterni utilizzando lo stesso protocollo IP.
- Una macchina interna può comunicare con vari server esterni utilizzando diversi protocolli IP.
- Più macchine interne possono comunicare con vari server esterni utilizzando lo stesso protocollo IP.
- Più macchine interne possono comunicare con lo stesso server utilizzando diversi protocolli IP.
- Più macchine interne *non possono comunicare* con lo stesso server esterno utilizzando lo stesso protocollo IP.



Nota: queste restrizioni si applicano *solo* ai protocolli di livello IP diversi da TCP, UDP e ICMP, ad esempio OSPF, L2TP e così via. *Non* si applicano invece ai "protocolli" trasportati da TCP, UDP e ICMP quali Telnet, FTP, HTTP, SMTP e così via. Il firewall può modificare le informazioni sui numeri delle porte nelle intestazioni TCP e UDP per rendere univoca ciascuna connessione, anche se gli indirizzi del mittente di tali connessioni sono stati tradotti nello stesso IP.

Alcuni protocolli, indipendentemente dal metodo di trasporto utilizzato, possono causare problemi durante la traduzione dell'indirizzo. Sebbene non sia stato ancora redatto un elenco completo di questi protocolli, per avere un'idea di ciò che può causare tali problemi e per ottenere esempi dei protocolli inclusi, consultare il paragrafo 8.1.6 più avanti.

8.1.3 Perché NAT Hide modifica la porta di origine?

Ogni connessione originata da indirizzi tradotti dinamicamente deve utilizzare un numero di porta univoco e una combinazione di indirizzi IP uguali al relativo mittente. Se non viene utilizzata la traduzione dinamica dell'indirizzo, non ha importanza se due computer scelgono lo stesso numero di porta di origine in quanto i rispettivi indirizzi IP saranno diversi.

Tuttavia, quando è utilizzata la traduzione dinamica dell'indirizzo, le porte di origine rischiano di entrare in conflitto dato che tutti gli indirizzi del mittente saranno gli stessi. Di conseguenza, la porta di origine deve essere modificata.

8.1.4 Traduzione di intervalli di indirizzi e di porte

EnterNet FireWall può tradurre intervalli di indirizzi IP e/o porte. Tali traduzioni sono *trasposizioni*, vale a dire che ogni indirizzo o porta viene mappata su un indirizzo o porta corrispondente nel nuovo intervallo, piuttosto che tradurli tutti con lo stesso indirizzo o porta.

SAT	ANY	all-nets	194.1.2.16/28	TCP	ALL → 80 SetDest 192.168.0.50 80
-----	-----	----------	---------------	-----	-------------------------------------

Questa regola genera una traduzione 1:1 di tutti gli indirizzi nell'intervallo 194.1.2.16-194.1.2.31 all'intervallo 192.168.0.50-192.168.0.65.

Tutti i tentativi di connessione all'indirizzo 194.1.2.16, porta 80, avranno come risultato la connessione all'indirizzo 192.168.0.50.

Tutti i tentativi di connessione all'indirizzo 194.1.2.24, porta 80, avranno come risultato la connessione all'indirizzo 192.168.0.58.

SAT	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80—85 SetDest wwwsrv-priv 1080
-----	-----	----------	---------------	-----	---

Questa regola genera una traduzione 1:1 di tutte le porte dell'intervallo 80-85 all'intervallo 1080-1085.

I tentativi di comunicazione con l'indirizzo pubblico del server Web, porta 80, comporteranno la connessione all'indirizzo privato del server Web, porta 1080.

I tentativi di comunicazione con l'indirizzo pubblico del server Web, porta 84, comporteranno la connessione all'indirizzo privato del server Web, porta 1084.

8.1.5 Quale delle regole SAT viene eseguita se il firewall trova più corrispondenze?

EnterNet FireWall non termina la consultazione del set di regole dopo aver trovato una regola SAT che soddisfa i requisiti. Continua a cercare una regola Allow, NAT o FwdFast corrispondente. Solo dopo aver trovato una regola corrispondente, il firewall esegue la traduzione statica dell'indirizzo.

Nonostante ciò, *la prima regola SAT corrispondente trovata per ogni indirizzo è proprio quella che verrà eseguita.*

Per "ogni indirizzo" si intende che *due* regole SAT possono essere applicate contemporaneamente alla stessa connessione, a condizione che una traduca l'indirizzo del mittente mentre l'altra traduca l'indirizzo di destinazione.

SAT	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80—85 SetDest wwwsrv-priv 1080
SAT	int	intnet	all-nets	Std	SetSrc pubnet

Le due regole sopra citate possono essere eseguite simultaneamente sullo stesso collegamento. In questo esempio, gli indirizzi del mittente interni saranno tradotti in indirizzi del "pubnet" con una relazione 1:1. Inoltre, se qualcuno prova a collegarsi all'indirizzo pubblico del server Web, l'indirizzo di destinazione verrà cambiato nel relativo indirizzo privato.

SAT	int	intnet	wwwsrv-pub/32	TCP	ALL → 80—85 SetDest intrasrv 80
SAT	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80—85 SetDest wwwsrv-priv 1080

In questo esempio, entrambe le regole sono impostate per tradurre l'indirizzo di destinazione, ma solo una di esse sarà eseguita. Se si tenta di comunicare internamente con l'indirizzo pubblico del server Web, la richiesta sarà reindirizzata a un server intranet. Tutti gli altri tentativi di comunicazione con l'indirizzo pubblico del server Web verranno reindirizzati all'indirizzo privato del server Web accessibile pubblicamente.



Notare che, per funzionare correttamente, le regole sopra citate devono soddisfare una regola Allow in un punto successivo del set di regole.

8.1.6 Quali protocolli possono essere gestiti dalla funzione SAT?

In genere, la traduzione statica dell'indirizzo può gestire tutti i protocolli che supportano tale funzione. Infatti, alcuni protocolli possono essere tradotti solo in casi specifici mentre altri non possono essere tradotti in alcun modo.

I protocolli che non possono essere tradotti mediante la funzione SAT sono probabilmente in traducibili anche mediante le regola NAT, per i seguenti motivi:

- Il protocollo richiede crittograficamente che gli indirizzi rimangano inalterati; questo si applica a molti protocolli VPN.
- Il protocollo inserisce gli indirizzi IP all'interno dei dati di livello TCP o UDP e richiede, successivamente, che gli indirizzi visibili a livello IP siano gli stessi di quelli inseriti nei dati. Alcuni esempi includono FTP e gli accessi ai domini NT mediante NetBIOS.
- Entrambe le parti tentano di aprire una nuova connessione dinamica verso gli indirizzi visibili a quella parte. In alcuni casi questo può essere risolto modificando l'applicazione o la configurazione del firewall.

Non esiste un elenco definitivo dei protocolli che supportano la traduzione degli indirizzi. Generalmente i protocolli VPN non possono essere tradotti. Inoltre, può risultare difficile tradurre i protocolli che aprono collegamenti secondari oltre al collegamento iniziale.

Alcuni protocolli su cui è difficile eseguire la traduzione degli indirizzi possono essere gestiti da algoritmi sviluppati specificatamente per leggere e/o modificare i dati dell'applicazione. Questi vengono comunemente chiamati Application Layer Gateways oppure Application Layer Filters.

8.1.7 Esempi di traduzione degli indirizzi

Questa sezione evidenzia alcuni esempi di traduzione statica e dinamica degli indirizzi:

8.1.7.1 Server pubblicamente accessibile con un indirizzo privato in un'area DMZ

Il seguente esempio descrive un server Web con un indirizzo privato situato in un'area DMZ.

Per consentire agli utenti esterni di accedere al server Web, questo deve essere raggiungibile da un indirizzo pubblico. Si è scelto di tradurre la porta 80 sull'indirizzo esterno del firewall nella porta 80 del server Web:

1	SAT	ANY	All-nets	ip_ext/32	All → 80 SetDest wwwsrv 80
2	Allow	ANY	All-nets	ip_ext/32	All → 80

Queste due regole consentono di accedere al server Web tramite l'indirizzo IP esterno del firewall. Con la regola 1 viene stabilito che la traduzione dell'indirizzo può avvenire se è stata autorizzata la connessione, mentre la regola 2 consente la connessione.

Naturalmente, è necessaria una regola che consenta la traduzione dinamica degli indirizzi delle macchine interne per accedere a Internet. In questo esempio viene utilizzata una regola che consente a tutti gli elementi della rete interna di accedere a Internet tramite NAT Hide.

3	NAT	int	Intnet	all-nets	All → All
---	-----	-----	--------	----------	-----------

Dove si trova l'errore nel set di regole?

Supponendo di volere eseguire la traduzione dell'indirizzo per ragioni di sicurezza e di funzionalità, si scopre che questo set di regole rende visibili gli indirizzi interni alle macchine nella zona demilitarizzata. Quando le macchine interne si collegano a ip_ext port 80, verranno autorizzate a procedere in base alla regola 2 in quanto soddisfa i requisiti per quella comunicazione.

Da una prospettiva interna, tutte le macchine nella zona demilitarizzata devono essere considerate come un qualsiasi altro server collegato a Internet; questa è la ragione per cui all'inizio tali macchine vengono collocate in una zona demilitarizzata.

Esistono due soluzioni possibili:

1. Cambiare la regola 2 in modo che venga applicata solo al traffico esterno.
2. Sostituire la regola 2 con la 3 in modo che la regola NAT venga eseguita per il traffico interno prima che sia applicata la regola Allow.

Quale di queste due opzioni è la migliore?

Per questo tipo di configurazione è del tutto indifferente. Entrambe le soluzioni funzionano benissimo.

Tuttavia, si supponga di aggiungere un'altra interfaccia al firewall e di collegarla a un'altra rete, ad esempio quella di una filiale, in modo tale da poter comunicare più rapidamente con i server centrali. Questa viene definita l'interfaccia ext2.

Se è stata selezionata l'opzione 1, è necessario adeguare il set di regole come segue:

1	SAT	ANY	all-nets	ip_ext/32	All → 80 SetDest wwwsrv 80
2	Allow	ext	all-nets	ip_ext/32	All → 80
3	Allow	ext2	ext2net	ip_ext/32	All → 80
4	NAT	int	intnet	all-nets	All → All

Questo aumenta il numero di regole per ciascuna interfaccia a cui è permesso comunicare con il server Web. Tuttavia, essendo l'ordine delle regole insignificante, non è possibile commettere errori.

Se è stata selezionata l'opzione 2, è necessario adeguare il set di regole come segue:

1	SAT	ANY	all-nets	ip_ext/32	All → 80 SetDest wwwsrv 80
2	NAT	int	intnet	all-nets	All → All
3	Allow	ANY	all-nets	ip_ext/32	All → 80

Questo significa che il numero di regole non ha bisogno di essere aumentato. Ciò può andare bene finché si conoscono tutte le interfacce che comunicano con il server Web. Tuttavia, se in un punto successivo viene aggiunta un'interfaccia di comunicazione con il server Web di cui *non* si ha fiducia, le singole regole Drop dovrebbero essere collocate *prima* della regola che autorizza l'accesso di tutte le macchine al server Web.

La scelta della migliore azione da intraprendere deve avvenire caso per caso, prendendo in considerazione tutte le possibili circostanze.

8.1.7.2 Server accessibile pubblicamente con un indirizzo privato su una rete interna

L'esempio riportato di seguito è quello di un server Web con un indirizzo privato ubicato su una rete interna. Dal punto di vista della sicurezza, questo approccio non è corretto, poiché i server Web sono molto vulnerabili e dovrebbero essere quindi situati in una zona demilitarizzata. Tuttavia, si è scelto di utilizzare questo modello nel nostro esempio per la sua semplicità.

Affinché gli utenti esterni accedano al server Web, è necessario contattarlo utilizzando un indirizzo pubblico. Nell'esempio, si è scelto di tradurre la porta 80 sull'indirizzo esterno del firewall nella porta 80 del server Web:

1	SAT	ANY	all-nets	ip_ext/32	All → 80 SetDest wwwsrv 80
2	Allow	ANY	all-nets	ip_ext/32	All → 80

Queste due regole consentono di accedere al server Web tramite l'indirizzo IP esterno del firewall. Con la regola 1 viene stabilito che la traduzione dell'indirizzo può avvenire se è stata autorizzata la connessione, mentre la regola 2 consente la connessione.

Naturalmente, è necessaria una regola che consenta la traduzione dinamica degli indirizzi delle macchine interne per accedere a Internet. In questo esempio viene utilizzata una regola che consente a tutti gli elementi della rete interna di accedere a Internet tramite NAT Hide.

3	NAT	int	intnet	all-nets	All → All
---	-----	-----	--------	----------	-----------

Questo set di regole *non funzionerà per il traffico dalla rete interna.*

Per mostrare precisamente la successione degli eventi, saranno utilizzati i seguenti indirizzi IP:

ip_ext 195.55.66.77 – indirizzo IP pubblico
ip_int 10.0.0.1 – indirizzo IP privato e interno del firewall
wwwsrv 10.0.0.2 – indirizzo IP privato del server Web
pc1 10.0.0.3 – computer con un indirizzo IP privato

- Il PC1 invia un pacchetto a ip_ext per raggiungere "www.ourcompany.com":
10.0.0.3:1038 → 195.55.66.77:80
- Il firewall traduce l'indirizzo in base alla regola 1 e inoltra il pacchetto in base alla regola 2:
10.0.0.3:1038 → 10.0.0.2:80
- Wwwwsrv elabora il pacchetto e risponde:
10.0.0.2:80 → 10.0.0.3:1038

Questa risposta arriva direttamente al PC1 senza attraversare il firewall. Ciò può causare alcuni problemi. La ragione per cui non funzionerà risiede nel fatto che il PC1 attende una risposta da 195.55.66.77:80 e *non* da 10.0.0.2:80. La risposta inattesa viene eliminata e il PC1 continua ad attendere una risposta da 195.55.66.77:80, che non arriverà mai.

Con una piccola modifica al set di regole come descritto nel paragrafo 8.1.7.1, si potrà risolvere il problema. In questo esempio, senza una ragione particolare, si è scelto di utilizzare l'opzione 2:

1	SAT	ANY	all-nets	ip_ext/32	All → 80 SetDest wwwsrv 80
2	NAT	int	intnet	all-nets	All → All
3	Allow	ANY	all-nets	ip_ext/32	All → 80

- Il PC1 invia un pacchetto a ip_ext per raggiungere "www.ourcompany.com":
10.0.0.3:1038 → 195.55.66.77:80
- L'indirizzo del firewall esegue la traduzione statica in base alla regola 1 mentre quella dinamica in base alla regola 2:
10.0.0.1:32789 → 10.0.0.2:80
- Wwsvr elabora il pacchetto e risponde:
10.0.0.2:80 → 10.0.0.1:32789
- La risposta arriva al firewall e vengono ripristinate entrambe le traduzioni dell'indirizzo:
195.55.66.77:80 → 10.0.0.3:1038

In questo modo, la risposta arriva al PC1 dall'indirizzo previsto.

Un'altra possibile soluzione a questo problema consiste nel permettere ai client interni di comunicare direttamente con 10.0.0.2, in modo da evitare completamente tutti i problemi associati alla traduzione dell'indirizzo. Tuttavia, tale soluzione non è sempre pratica.

8.1.7.3 Regole SAT e FwdFast

È possibile utilizzare la traduzione statica dell'indirizzo insieme alle regole FwdFast, sebbene il traffico di ritorno debba essere esplicitamente autorizzato e tradotto.

Le seguenti regole descrivono un esempio funzionante di traduzione statica dell'indirizzo mediante le regole FwdFast per un server Web ubicato su una rete interna:

1	SAT	ANY	all-nets	ip_ext/32	All → 80 SetDest wwsvr 80
2	SAT	int	wwsvr/32	all-nets	80 → All SetSrc ip_ext 80
3	FwdFast	ANY	all-nets	ip_ext/32	All → 80
4	FwdFast	int	wwsvr/32	all-nets	80 → All

Viene aggiunta una regola NAT per autorizzare le connessioni dalla rete interna a Internet.

5	NAT	int	intnet	all-nets	All → All
---	-----	-----	--------	----------	-----------

Conseguenze:

- Il traffico esterno verso ip_ext:80 che soddisfa le regole 1 e 3 verrà quindi inviato a wwwsrv. Corretto.
- Il traffico di ritorno sarà automaticamente gestito dal meccanismo di stateful inspection del firewall.
- Il traffico interno verso ip_ext:80 che soddisfa le regole 1 e 3 verrà quindi inviato a wwwsrv. Quasi corretto: i pacchetti arriveranno a wwwsrv.
- Il traffico di ritorno da wwwsrv: 80 alle macchine interne verrà inviato direttamente alle macchine stesse. Questo non funzionerà in quanto i pacchetti saranno interpretati come provenienti dall'indirizzo sbagliato.

Ora si proverà a spostare la regola NAT fra le regole SAT e FwdFast:

1	SAT	ANY	all-nets	ip_ext/32	All → 80 SetDest wwwsrv 80
2	SAT	int	wwwsrv/32	all-nets	80 → All SetSrc ip_ext 80
3	NAT	int	intnet	all-nets	All → All
4	FwdFast	ANY	all-nets	ip_ext/32	All → 80
5	FwdFast	int	wwwsrv/32	all-nets	80 → All

Conseguenze

- Il traffico esterno verso ip_ext:80 che soddisfa le regole 1 e 4 verrà quindi inviato a wwwsrv. Corretto.
- Il traffico di ritorno da wwwsrv: 80 soddisfa le regole 2 e 3. Sulle risposte verrà quindi eseguita la traduzione dinamica dell'indirizzo. Ciò modificherà la porta di origine in una porta completamente diversa, che non funzionerà.

Il problema può essere risolto utilizzando il seguente set di regole:

1	SAT	ANY	all-nets	ip_ext/32	All → 80 SetDest wwwsrv 80
2	SAT	int	wwwsrv/32	all-nets	80 → All SetSrc ip_ext 80
3	FwdFast	int	wwwsrv/32	all-nets	80 → All
4	NAT	int	intnet	all-nets	All → All

5	FwdFast	ANY	all-nets	ip_ext/32	All → 80
---	---------	-----	----------	-----------	----------

- Il traffico esterno verso ip_ext:80 che soddisfa le regole 1 e 5 verrà quindi inviato a wwsvr. Corretto.
- Il traffico di ritorno da wwsvr: 80 soddisfa le regole 2 e 3. Corretto.
- Il traffico interno verso ip_ext:80 che soddisfa le regole 1 e 4 verrà quindi inviato a wwsvr. L'indirizzo del mittente sarà l'indirizzo IP interno del firewall in modo da garantire che il traffico di ritorno passi attraverso il firewall.
 - Il traffico di ritorno sarà automaticamente gestito dal meccanismo di ispezione sullo stato del firewall. Corretto.

8.2 Console del firewall

La console di EnterNet FireWall è un'interfaccia a riga di comando. Consente un'analisi dettagliata dei diversi aspetti statistici del firewall nonché una diagnostica avanzata.

Gli amministratori che dispongono dei diritti "NetCon" possono utilizzare questa console mediante la rete utilizzando EnterNet FireWall

Manager

```

EnterNet FireWall 6.00.00 : Below: 'pps.mbps', per interface
2500.11.5 600.36.0 3500.20.5
CPU: 8% ; Bufrs: 2% ; Conns: 3% ; Frags: 0% ; Drops: 5 ; LogMsgs: 4
EnterNet FireWall 6.00.00
Copyright EnterNet Sweden 1996-2001. All rights reserved.
Build : Jan 26 2001
Reading previous random state from efwand.bin...OK
Configuring from A:\FIREWALL\FWCore.CFG
Configuration done
NetCon initialization complete
Memory: Buffer size is 2084 bytes, 1992 bytes raw data
Memory: Using a total of 180 packet buffers (375120 bytes)
Interfaces:
0 : int IPAddr 10.20.250.2 HwAddr 00c0:df50:51d1
Packet driver 0x60 Handles: 0x01fa 0x0208
1 : ext IPAddr 10.20.0.1 HwAddr 0010:a060:77fd
Packet driver 0x65 Handles: 0x01fa 0x0208
1 : dmz IPAddr 192.168.234.1 HwAddr 0010:a060:77e9
Packet driver 0x69 Handles: 0x01fa 0x0208
Activating attached hub ports...
Previous shutdown: 2001-01-25 06:00:00: Shutdown due to console command
System running

```

8.2.1 Barra di stato della console

La prima riga di stato mostra le informazioni sul numero di pacchetti e di bit al secondo che attraversano ciascuna interfaccia. I numeri forniti in questo esempio mostrano che:

- Nell'interfaccia interna stanno passando:
2500 pacchetti al secondo
15.5 Megabit al secondo
- Nell'interfaccia esterna stanno passando:
6000 pacchetti al secondo
36 Megabit al secondo
- Nell'interfaccia DMZ stanno passando:
3500 pacchetti al secondo
30,5 Megabit al secondo



Questi numeri includono il totale dei dati inviati e ricevuti da ciascuna interfaccia. Questa riga di stato può visualizzare un massimo di otto interfacce.

La seconda riga di stato fornisce le seguenti informazioni:

- **CPU** – Percentuale del carico relativa alla CPU del firewall.
- **Bufs** – Percentuale di utilizzo dei buffer per i pacchetti disponibili. Il numero totale di buffer per i pacchetti viene visualizzato nel comando `stats`.
- **Conns** – Percentuale di utilizzo delle connessioni disponibili. Il numero massimo di connessioni è determinato dalla sezione `Settings`. La configurazione predefinita imposta un limite di 4096 connessioni contemporanee. Ogni connessione consuma 128 byte di RAM. Per vedere la quantità effettiva di RAM utilizzata dalla tabella di stato, vedere il comando di console **memory**, più avanti.
- **Frag** – Percentuale di utilizzo delle risorse di riassettaggio disponibili. EnterNet FireWall limita il numero di tentativi di riassettaggio dei frammenti che possono essere eseguiti contemporaneamente. La versione 6.0 imposta questo limite a 1024 tentativi simultanei.

- **Drops** - Numero di pacchetti scartati in seguito a test strutturali non riusciti o all'eliminazione da parte del set di regole nel secondo precedente.
- **LogMsgs** - Numero di messaggi di log generati durante il secondo precedente. EnterNet FireWall è in grado di limitare il numero di messaggi di log che possono essere generati ogni secondo mediante l'impostazione LogSendPerSecLimit nella sezione Settings.

8.2.2 Comandi della console

Di seguito viene riportato un elenco di tutti i comandi accessibili attraverso la console del firewall. Tali comandi possono essere abbreviati immettendo il testo incluso all'interno delle virgolette dopo ciascun comando. Sulla console è disponibile una Guida in linea che può essere richiamata mediante il comando "help".

About, "ab"

Apri una finestra contenente le informazioni che si riferiscono alla versione del software del firewall in uso e alle note sul copyright.

Access, "ac"

Visualizza il contenuto della sezione di configurazione Access.

ARP, "a"

Sintassi: arp [options] <interface pattern>

Opzioni: -ip <ip address pattern>
[] - hw <hw indirizzano pattern>
[] - num <n>

Esempi: arp int
arp-ip 10.*.1 dmz*

Visualizza le voci ARP per l'interfaccia specificata. Vengono mostrati gli elementi pubblicati, statici e dinamici.

ARPSnoop, "arps"

Consente di passare alla visualizzazione a video delle query ARP. Questo comando può essere di grande aiuto nella configurazione hardware del firewall, poiché mostra gli indirizzi IP identificati su ogni interfaccia.

```
> arpsnoop all
ARP snooping active on interfaces: int ext dmz
ARP su ext: gw-world requesting ip_ext
ARP on int: 192.168.123.5 requesting ip_int
```

Buffers, "b"

Questo comando può essere utile nella risoluzione dei problemi, ad esempio, quando un elevato numero di pacchetti non previsto inizia a mettersi in coda nel firewall oppure quando il traffico non sembra scorrere in modo corretto per qualche ragione inspiegabile. Analizzando il contenuto dei buffer, è possibile determinare se tale traffico raggiunge il firewall.

Sintassi: `buffers`

Apri un elenco degli ultimi buffer liberati.

Sintassi: `buffer <number>`

Mostra il contenuto del buffer specifico.

Sintassi: `buffer . (punto)`

Mostra il contenuto dell'ultimo buffer utilizzato.

CfgLog, "cfl"

Mostra i risultati dell'ultima riconfigurazione o dell'ultimo avvio di EnterNet FireWall. Il testo è uguale a quello visualizzato a video durante la riconfigurazione o l'avvio.

Connections, "conn"

Mostra le ultime 20 connessioni aperte per il firewall. Le connessioni vengono create quando il traffico è autorizzato mediante le regole Allow o NAT. Il traffico autorizzato a passare in base alle regole FwdFast non è incluso in questo elenco.

```
> conn
State      Prot Source                Destination      Time
TCP_OPEN   TCP  ext:60.20.37.6:5432  dmz:wwsrv:80  3600
SYN_RECV   TCP  ext:60.20.37.6:5433  dmz:wwsrv:80  30
UDP_OPEN   UDP  int:10.5.3.2:5433    dmz:dnsrv:53  50
```

Ciascuna connessione dispone di due valori di timeout, uno su ogni direzione. Questi valori vengono aggiornati quando il firewall riceve i pacchetti da ciascuna delle due estremità della connessione. Il valore mostrato nella colonna Timeout è quello inferiore.

I valori possibili nella colonna State includono:

SYN_RECV	Pacchetto TCP con flag SYN ricevuto
SYNACK_S	Pacchetto TCP con flag SYN + ACK inviato
ACK_RECV	Pacchetto TCP con flag ACK ricevuto
TCP_OPEN	Pacchetto TCP con flag ACK inviato
FIN_RECV	Pacchetto TCP con flag FIN/RST ricevuto
PING	Collegamento ICMP ECHO
UDP	Collegamento UDP
RAWIP	Collegamento che utilizza un protocollo IP diverso da TCP, da UDP o ICMP.

Cpuid, "cpu"

Mostra le informazioni sulla CPU nell'hardware del firewall.

Frag, "frag"

Mostra gli ultimi 20 tentativi di riassettaggio dei frammenti. Include i tentativi in corso e quelli già completati.

```
> frags
RecvIf  Num  State  Source      Destination  Proto  Next  Timeout
int     2    Done   10.5.3.2    206.23.98.4 ICMP    2000  58
ext     8    Accep  203.3.98    10.5.3.2    ICMP    1480  60
```

Hosts, "hos"

Mostra il contenuto della sezione Hosts nella configurazione.

IfStat, "i"

Sintassi: ifstat

Mostra un elenco delle interfacce installate nel firewall.

Sintassi: ifstat <interface_name>

Mostra le statistiche hardware e software per il NIC specifico.

```
> ifstat int
Iface 0: int
  Builtin "3c509" - 3Com 3c905B-TX Slot 10/0 IRQ 11
  Flags          : full-duplex, polled
  Media          : "Autonegotiate"
  Link Partner   : 100BASE-X, 100BASE-X FDX
  IP Address     : 192.168.123.1
  Hw Address     : 0010:4bb2:9ef7

Software Statistics:
  Soft received : 5  Soft sent      : 6  Net congested : 0
  Send errors   : 0  Dropped      : 2  Wrong IP ver  : 0
  IP Input Errs : 0  ICMPRedirects : 0

Hardware statistics:
  IN : packets= 20  bytes= 5000  errors= 0  dropped= 0
  OUT: packets= 28  bytes= 1680  errors= 0  dropped= 0
  Multicast packets      : 0
  Collisions             : 0
  In  : Length errors    : 0
  In  : Buffer overruns   : 0
  In  : CRC errors       : 0
  In  : Frame errors     : 0
  In  : FIFO errors     : 0
  In  : Packets missed   : 0
  Out : Sends aborted    : 0
  Out : Carrier errors   : 0
  Out : FIFO errors     : 0
  Out : Heartbeat errors : 0
  Out : Window errors    : 0
```

Il contatore "Dropped" della sezione Software indica il numero di pacchetti eliminati dopo i test di integrità strutturale oppure in seguito all'applicazione dell'insieme di regole del firewall.

Il contatore "IP Input Errs" nella sezione Software specifica il numero di pacchetti eliminati a causa di errori checksum o di intestazioni IP danneggiate che non sono state riconosciute. Quest'ultimo caso è probabilmente il risultato di problemi di rete locale piuttosto che di attacchi remoti.

Loghosts, "logh"

Mostra l'elenco dei destinatari dei log configurati nel firewall a cui inviare i dati di log.

Netcon, "netc"

Mostra un elenco di "utenti" connessi correntemente al firewall mediante il protocollo di gestione *netcon*, ad esempio da EnterNet FireWall Manager.

Nets, "net"

Visualizza il contenuto della sezione di configurazione Nets.

Ping, "pi"

Sintassi: ping <IPAddr> [<# of packets> [<size>]]

Esempio: ping 1.2.3.4 10 1000

Invia un numero specifico di pacchetti ICMP Echo Request a una determinata destinazione. Tutti i pacchetti vengono inviati in successione immediata, invece di uno al secondo. Tale approccio è il migliore per diagnosticare problemi di connettività.

Pipes, "pip"

Sintassi: pipes

Mostra l'elenco dei pipe configurati, il contenuto della sezione di configurazione Pipes nonché i valori relativi alla velocità di trasmissione di ciascun pipe.

Sintassi: pipes <name>

Visualizza i dettagli relativi ad un determinato pipe.

Sintassi: pipes -u <name>

Visualizza i 20 utenti più attivi di un determinato pipe.

ReConfigure, "reco"

Legge nuovamente il file FWCore.cfg dal disco. Questo processo dura approssimativamente un secondo se seguito da disco floppy, mentre circa un decimo di secondo se eseguito da disco rigido o disco flash. Se sul disco esiste già un file FWCore_N.cfg file, sarà invece questo ad essere letto. Tuttavia, poiché non c'è FireWall Manager che tenta di eseguire una comunicazione bidirezionale con il firewall, la configurazione verrà considerata errata e il firewall ritornerà a FWCore.cfg dopo che il timeout per la verifica della comunicazione bidirezionale è scaduto (generalmente 30 secondi).

Remotes, "rem"

Visualizza il contenuto della sezione di configurazione Remotes.

Routes, "r"

Visualizza il contenuto della sezione di configurazione Routes.

Rules, "ru"

Sintassi: `rules [<options>] [<range>]`

Mostra il contenuto della sezione di configurazione Rules.

Opzioni:

- u - Append usage information
- l - Append logging information
- n - Append symbolic rule names
- p - Append pipe information
- a - Append all the information above

Il parametro di intervallo specifica le regole da includere nell'output del comando.

Esempio: `rules -l -u 15-20, 23, 25-29`

Scrsave, "scr"

Attiva o disattiva il salvaschermo incluso nel software del firewall.

Settings, "set"

Visualizza il contenuto della sezione di configurazione Settings.

Sintassi: `settings`

Mostra i gruppi di impostazioni disponibili.

Sintassi: `settings <group_name>`

Mostra le impostazioni per un gruppo specifico.

Sono disponibili i seguenti gruppi di impostazione:

IP	IP (Internet Protocol)
TCP	TCP (Transmission Control Protocol)
ICMP	ICMP (Internet Control Message Protocol)
ARP	ARP (Address Resolution Protocol)
State	Impostazioni stateful inspection
ConnTimeouts	Timeout di connessione predefinita
LengthLim	Limiti di lunghezza predefinita nei protocolli
Frag	Impostazioni di frammentazione
Log	Impostazioni del log
Misc	Impostazioni varie

Per ulteriori informazioni sulle singole impostazioni, consultare la sezione 7.3.2, Scheda SettingsScheda Settings.

Shutdown, "shut"

Sintassi: `shutdown <seconds>`

Istruisce il firewall ad eseguire la chiusura della sessione entro un certo numero di secondi. Non è necessario chiudere la sessione prima che il firewall venga spento, poiché non vi sono file aperti durante il funzionamento.

Stats, "st"

Mostra le statistiche e i contatori.

SymNames, "symn"

Consente di passare alla visualizzazione dei nomi simbolici. Se la funzione SymNames è disattiva, gli altri comandi della console visualizzeranno gli IP numerici e gli indirizzi di rete invece dei nomi simbolici.

8.3 Supporti di avvio di EnterNet FireWall

I supporti di avvio di EnterNet FireWall includono generalmente il sistema Caldera DR-DOS, un sistema operativo compatibile con MS-DOS. DR-DOS viene utilizzato principalmente per fornire un file system standard e consentire ai driver ODI di entrare in funzione nel caso in cui fosse necessario l'utilizzo di tali driver. Inoltre, il software del firewall non utilizza realmente DOS, dal momento che dispone di un sistema operativo integrato a 32 bit in tempo reale.

Contenuto di \

- Directory FireWall
Contiene il software di EnterNet FireWall e i relativi file di configurazione.
- Directory ODI
Contiene i driver delle schede di rete ODI e i relativi file di configurazione, incluso il file net.cfg. Il contenuto di net.cfg e la configurazione delle schede di rete non possono essere modificati in modalità remota. Il file Net.cfg viene generato in base alla configurazione del firewall ogniquale volta viene creato un supporto di avvio del firewall oppure viene salvata la configurazione nel supporto di avvio.
- AutoExec.bat
- Config.sys

Contenuto di \FireWall

- FWCore.exe
Il software di EnterNet FireWall.
- FWCore.cfg
La configurazione corrente utilizzata dal firewall.
- FWCore_O.cfg
Il file FWCore.cfg viene anche salvato come FWCore_O.cfg ogni volta che si seleziona **Save To Boot Media** nel menu **FireWall**. Tuttavia, questo file non viene modificato quando si invia una nuova configurazione al firewall mediante la rete.

- FWCore_N.cfg
In genere questo file *non* esiste. Viene utilizzato come file temporaneo per ricevere una nuova configurazione dalla rete. Una volta verificata la configurazione, questo viene spostato nel file FWCore.cfg.
- Security.bin
Utilizzato per calcolare le chiavi di crittografia con cui devono essere crittografate tutte le comunicazioni verso il firewall.

Contenuto di \ODI

- Lsl.com
ODI Link Support Layer.
- Net.cfg
Impostazioni della scheda di rete. EnterNet FireWall Manager crea automaticamente questo file quando viene selezionato **Create Boot Media** o **Save to Boot Media** nel menu **FireWall**.
- NetStart.bat
I comandi necessari per il caricamento dei driver della scheda di rete. EnterNet FireWall Manager crea automaticamente questo file quando viene selezionato **Create Boot Media** o **Save to Boot Media** nel menu **FireWall**.

Inoltre, in questa directory saranno memorizzati i file dei driver ODI per ogni tipo di scheda di rete utilizzata, se vengono impiegati i driver ODI invece dei driver integrati.

8.4 Considerazioni generali prima della configurazione

- Per tutti gli elenchi di regole, ad esempio Access e Rules, *viene eseguita la prima regola compatibile*. È del tutto indifferente se, ad esempio, esiste una regola alla riga 20 che autorizza il passaggio del protocollo SMTP a un server di posta interno quando invece la regola della riga 10 vieta l'accesso a tutta la rete interna.



- Se si utilizza una zona demilitarizzata, è possibile bloccare le comunicazioni dall'area DMZ alla rete interna *prima* di autorizzare l'area DMZ a comunicare con "tutta la rete", altrimenti si rischia di consentire anche la comunicazione tra l'area DMZ e la propria rete interna. È importante ricordare che la rete interna è inclusa in "tutte le reti". In alternativa, è possibile consentire alle macchine che si trovano nell'area DMZ di comunicare con tutti i dispositivi instradati all'interfaccia "ext" specificando "ext" come interfaccia di destinazione in tutte le regole riguardanti le connessioni verso l'esterno dall'area DMZ.

- Le regole SAT hanno alcune particolarità. Se un pacchetto soddisfa una regola SAT, il firewall ricorderà solo che la traduzione statica dell'indirizzo verrà eseguita successivamente. Quindi continuerà a ricercare una regola compatibile FwdFast, Allow, NAT, Drop o Reject nel set di regole.

- Le regole SAT vengono eseguite solo *dopo* che una regola FwdFast, Allow o NAT ha autorizzato il traffico. Ciò significa che se una regola SAT traduce l'indirizzo di destinazione da 1.1.1.1 a 2.2.2.2, le regole FwdFast, Allow o NAT dovranno consentire il traffico all'indirizzo di destinazione 1.1.1.1 e *non* 2.2.2.2.

- Se si utilizza un inoltro senza stato, come FwdFast, bisognerà anche autorizzare esplicitamente il *traffico di ritorno*. In questo caso, il firewall non rileva le connessioni aperte e quindi non può determinare automaticamente il traffico di ritorno da autorizzare. È buona norma attivare l'impostazione "*Only established*" relativa al traffico di ritorno.

- Il filtro dell'interfaccia di destinazione nella sezione Rules si applica solo alle ricerche dei percorsi eseguite *prima* che il pacchetto entri nel set di regole. La traduzione dell'indirizzo *non* viene presa in considerazione. L'unico fattore decisivo nel calcolo dell'interfaccia di destinazione è la tabella di instradamento.

8.5 Esempi di configurazione

In questa sezione vengono illustrati vari esempi di configurazione, che è possibile trovare in FireWall Manager come modelli già preinstallati.

Esempio 1: Default

Questa configurazione di base, che utilizza due interfacce, esegue la traduzione dinamica dell'indirizzo su tutto il traffico verso l'esterno e contiene regole predefinite per autorizzare il traffico diretto ad un server Web o di posta situato sulla rete interna.

Esempio 2: Default-ProxyARP

Una caso particolare di configurazione "Default", che utilizza la regola Proxy ARP per autorizzare l'installazione con poche modifiche, o nessuna, agli host e ai router connessi.

Esempio 3: DMZ

Una configurazione con tre interfacce in cui un server Web, un server di posta elettronica e un server FTP si trovano in una zona demilitarizzata (DMZ).

Esempio 4: DMZ-MailFwd-DNS

Simile alla configurazione "DMZ". Il server di posta viene spostato nella rete interna ed è aggiunto un sistema di instradamento della posta all'area DMZ. Questo modello contiene regole predefinite per un server DNS situato nell'area DMZ.

Esempio 5: DMZ-ProxyARP

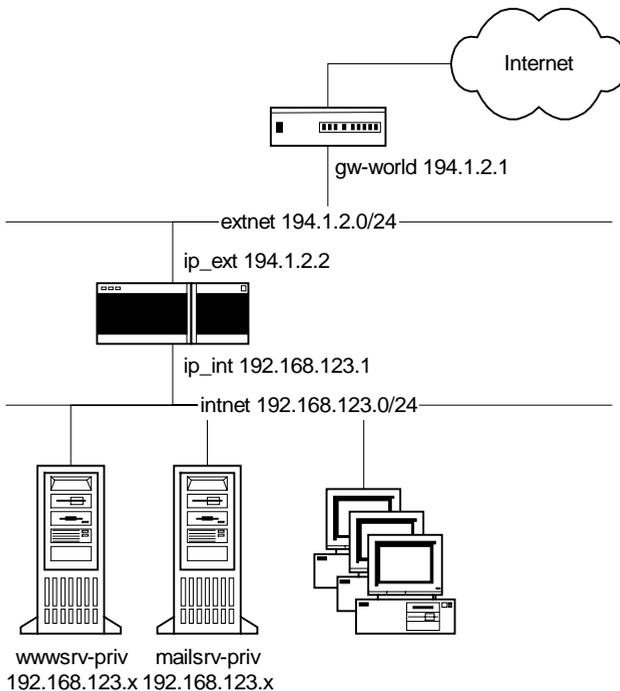
Una caso particolare di configurazione "DMZ", che utilizza la regola Proxy ARP per autorizzare l'installazione con poche modifiche, o nessuna, ai server e ai router connessi.

Esempio 6: DMZ-Shared-Extnet

Un adattamento della regola "DMZ-ProxyARP", basata però sul presupposto che il firewall esterno sia condiviso con altri clienti o server e che solo alcuni indirizzi sono instradati ai server in DMZ.

8.5.1 Esempio 1: Default

Questa configurazione, che utilizza due interfacce, esegue la traduzione dinamica dell'indirizzo di tutte le comunicazioni dalla rete protetta fatta eccezione per NetBIOS, a cui non è consentito passare attraverso il firewall in nessuna direzione.



La configurazione contiene anche regole che consentono il passaggio di HTTP verso un server Web e di SMTP verso un server di posta elettronica. Questi server sono connessi alla rete protetta e hanno indirizzi privati. Sulle connessioni viene eseguita la traduzione dinamica dell'indirizzo.

Descrizione della sezione Hosts

1	ip_int	192.168.123.1
2	br_int	192.168.123.255

È necessario sostituire l'indirizzo ip_int con l'IP relativo all'interfaccia interna del firewall. Sostituire l'indirizzo br_int con l'indirizzo broadcast della rete interna. L'indirizzo broadcast è il più alto della rete.

Gli indirizzi ip_int e br_int vengono utilizzati nella sezione Interfaces per configurare l'interfaccia "int".

3	ip_ext	194.1.2.2
4	br_ext	194.1.2.255

Apportare le modifiche descritte nelle istruzioni precedenti che verranno applicate all'interfaccia esterna del firewall. Questi indirizzi vengono forniti principalmente dal provider di servizi Internet (ISP, Internet Service Provider).

5	gw-world	194.1.2.1
---	----------	-----------

Si tratta dell'indirizzo del router più esterno e, nella maggior parte dei casi, viene fornito dal provider di servizi Internet (ISP, Internet Service Provider).

6	loghost	0.0.0.0
---	---------	---------

Dopo avere installato EnterNet FireWall Logger o un daemon syslog di terze parti, digitarne l'indirizzo in questa posizione.

L'indirizzo viene utilizzato nella sezione Loghosts perché il firewall disponga delle informazioni per l'invio dei dati da registrare.

Se si utilizza un destinatario syslog al posto di FireWall Logger, sarà necessario modificare il tipo di loghost nella sezione Loghosts.

7	wwwsrv-priv	0.0.0.0
8	mailsrv-priv	0.0.0.0

Se si dispone di server Web o di posta con indirizzi privati che si desidera rendere accessibili pubblicamente, digitarne l'indirizzo in questa posizione. È possibile ovviamente specificare un unico indirizzo per entrambi i servizi se questi sono installati sullo stesso server.

Questi indirizzi vengono utilizzati dalle regole SAT nella sezione Rules per implementare la traduzione statica degli indirizzi, rispettivamente nelle porte 80 e 25.

9	wwwsrv-pub	ip_ext
10	mailsrv-pub	ip_ext

È inoltre possibile specificare gli indirizzi tramite i quali sono pubblicati i server Web e di posta. Utilizzando gli indirizzi preimpostati, i server Web e di posta saranno pubblicati tramite l'indirizzo IP esterno del firewall.

Questi indirizzi vengono utilizzati nella sezione Rules per implementare la traduzione statica dell'indirizzo e consentire la connessione rispettivamente alle porte 80 e 25.

Gli indirizzi sopra descritti vengono pubblicati automaticamente nella sezione ARP. Se questi vengono modificati in un indirizzo differente dall'IP esterno del firewall, sarà probabilmente necessario che questo risponda alle query ARP per tali indirizzi. In questo caso, il traffico destinato a tali indirizzi sarà diretto al firewall. Se il traffico verso tali indirizzi era instradato comunque al firewall, gli indirizzi non saranno pubblicati. La pubblicazione ARP, che sia necessaria o meno, non provocherà alcun danno.

Descrizione della sezione ARP

1	Publish	mailsrv-pub
2	Publish	wwwsrv-pub

Queste due righe della sezione ARP consentono al router esterno di trovare gli indirizzi pubblici dei server Web e di posta, nel caso in cui sia necessario modificarli in qualcosa di diverso dall'indirizzo IP esterno del firewall.

In questa configurazione, si presuppone sempre che questi due indirizzi appartengano alla rete tra il router esterno e il firewall.

Descrizione della sezione Access

La sezione Access consente di verificare che gli indirizzi del mittente ricevuti su ciascuna interfaccia corrispondano a quelli attesi dal firewall. In questa configurazione, quindi, ci si aspetta che gli indirizzi interni provengano dall'interno e che quelli esterni provengano dall'esterno. Vengono inoltre bloccati alcuni indirizzi di mittenti non validi.

1	Drop	ANY	0.0.0.0/8
---	------	-----	-----------

La regola 1 consente di bloccare gli indirizzi di mittenti da 0.0.0.0 a 0.255.255.255, indipendentemente dall'origine. La rete non è valida e non si desidera ricevere pacchetti provenienti da essa.

2	Drop	ANY	127.0.0.0/8
---	------	-----	-------------

La regola 2 consente di bloccare gli indirizzi di mittenti da 127.0.0.0 a 127.255.255.255, indipendentemente dall'origine. La rete include l'host locale, 127.0.0.1, indirizzo che corrisponde sempre al computer locale. Non ci si aspetta che tali indirizzi siano visibili in rete e quindi vengono considerati non validi.

3	Drop	ANY	224.0.0.0/3
---	------	-----	-------------

La regola 3 consente di bloccare gli indirizzi di mittenti da 224.0.0.0 a 255.255.255.255, indipendentemente dall'origine. Si tratta di *indirizzi multicast*, che sono validi, ma possono essere utilizzati solo come destinazione, quindi non sono consentiti come indirizzi di mittente.

4	Expect	int	intnet
---	--------	-----	--------

La regola 4 presuppone che gli indirizzi dei mittenti appartenenti a internet arrivino all'interfaccia interna. Se l'indirizzo del mittente del pacchetto appartiene a intnet ma raggiunge un'interfaccia differente, viene scartato e registrato.

5	Expect	ext	all-nets
---	--------	-----	----------

La regola 5 presuppone che tutti gli indirizzi, non appartenenti alle categorie descritte in precedenza, arrivino all'interfaccia esterna. Se i pacchetti con tali indirizzi di mittente raggiungono un'interfaccia differente, vengono scartati e registrati.

Notare che la regola è applicata al parametro "all-nets" che, come detto in precedenza, equivale a tutti gli indirizzi IP. Tuttavia, visto che la ricerca all'interno del set di regole viene eseguita dall'alto verso il basso, gli indirizzi 0.0.0.0/8, 127.0.0.0/8 e 224.0.0.0/3 e intnet saranno già stati presi in considerazione prima che, nell'ordine, venga raggiunta la regola 5.

Descrizione della sezione Rules

L'insieme di regole di questo modello di configurazione può essere riassunto nel modo seguente:

- Consente tutte le connessioni originate dall'interno, tranne NetBIOS, tramite traduzione dinamica dell'indirizzo.
- Consente l'accesso HTTP a un indirizzo pubblico che a sua volta viene tradotto staticamente in un server Web con indirizzo privato sulla rete interna.
- Consente l'accesso SMTP a un indirizzo pubblico, che a sua volta viene tradotto staticamente in un server di posta con indirizzo privato sulla rete interna.

1	Drop	ANY	all-nets	all-nets	UDP	ALL → 137
2	Drop LOG	ANY	all-nets	all-nets	Ports	ALL → 135-139

Queste due regole garantiscono che il traffico NetBIOS venga bloccato in tutte le direzioni. In realtà, non sono state studiate per il blocco del traffico NetBIOS in entrata, quanto per quello in *uscita*. Tuttavia, il fatto che queste regole appaiano prima nella configurazione significa che un protocollo non sicuro come questo non viene mai autorizzato erroneamente a passare nella configurazione.

Inizialmente, la prima regola potrebbe apparire inutile. Tuttavia, la registrazione viene attivata solo per la regola 2. La porta 137 UDP è del tipo NetBIOS Name Resolution, cosa che si verifica più o meno costantemente. Di conseguenza, non viene registrata.

Se si riceve il traffico UDP verso la porta 137, esso verrà eliminato senza essere registrato dalla regola 1, poiché è la prima regola compatibile, invece di venir eliminato e registrato dalla regola 2.

3	SAT	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80 SetDest wwwsrv-priv 80
4	SAT	ANY	all-nets	mailsrv-pub/32	TCP	ALL → 25 SetDest mailsrv-priv 25

Le regole 3 e 4 consentono di implementare la traduzione statica dell'indirizzo per la pubblicazione di un server Web o di posta tramite indirizzi pubblici. Gli indirizzi pubblici vengono preimpostati nella sezione Hosts come equivalenti dell'indirizzo IP esterno del firewall. È comunque possibile trasformarli in altri indirizzi pubblici.



Notare che queste due regole *non* consentono alcun passaggio di traffico. Quando viene soddisfatta una delle due regole, il firewall ricorda che la traduzione dell'indirizzo verrà eseguita successivamente, continuando a cercare una regola che consenta la connessione. In questa configurazione, la regola necessaria può essere, a seconda delle circostanze, 6, 7 oppure 8.

5	Fwd	int	intnet	intnet	Std	
---	-----	-----	--------	--------	-----	--

Questa regola consente al traffico proveniente dalla rete interna di ritornare sulla rete interna utilizzando *l'inoltro del pacchetto senza stato*. In questa configurazione, il motivo dell'esistenza di questa regola non è molto evidente. Se si prende in considerazione però una rete più estesa in cui il firewall funziona da *gateway predefinito* per un gran numero di router interni, questa regola può risultare estremamente utile.

Nella maggior parte dei casi, tale regola diventa ancora più specifica autorizzando solo il traffico destinato all'indirizzo IP interno del firewall, UDP porta 999. Senza questa regola, non potrà funzionare l'amministrazione remota dalla rete interna.

6	NAT	int	intnet	all-nets	Std	
---	-----	-----	--------	----------	-----	--

La regola 6 consente la traduzione dinamica dell'indirizzo per tutto il traffico proveniente dalla rete interna verso l'esterno.

In questa regola sono comprese le connessioni interne agli indirizzi pubblici tramite i quali sono pubblicati il server Web e di posta. Di conseguenza, le connessioni originate internamente verso questi server saranno tradotte dinamicamente. Tale approccio consentirà ai log del server di visualizzare l'indirizzo IP del firewall invece dei singoli indirizzi privati. Ciò non può essere evitato quando si utilizza questa struttura di rete e si desidera comunicare con i server privati mediante gli indirizzi pubblici. Per un approfondimento sui relativi problemi, consultare la sezione 8.1, Traduzione degli indirizzi.

7	Allow	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80
8	Allow	ANY	all-nets	mailsrv-pub/32	TCP	ALL → 25

Le regole 7 e 8 consentono l'accesso del traffico agli indirizzi pubblici dei server Web e di posta, rispettivamente le porte 80 e 25. Gli indirizzi di destinazione saranno inoltre tradotti secondo le regole NAT descritte in precedenza.

9	Reject	ANY	all-nets	ip_ext/32	TCP	ALL → 113
10	Drop LOG	ANY	all-nets	all-nets	All	

Le regole 9 e 10 non sono in relazione diretta con la protezione.

Il traffico che non soddisfa nessuna delle regole incluse nel set viene sempre scartato *senza essere registrato*. È per questo motivo che conviene aggiungere una regola finale che oltre a scartare il traffico lo registra.

La regola 9 è necessaria poiché molti server FTP in Internet eseguono tentativi di apertura di connessioni verso il mittente quando vi si accede. La porta 113 è stata ideata per "ident daemon", che nei sistemi Unix consente al server di determinare l'utente locale che tenta la connessione. Se in questa posizione non è presente una regola Reject, tali server possono ritardare la connessione fino ad un minuto nel tentativo di aprire una connessione verso la porta 113. La regola Reject predispone il firewall per la restituzione di un messaggio TCP RESET per notificare immediatamente al server che la connessione alla porta 113 non sarà possibile e la procedura di accesso proseguirà senza ritardi.

Commenti sulla configurazione

- Si sconsiglia di posizionare i server Web e di posta nella rete interna accessibile pubblicamente. Si tratta di parti software molto complesse e di conseguenza presentano numerosi problemi di sicurezza. Un'ottima alternativa è quella di posizionare il server Web e un sistema di instradamento della posta in un'area DMZ, una zona demilitarizzata. Per alcuni esempi, consultare la sezione Esempio 3: DMZ oppure Esempio 4: DMZ-MailFwd-DNS più avanti.
- Il fatto che il firewall esegua la traduzione dinamica dell'indirizzo dall'interno dei server Web e di posta potrebbe sembrare leggermente strano, poiché significa che i log dei server non sono in grado di distinguere tra i vari client interni. Tuttavia, esiste una buona ragione per tale comportamento. Consultare il paragrafo 8.1.7.2, Server accessibile pubblicamente con un indirizzo privato su una rete interna_{server} accessibile pubblicamente con un indirizzo privato su una rete interna, nella sezione relativa alla traduzione dell'indirizzo.

- Se non si desidera la traduzione dell'indirizzo relativa al traffico interno verso i server accessibili pubblicamente, è possibile aggiungere un server DNS interno che viene utilizzato solo dai client interni. In questo server DNS, i record degli indirizzi sono impostati per puntare agli indirizzi interni dei server. Naturalmente, l'accesso a questo server DNS non può essere consentito dall'esterno.

8.5.2 Esempio 2: Default-ProxyARP

Il modello di configurazione "Default-ProxyARP" si basa sul modello "Default". Questo modello presenta le stesse funzionalità di base, ma consente inoltre agli host interni di conservare gli stessi indirizzi e allo stesso tempo di non dover creare una nuova rete tra il router esterno e il firewall.

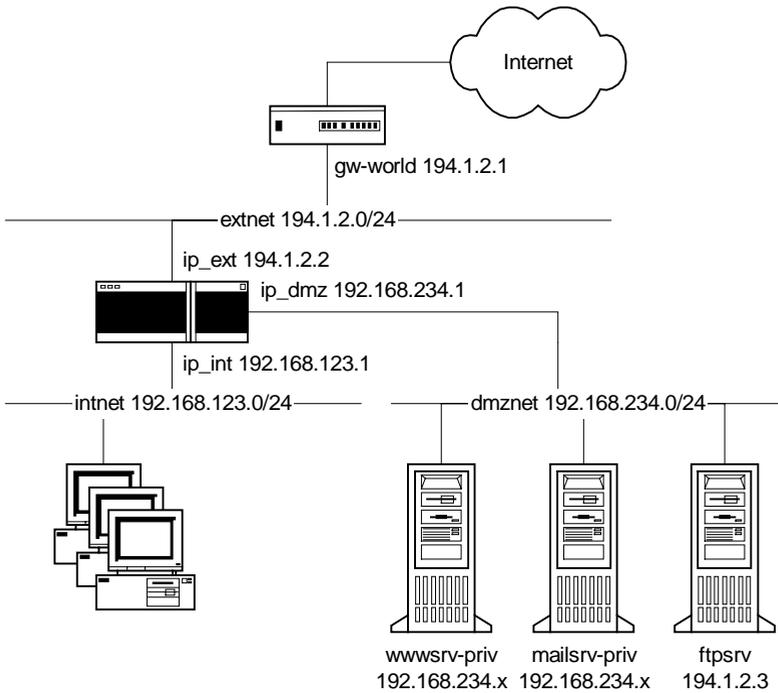
Ciò è possibile utilizzando la funzione Proxy ARP, che consente di "inserire" il firewall tra il router esterno e le reti protette senza dover apportare delle modifiche a router o agli host esistenti.

Differenze:

- La rete "extnet" è scomparsa. Il firewall riceve l'informazione che esiste solo un indirizzo IP connesso direttamente all'adattatore di rete esterno: il router esterno.
- Il percorso extnet è sostituito da "gw-world/32".
- La funzione Proxy ARP viene utilizzata per pubblicare "gw-world" nel settore interno del firewall. In questo modo i computer protetti non devono modificare il *gateway predefinito* nelle loro impostazioni di rete.

8.5.3 Esempio 3: DMZ

Il modello di configurazione DMZ prende in esame su un firewall con tre interfacce. Un'interfaccia è connessa al router esterno, la seconda alla rete protetta cui sono collegati le workstation e i server interni. La terza interfaccia è connessa alla zona demilitarizzata (DMZ, DeMilitarized Zone).



L'area DMZ contiene:

- Un server Web, `wwsrv-priv`, con la porta 80 accessibile tramite un indirizzo pubblico, `wwsrv-pub`. Nelle opzioni predefinite, l'indirizzo viene impostato come equivalente all'indirizzo IP esterno del firewall.
 - Un server di posta, `mailsrv-priv`, con la porta 25 accessibile da un indirizzo pubblico, `mailsrv-pub`. Nelle opzioni predefinite, l'indirizzo viene impostato come equivalente all'indirizzo IP esterno del firewall.
 - Un server FTP, `ftpsrv`, che ha un indirizzo pubblico nonostante si trovi nell'area DMZ insieme ad altri server con indirizzi privati. Affinché EnterNet FireWall v5.1 possa gestire le comunicazioni con un server FTP, il server deve avere un indirizzo pubblico. A tal fine, la porta 21 e le porte 1024—65535 sul server FTP devono essere accessibili pubblicamente.
 -

Descrizione della sezione Hosts

1	<code>ip_int</code>	192.168.123.1
2	<code>br_int</code>	192.168.123.255

È necessario sostituire l'indirizzo `ip_int` con l'IP relativo all'interfaccia interna del firewall. Sostituire l'indirizzo `br_int` con l'indirizzo broadcast della rete interna. L'indirizzo broadcast è il più alto della rete.

Gli indirizzi `ip_int` e `br_int` vengono utilizzati nella sezione Interfaces per configurare l'interfaccia "int".

3	<code>ip_ext</code>	194.1.2.2
4	<code>br_ext</code>	194.1.2.255

Apportare le modifiche descritte nelle istruzioni precedenti che verranno applicate all'interfaccia esterna del firewall. Questi indirizzi vengono forniti principalmente dal provider di servizi Internet (ISP, Internet Service Provider).

5	ip_dmz	192.168.234.1
6	br_dmz	192.168.234.255

Modificare in base alle istruzioni precedenti. Queste impostazioni si applicano solo all'interfaccia DMZ del firewall.

7	gw-world	194.1.2.1
---	----------	-----------

Questo è l'indirizzo del router più esterno e nella maggior parte dei casi viene fornito dal provider di servizi Internet (ISP, Internet Service Provider).

8	loghost	0.0.0.0
---	---------	---------

Dopo avere installato EnterNet FireWall Logger o un daemon syslog di terze parti, digitarne l'indirizzo in questa posizione.

L'indirizzo viene utilizzato nella sezione Loghosts perché il firewall disponga delle informazioni per l'invio dei dati di log.

Se si utilizza un destinatario syslog al posto di FireWall Logger, sarà necessario modificare il tipo di loghost nella sezione Loghosts.

9	wwsrv-priv	0.0.0.0
10	mailsrv-priv	0.0.0.0

Se si dispone di server Web o di posta con indirizzi privati che si desidera rendere accessibili pubblicamente, digitarne l'indirizzo in questa posizione. È possibile ovviamente specificare un unico indirizzo per entrambi i servizi se questi sono installati sullo stesso server.

Questi indirizzi vengono utilizzati dalle regole SAT nella sezione Rules per implementare la traduzione statica degli indirizzi, rispettivamente nelle porte 80 e 25.

11	wwwsrv-pub	ip_ext
12	mailsrv-pub	ip_ext

È inoltre possibile specificare gli indirizzi tramite i quali sono pubblicati i server Web e di posta. Utilizzando gli indirizzi predefiniti, i server Web e di posta saranno pubblicati tramite l'indirizzo IP esterno del firewall.

Questi indirizzi vengono utilizzati nella sezione Rules per implementare la traduzione statica dell'indirizzo e consentire la connessione, rispettivamente alle porte 80 e 25.

Gli indirizzi sopra descritti vengono pubblicati automaticamente nella sezione ARP. Se questi vengono modificati in un indirizzo differente dall'IP esterno del firewall, sarà probabilmente necessario che questo risponda alle query ARP per tali indirizzi. In questo caso il traffico destinato a tali indirizzi sarà diretto al firewall. Se il traffico verso tali indirizzi era instradato comunque al firewall, gli indirizzi non saranno pubblicati. La pubblicazione ARP, che sia necessaria o meno, non provocherà alcun danno.

13	ftpsrv	194.1.2.3
----	--------	-----------

Il server FTP che si trova nell'area DMZ viene configurato con un indirizzo pubblico, nonostante sia ubicato nella stessa rete di altri server con indirizzi privati. Questo indirizzo viene utilizzato nella sezione Rules per autorizzare il traffico verso la porta 21 e le porte 1024—65535. Il server FTP può inoltre aprire connessioni esterne verso le porte 1024—65535. Tale indirizzo viene utilizzato nella sezione Routes per dirigere al server, ubicato nell'area DMZ, tutto il traffico verso questo indirizzo. La funzione Proxy ARP viene attivata sull'interfaccia esterna per questo percorso, in modo da istruire il router esterno a inviare al firewall il traffico destinato al server FTP.

Descrizione della sezione Routes

La sezione di configurazione Routes merita un'attenzione particolare, in quanto la situazione di instradamento è leggermente atipica. Il server FTP, che dispone di un indirizzo pubblico IP ottenuto dall'intervallo esterno di indirizzi IP, si trova nell'area DMZ insieme ad altri server che hanno indirizzi privati.

	Ifaces	Net	Gateway	ProxyARP
1	int	intnet		

Il percorso 1 è normale; il traffico verso la rete interna viene instradato attraverso l'interfaccia interna.

2	dmz	ftpsrv/32		ext
---	-----	-----------	--	-----

Il percorso 2 è atipico; il traffico verso il server FTP viene instradato attraverso l'interfaccia DMZ, nonostante il fatto che ftpsrv appartenga normalmente alla rete esterna se si considera il relativo indirizzo. Inoltre, l'indirizzo viene pubblicato anche sull'interfaccia esterna mediante Proxy ARP in modo da istruire il router esterno a inviare al firewall il traffico destinato al server FTP.

3	ext	extnet		dmz
---	-----	--------	--	-----

Il percorso 3 è abbastanza normale. Il traffico verso la rete esterna viene instradato attraverso l'interfaccia esterna, proprio come nella maggior parte delle configurazioni. Tuttavia, gli indirizzi presenti sulla rete esterna, fatta eccezione per ftpsrv, vengono pubblicati mediante Proxy ARP sull'interfaccia DMZ. Ciò consente al server FTP di utilizzare il normale gateway predefinito che appartiene alla rete esterna.

4	dmz	dmznet		
---	-----	--------	--	--

Il percorso 4 è normale; il traffico verso l'area DMZ viene instradato attraverso l'interfaccia DMZ.

5	ext	all-nets	gw-world	
---	-----	----------	----------	--

Il percorso 5 gestisce tutto il traffico che non è controllato da nessuno dei percorsi già menzionati; viene instradato mediante il gateway predefinito del firewall, gw-world, verso l'interfaccia esterna. Notare che non è importante la posizione in cui si trovano i percorsi nell'elenco, poiché essi sono sempre disposti in un ordine tale che, nel momento in cui il firewall legge la tabella di instradamento, viene sempre per primo il percorso più specifico. Di conseguenza, un percorso che gestisce "tutti gli indirizzi" sarà sempre considerato per ultimo e solo quando nessun altro percorso corrisponde all'indirizzo di destinazione.

Descrizione della sezione Access

La sezione Access consente di verificare che gli indirizzi del mittente ricevuti su ciascuna interfaccia corrispondano a quelli attesi dal firewall. In questa configurazione, quindi, ci si aspetta che gli indirizzi interni provengano dall'interno e che quelli esterni provengano dall'esterno. Vengono inoltre bloccati alcuni indirizzi di mittenti non validi.

1	Drop	ANY	0.0.0.0/8
---	------	-----	-----------

La regola 1 consente di bloccare gli indirizzi di mittenti da 0.0.0.0 a 0.255.255.255, indipendentemente dall'origine. La rete non è valida e non si desidera ricevere pacchetti provenienti da essa.

2	Drop	ANY	127.0.0.0/8
---	------	-----	-------------

La regola 2 consente di bloccare gli indirizzi di mittenti da 127.0.0.0 a 127.255.255.255, indipendentemente dall'origine. La rete include l'host locale, 127.0.0.1, indirizzo che corrisponde sempre al computer locale. Non ci si aspetta che tali indirizzi siano visibili in rete e quindi vengono considerati non validi.

3	Drop	ANY	224.0.0.0/3
---	------	-----	-------------

La regola 3 consente di bloccare gli indirizzi di mittenti da 224.0.0.0 a 255.255.255.255, indipendentemente dall'origine. Si tratta di *indirizzi multicast*, che sono validi, ma possono essere utilizzati solo come destinazione, quindi non sono consentiti come indirizzi di mittente.

4	Expect	int	intnet
---	--------	-----	--------

La regola 4 presuppone che gli indirizzi dei mittenti appartenenti a internet arrivino all'interfaccia interna. Se l'indirizzo del mittente del pacchetto appartiene a intnet ma raggiunge un'interfaccia differente, viene scartato e registrato.

5	Expect	dmz	ftpsrv/32
---	--------	-----	-----------

La regola 5 presuppone che i pacchetti inviati dall'indirizzo del server FTP arrivino all'interfaccia DMZ. Questa regola particolare è richiesta poiché l'indirizzo del server FTP sarebbe altrimenti atteso sull'interfaccia esterna.

6	Expect	dmz	dmznet
---	--------	-----	--------

La regola 6 presuppone che gli indirizzi dei mittenti appartenenti a dmznet arrivino all'interfaccia DMZ. Se l'indirizzo del mittente del pacchetto appartiene a dmznet, ma raggiunge un'interfaccia differente, viene scartato e registrato.

7	Expect	ext	all-nets
---	--------	-----	----------

La regola 7 presuppone che tutti gli indirizzi, non appartenenti alle categorie descritte in precedenza, arrivino all'interfaccia esterna. Se i pacchetti con tali indirizzi di mittente raggiungono un'interfaccia differente, vengono scartati e registrati.

Notare che la regola è applicata al parametro "all-nets" che, come detto in precedenza, equivale a tutti gli indirizzi IP. Tuttavia, visto che la ricerca all'interno del set di regole viene eseguita dall'alto verso il basso, gli indirizzi 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/3, dmznet, intnet nonché ftpsrv/32 saranno già stati presi in considerazione prima che nell'ordine venga raggiunta la regola 7.

Descrizione della sezione Rules

L'insieme di regole di questo modello di configurazione può essere riassunto nel modo seguente:

- Consente tutte le connessioni originate dall'interno, tranne NetBIOS, tramite traduzione dinamica dell'indirizzo.
- Consente le comunicazioni NetBIOS dalla rete interna a DMZ, mediante traduzione dinamica dell'indirizzo.
- Consente l'accesso HTTP a un indirizzo pubblico che a sua volta viene tradotto staticamente in un server Web con indirizzo privato sulla rete DMZ.
- Consente l'accesso SMTP a un indirizzo pubblico, che a sua volta viene tradotto staticamente in un server di posta con indirizzo privato sulla rete DMZ.
- Consente l'accesso FTP ad un server FTP con un indirizzo pubblico, situato in un'area DMZ. Ciò include comunicazioni complete bidirezionali sulle porte 1024—65535 per garantire che il canale dei dati FTP funzioni correttamente in entrambe le modalità, attiva e passiva.
- Consente ai server che si trovano nell'area DMZ di eseguire query DNS a tutte le reti tranne quella interna.
- Consente ai server di posta che si trovano nell'area DMZ di comunicare mediante SMTP con tutte le reti tranne quella interna.

1	NAT	int	intnet	dmznet	Ports	ALL → 135-139
---	-----	-----	--------	--------	-------	---------------

La regola 1 autorizza le connessioni NetBIOS originate internamente verso un'area DMZ mediante traduzione dinamica dell'indirizzo. Questa regola esplicita è necessaria poiché le regole 2 e 3 che seguono bloccano tutte le connessioni NetBIOS.

Il motivo per cui vengono tradotti gli indirizzi delle connessioni interne all'area DMZ è che non si desidera rivelare la struttura della rete interna dei server presenti nell'area DMZ, per evitare che finiscano sotto il controllo di un utente indesiderato.

2	Drop	ANY	all-nets	all-nets	UDP	ALL → 137
3	Drop LOG	ANY	all-nets	all-nets	Ports	ALL → 135-139

Le regole 2 e 3 consentono il blocco di tutte le comunicazioni NetBIOS ad eccezione di quelle consentite dalla regola 1. Come nell'esempio 1, la risoluzione del nome NetBIOS, porta 137 UDP, viene scartata senza essere registrata se si verifica molto spesso. D'altra parte, tutte le altre porte dell'intervallo 135-139, inclusa la porta 137 TCP, vengono registrate e bloccate.

4	SAT	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80 SetDest wwwsrv-priv 80
5	SAT	ANY	all-nets	mailsrv-pub/32	TCP	ALL → 25 SetDest mailsrv-priv 25

Le regole 3 e 4 consentono di implementare la traduzione statica dell'indirizzo per la pubblicazione di un server Web o di posta tramite indirizzi pubblici. Gli indirizzi pubblici vengono preimpostati nella sezione Hosts come equivalenti dell'indirizzo IP esterno del firewall. È comunque possibile trasformarli in altri indirizzi pubblici.



Notare che queste due regole *non* consentono alcun passaggio di traffico. Quando viene soddisfatta una delle due regole, il firewall ricorda che la traduzione dell'indirizzo verrà eseguita successivamente, continuando a cercare una regola che consenta la connessione. In questa configurazione, la regola necessaria può essere, a seconda delle circostanze, 7, 8 oppure 9.

6	Fwd	int	intnet	intnet	All	
---	-----	-----	--------	--------	-----	--

Questa regola consente al traffico proveniente dalla rete interna di ritornare sulla rete interna utilizzando *l'inoltro del pacchetto senza stato*. In questa configurazione, il motivo dell'esistenza di questa regola non è molto evidente. Se si prende in considerazione però una rete più estesa in cui il firewall funziona da *gateway predefinito* per un gran numero di router interni, questa regola può risultare estremamente utile.

Nella maggior parte dei casi, tale regola diventa ancora più specifica autorizzando solo il traffico destinato all'indirizzo IP interno del firewall, UDP porta 999. Senza questa regola, non potrà funzionare l'amministrazione remota dalla rete interna.

7	NAT	int	intnet	all-nets	Std	
---	-----	-----	--------	----------	-----	--

La regola 7 consente la traduzione dinamica dell'indirizzo per tutto il traffico proveniente dalla rete interna verso l'esterno.

In questa regola sono comprese le connessioni interne agli indirizzi pubblici tramite i quali sono pubblicati il server Web e di posta. Le connessioni a questi indirizzi ne risultano tradotte dinamicamente, purché siano interne.

Il motivo per cui vengono tradotti gli indirizzi delle connessioni interne all'area DMZ è che non si desidera rivelare la struttura della rete interna dei server presenti nell'area DMZ, per evitare che finiscano sotto il controllo di un utente indesiderato.

Uno spiacevole effetto secondario è che i log nei server Web e di posta mostreranno che l'accesso è stato effettuato dall'interfaccia DMZ del firewall e non dai singoli indirizzi interni.

8	Allow	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80
9	Allow	ANY	all-nets	mailsrv-pub/32	TCP	ALL → 25

Le regole 8 e 9 consentono l'accesso del traffico agli indirizzi pubblici dei server Web e di posta, rispettivamente le porte 80 e 25. Gli indirizzi di destinazione saranno inoltre tradotti secondo le regole NAT descritte in precedenza.

10	Allow	ANY	all-nets	ftpsrv/32	TCP	ALL → 21
11	Allow	ANY	all-nets	ftpsrv/32	TCP	ALL → High

La regola 10 consente le connessioni alla porta 21 sul server FTP, il canale dei comandi di FTP. La regola 11 consente di connettersi a tutte le porte più alte del server FTP in modo da far lavorare FTP in modalità passiva.



Prima di consentire le connessioni a tutte le porte alte di un server FTP, è necessario determinare se esistono servizi di rete che possono riceverle. Nel caso in cui sono presenti, l'accesso a queste porte deve essere bloccato prima di consentire il traffico a tutte le restanti porte alte.

12	Drop LOG	ANY	all-nets	intnet	All	
----	-------------	-----	----------	--------	-----	--

La regola 12 consente di bloccare tutto il traffico diretto alla rete interna, indipendentemente dall'utente. In tal modo le regole seguenti, che consentono varie forme di comunicazione dall'area DMZ, non devono autorizzare la connessione dell'interfaccia DMZ alla rete interna.

13	Allow	dmz	ftpsrv/32	all-nets	TCP	ALL → High
----	-------	-----	-----------	----------	-----	------------

La regola 13 consente al server FTP di riaprire le connessioni di dati a tutti i client connessi sulle porte alte, cosa che si verifica quando si utilizza la modalità attiva di FTP. Notare che ciò *non* consente di ristabilire connessioni verso la rete interna, poiché tali comunicazioni sono bloccate dalla regola 12. Ciò significa che i client nella rete interna devono utilizzare la modalità passiva di FTP per comunicare con il server FTP. La modalità passiva di FTP dalla rete interna è consentita dalla regola 7, che abilita tutte le connessioni dalla rete interna mediante traduzione dinamica dell'indirizzo.

14	NAT	dmz	mailsrv-priv/32	all-nets	TCP	ALL → 25 SetSrc mailsrv-pub 0
----	-----	-----	-----------------	----------	-----	----------------------------------

La regola 14 consente al server di posta di stabilire connessioni SMTP verso reti esterne. Su queste comunicazioni viene eseguita la traduzione dinamica dell'indirizzo, utilizzando un indirizzo pubblico del server di posta come indirizzo del mittente.

15	NAT	dmz	dmznet	all-nets	UDP	ALL → 53
----	-----	-----	--------	----------	-----	----------

La regola 15 consente a tutte le macchine presenti nell'area DMZ di eseguire query DNS verso reti esterne. Su queste comunicazioni viene eseguita la traduzione dinamica dell'indirizzo, utilizzando l'indirizzo esterno del firewall come indirizzo del mittente.

16	Drop LOG	dmz	all-nets	all-nets	All	
----	-------------	-----	----------	----------	-----	--

La regola 16 consente di bloccare tutte le altre comunicazioni dall'area DMZ e le registra con un avviso di alta priorità. In tal modo, è possibile attribuire una comunicazione inattesa dai server nell'area DMZ ad un'intrusione. Le comunicazioni autorizzate da questi server devono perciò essere limitate ad un valore minimo per aumentare la possibilità di scoprire tali attacchi e di rendere sempre più difficile l'accesso di un intruso alle altre parti del sistema.

17	Reject	ANY	all-nets	ip_ext/32	TCP	ALL → 113
18	Drop	ANY	all-nets	all-nets	All	

Le regole 17 e 18 non sono in relazione diretta con la protezione.

Il traffico che non soddisfa nessuna delle regole incluse nel set viene sempre scartato *senza essere registrato*. È per questo motivo che conviene aggiungere una regola finale che oltre a scartare il traffico lo registra.

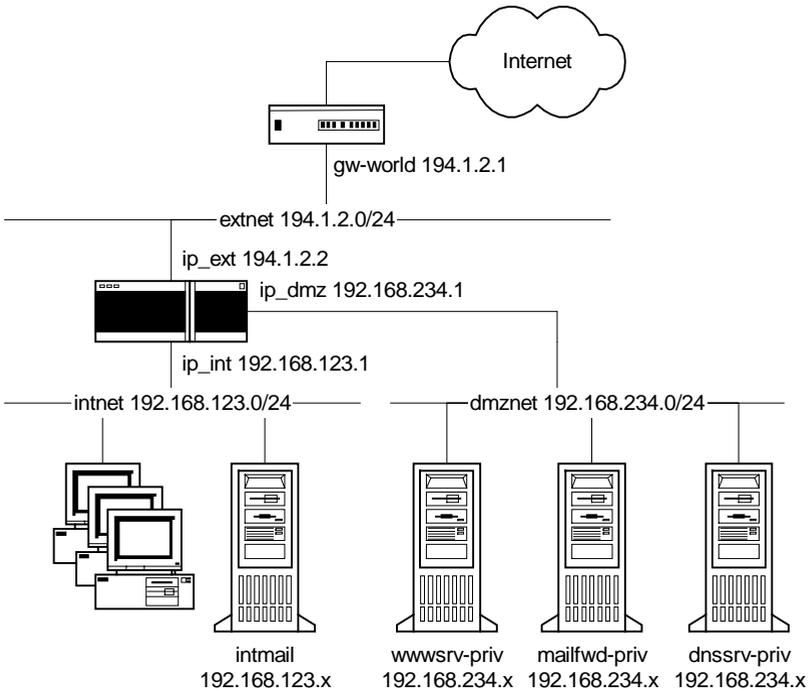
La regola 17 è necessaria poiché molti server FTP in Internet eseguono tentativi di apertura di connessioni verso il mittente quando vi si accede. La porta 113 è stata ideata per "ident daemon", che nei sistemi Unix consente al server di determinare l'utente locale che tenta la connessione. Se in questa posizione non è presente una regola Reject, tali server possono ritardare la connessione fino a un minuto nel tentativo di aprire una connessione verso la porta 113. La regola Reject predispose il firewall per la restituzione di un messaggio TCP RESET, il quale notifica immediatamente al server che la connessione alla porta 113 non sarà possibile e che la procedura di accesso proseguirà senza ritardi.

Commenti sulla configurazione

- Si consiglia di collocare il server Web in un'area DMZ.
 - Se il server di posta utilizzato offre altri servizi oltre a SMTP/POP3/IMAP4, ad esempio server Exchange, Notes o GroupWise, potrebbe essere necessario posizionarlo nella rete interna. In tali situazioni, il server nell'area DMZ dovrebbe essere invece un Mail Forwarder, che riceve la posta dall'esterno e la inoltra al server di posta interno. Per alcuni esempi, consultare la sezione Esempio 4: DMZ-MailFwd-DNS più avanti.
 - Potrebbe essere interessante creare un'area DMZ separata per il server di posta/sistema di inoltro invece di posizionarlo nella stessa DMZ del server Web. Il motivo è che il server Web è probabilmente più vulnerabile rispetto al server di posta per ciò che concerne le rispettive porte di comunicazione. Se un intruso indesiderato prende il controllo del server Web, avrebbe facilmente accesso al server di posta che si trova sulla stessa LAN. Questo non è il caso se il server di posta si trova in un'area DMZ separata.
 - Prima di consentire le connessioni a tutte le porte alte di un server FTP, è necessario determinare se esistono servizi di rete che possono riceverle. Nel caso in cui sono presenti, l'accesso a queste porte deve essere bloccato prima di consentire il traffico a tutte le altre porte alte.

8.5.4 Esempio 4: DMZ-MailFwd-DNS

Il modello di configurazione DMZ impiega su un firewall con tre interfacce. Un'interfaccia connessa al router esterno. La seconda connessa alla rete protetta cui sono collegati le workstation ed i server interni. La terza interfaccia connessa all'area demilitarizzata (DMZ, DeMilitarized Zone).



La zona DMZ contiene:

- Un server Web, wwwsrv-priv, con la porta 80 accessibile tramite un indirizzo pubblico, wwwsrv-pub. Nelle opzioni predefinite, l'indirizzo viene impostato come equivalente all'indirizzo IP esterno del firewall.
- Un server di posta, mailsrv-priv, con la porta 25 accessibile da un indirizzo pubblico, mailsrv-pub. Nelle opzioni predefinite, l'indirizzo viene impostato come equivalente all'indirizzo IP esterno del firewall.
- Un server DNS, dnssrv-priv, con la porta 53 accessibile tramite un indirizzo pubblico, dnssrv-pub. Nelle opzioni predefinite, l'indirizzo viene impostato come equivalente all'indirizzo IP esterno del firewall.

Descrizione della sezione Hosts

1	ip_int	192.168.123.1
2	br_int	192.168.123.255

È necessario sostituire l'indirizzo ip_int con l'IP relativo all'interfaccia interna del firewall. Sostituire l'indirizzo br_int con l'indirizzo broadcast della rete interna. L'indirizzo broadcast è il più alto della rete.

Gli indirizzi ip_int e br_int vengono utilizzati nella sezione Interfaces per configurare l'interfaccia "int".

3	ip_ext	194.1.2.2
4	br_ext	194.1.2.255

Apportare le modifiche descritte nelle istruzioni precedenti che verranno applicate all'interfaccia esterna del firewall. Questi indirizzi vengono forniti principalmente dal provider di servizi Internet (ISP, Internet Service Provider).

5	ip_dmz	192.168.234.1
6	br_dmz	192.168.234.255

Modificare in base alle istruzioni precedenti. Queste impostazioni si applicano solo all'interfaccia DMZ del firewall.

7	gw-world	194.1.2.1
---	----------	-----------

Questo è l'indirizzo del router più esterno e nella maggior parte dei casi viene fornito dal provider di servizi Internet (ISP, Internet Service Provider).

8	loghost	0.0.0.0
---	---------	---------

Dopo avere installato EnterNet FireWall Logger o un daemon syslog di terze parti, digitarne l'indirizzo in questa posizione.

L'indirizzo viene utilizzato nella sezione Loghosts perché il firewall disponga delle informazioni per l'invio dei dati di log.

Se si utilizza un destinatario syslog al posto di FireWall Logger, sarà necessario modificare il tipo di loghost nella sezione Loghosts.

9	wwwsrv-priv	0.0.0.0
10	mailfwd-priv	0.0.0.0
11	dnssrv-priv	0.0.0.0

Se si dispone di server Web, di posta o DNS con indirizzi privati che si desidera rendere accessibili pubblicamente, digitarne l'indirizzo in questa posizione. È possibile ovviamente specificare un unico indirizzo per i tre servizi se questi sono installati sullo stesso server.

Questi indirizzi vengono utilizzati dalle regole SAT nella sezione Rules per implementare la traduzione degli indirizzi statici rispettivamente nelle porte 80,25 e 53.

12	wwwsrv-pub	ip_ext
13	mailfwd-pub	ip_ext
14	dnssrv-pub	ip_ext

È inoltre possibile specificare gli indirizzi tramite i quali sono pubblicati i server Web e di posta. Utilizzando gli indirizzi predefiniti, i server Web e di posta saranno pubblicati tramite l'indirizzo IP esterno del firewall.

Questi indirizzi vengono utilizzati nella sezione Rules per implementare la traduzione dell'indirizzo statico e consentire la connessione, rispettivamente alle porte 80, 25 e 53.

Gli indirizzi sopra descritti vengono pubblicati automaticamente nella sezione ARP. Se questi vengono modificati in un indirizzo differente dall'IP esterno del firewall, sarà probabilmente necessario che questo risponda alle query ARP per tali indirizzi. In questo caso il traffico destinato a tali indirizzi sarà diretto al firewall. Se il traffico verso tali indirizzi era instradato comunque al firewall, gli indirizzi non saranno pubblicati. La pubblicazione ARP, che sia necessaria o meno, non provocherà alcun danno.

15	int-mail	0.0.0.0
----	----------	---------

Se il sistema di inoltro della posta che si trova nell'area DMZ sta per inviare la posta ad un server interno, l'opzione int-mail deve essere impostata in base all'indirizzo del server di posta interno.

16	dnsslave	0.0.0.0
----	----------	---------

Se esiste un server DNS secondario (backup) per l'area che si trova all'esterno dei propri uffici, l'opzione Dnsslave deve essere impostata in base all'indirizzo di quel server. Tale indirizzo viene utilizzato nella sezione Rules per consentire le connessioni TCP verso la porta 53 del server DNS. In genere, viene utilizzato il protocollo UDP per eseguire la query DNS. In base a tale configurazione, chiunque è autorizzato a farlo. Tuttavia, quando un server DNS secondario deve trasferire aree intere, viene utilizzato il protocollo TCP. In questa configurazione, l'accesso è limitato ad un singolo server esterno.

Descrizione della sezione Rules

L'insieme di regole di questo modello di configurazione può essere riassunto nel modo seguente:

- Consente tutte le connessioni originate dall'interno, tranne NetBIOS, tramite traduzione dinamica dell'indirizzo.
- Consente le comunicazioni NetBIOS dalla rete interna a DMZ, mediante traduzione dinamica dell'indirizzo.
- Consente l'accesso HTTP a un indirizzo pubblico che a sua volta viene tradotto staticamente in un server Web con indirizzo privato sulla rete DMZ.
- Consente l'accesso SMTP a un indirizzo pubblico, che a sua volta viene tradotto staticamente in un server di posta con indirizzo privato sulla rete DMZ.
- Consente le query DNS mediante UDP ad un indirizzo pubblico che a sua volta viene tradotto staticamente in un server DNS con indirizzo privato sulla rete DMZ.
- Consente il trasferimento dell'area DNS mediante TCP da un server DNS esterno specifico con la stessa procedura utilizzata per le query DNS, come descritto sopra.
- Consente ai server DNS che si trovano nell'area DMZ di comunicare con tutte le reti tranne quella interna. Gli altri server nell'area DMZ devono eseguire le proprie query DNS mediante il server DNS e non attraverso il firewall.
- Consente al sistema di inoltro della posta che si trova nell'area DMZ di comunicare mediante SMTP con tutte le reti tranne quella interna.
- Consente al sistema di inoltro della posta che si trova nell'area DMZ di comunicare con l'interfaccia DMZ del firewall mediante SMTP, che a sua volta esegue la traduzione statica dell'indirizzo verso il server di posta interno.

1	NAT	int	intnet	dmznet	Ports	ALL → 135-139
---	-----	-----	--------	--------	-------	---------------

La regola 1 autorizza le connessioni NetBIOS originate internamente verso un'area DMZ mediante traduzione dinamica dell'indirizzo. Questa regola esplicita è necessaria poiché le regole 2 e 3 che seguono bloccano tutte le connessioni NetBIOS.

Il motivo per cui vengono tradotti gli indirizzi delle connessioni interne all'area DMZ è che non si desidera rivelare la struttura della rete interna dei server presenti nell'area DMZ, per evitare che finiscano sotto il controllo di un utente indesiderato.

2	Drop	ANY	all-nets	all-nets	UDP	ALL → 137
3	Drop	ANY	all-nets	all-nets	Ports	ALL → 135-139

Le regole 2 e 3 consentono il blocco di tutte le comunicazioni NetBIOS ad eccezione di quelle consentite dalla regola 1. Come nell'esempio 1, la risoluzione del nome NetBIOS, porta 137 UDP, viene scartata senza essere registrata se si verifica molto spesso. D'altra parte, tutte le altre porte dell'intervallo 135-139, inclusa la porta 137 TCP, vengono registrate e bloccate.

4	SAT	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80 SetDest wwwsrv-priv 80
5	SAT	ANY	all-nets	mailfwd-pub/32	TCP	ALL → 25 SetDest mailfwd-priv 25
6	SAT	ANY	all-nets	dnssrv-pub/32	Ports	ALL → 53 SetDest dnssrv-priv 53

Le regole da 4 a 6 consentono di implementare la traduzione statica dell'indirizzo per la pubblicazione di server Web, di posta e DNS tramite indirizzi pubblici. Gli indirizzi pubblici vengono preimpostati nella sezione Hosts come equivalenti dell'indirizzo IP esterno del firewall. È comunque possibile trasformarli in altri indirizzi pubblici.



Notare che queste regole *non* consentono alcun passaggio di traffico. Quando viene soddisfatta una delle due regole, il firewall ricorda che la traduzione dell'indirizzo verrà eseguita successivamente, continuando a cercare una regola che consenta la connessione. In questa configurazione, le regole necessarie vanno da 8 a 12, a seconda delle circostanze.

7	Fwd	int	intnet	intnet	All	
---	-----	-----	--------	--------	-----	--

Questa regola consente al traffico proveniente dalla rete interna di ritornare alla rete interna utilizzando *l'inoltro del pacchetto senza stato*. In questa configurazione, il motivo dell'esistenza di questa regola non è molto evidente. Se si prende in considerazione però una rete più estesa in cui il firewall funziona da *gateway predefinito* per un gran numero di router interni, questa regola può risultare estremamente utile.

Nella maggior parte dei casi, tale regola diventa ancora più specifica autorizzando solo il traffico destinato all'indirizzo IP interno del firewall, UDP porta 999. Senza questa regola, non potrà funzionare l'amministrazione remota dalla rete interna.

8	NAT	int	intnet	all-nets	Std	
---	-----	-----	--------	----------	-----	--

La regola 8 consente la traduzione dinamica dell'indirizzo per tutto il traffico proveniente dalla rete interna verso l'esterno.

In questa regola sono comprese le connessioni interne agli indirizzi pubblici tramite i quali sono pubblicati il server Web e di posta. Le connessioni a questi indirizzi ne risultano tradotte dinamicamente, purché siano interne.

Il motivo per cui vengono tradotti gli indirizzi delle connessioni interne all'area DMZ è che non si desidera rivelare la struttura della rete interna dei server presenti nell'area DMZ, per evitare che finiscano sotto il controllo di un utente indesiderato.

Uno spiacevole effetto secondario è che i log nei server Web e di posta mostreranno che l'accesso è stato effettuato dall'interfaccia DMZ del firewall e non dai singoli indirizzi interni.

9	Allow	ANY	all-nets	wwwsrv-pub/32	TCP	ALL → 80
10	Allow	ANY	all-nets	mailfwd-pub/32	TCP	ALL → 25

Le regole 8 e 9 consentono l'accesso del traffico agli indirizzi pubblici del server Web e del sistema di inoltro della posta, rispettivamente porte 80 e 25. Gli indirizzi di destinazione saranno inoltre tradotti secondo le regole SAT descritte in precedenza.

11	Allow	ANY	all-nets	dnssrv-pub/32	UDP	ALL → 53
----	-------	-----	----------	---------------	-----	----------

La regola 11 consente di eseguire query DNS sulla porta 53 UDP dell'indirizzo pubblico del server DNS. Gli indirizzi di destinazione saranno inoltre tradotti secondo le regole SAT descritte in precedenza.

12	Allow	ANY	dnsslave/32	dnssrv-pub/32	TCP	ALL → 53
----	-------	-----	-------------	---------------	-----	----------

La regola 12 consente al server DNS secondario esterno di eseguire i trasferimenti dell'area DNS mediante la porta 53 TCP dell'indirizzo pubblico del server DNS. Queste comunicazioni vengono indirizzate in base alle regole SAT descritte sopra.

13	Drop	ANY	all-nets	intnet	All	
----	------	-----	----------	--------	-----	--

La regola 13 consente di bloccare tutto il traffico diretto alla rete interna, indipendentemente dall'utente. Il motivo di tale funzionamento è che le regole che seguono, che consentono varie forme di comunicazione da DMZ, non devono avere come effetto finale la connessione dell'interfaccia DMZ alla rete interna.

14	SAT	dmz	mailfwd-priv/32	ip_dmz/32	TCP	ALL → 25 SetDest int-mail 25
15	Allow	dmz	mailfwd-priv/32	ip_dmz/32	TCP	ALL → 25

La regola 14 consente di implementare la traduzione statica dell'indirizzo di connessioni SMTP dal sistema di inoltro della posta nell'area DMZ all'indirizzo privato del server di posta situati nella rete interna. Ciò rende il server di posta interno accessibile mediante indirizzo IP dell'interfaccia DMZ.

La regola 15 autorizza le connessioni tradotte nella regola 14.

La ragione per cui il server di posta interno viene reso accessibile mediante l'indirizzo IP dell'interfaccia DMZ sta nel fatto che, invece di consentire al sistema di inoltro della posta di connettersi direttamente al server di posta interno, la struttura della rete interna è nascosta dai server dell'area DMZ.

16	NAT	dmz	mailfwd-priv/32	all-nets	TCP	ALL → 25 SetSrc mailfwd-pub 0
----	-----	-----	-----------------	----------	-----	----------------------------------

La regola 16 consente al sistema di inoltro della posta di stabilire connessioni SMTP verso reti esterne. Su queste comunicazioni viene eseguita la traduzione dinamica dell'indirizzo, utilizzando un indirizzo pubblico del sistema di inoltro della posta come indirizzo del mittente.

17	NAT	dmz	dnssrv-priv/32	all-nets	Ports	ALL → 53
----	-----	-----	----------------	----------	-------	----------

La regola 17 consente al server DNS di eseguire query DNS verso reti esterne. Su queste comunicazioni viene eseguita la traduzione dinamica dell'indirizzo, utilizzando l'indirizzo pubblico del firewall come indirizzo del mittente.

18	Drop	dmz	all-nets	all-nets	All	
----	------	-----	----------	----------	-----	--

La regola 18 consente di bloccare tutte le altre comunicazioni dall'area DMZ e le registra con un avviso di alta priorità. In tal modo, è possibile attribuire una comunicazione inattesa dai server nell'area DMZ ad un'intrusione. Le comunicazioni autorizzate da questi server devono perciò essere limitate ad un valore minimo per aumentare la possibilità di scoprire tali attacchi e di rendere sempre più difficile l'accesso di un intruso alle altre parti del sistema.

19	Reject	ANY	all-nets	ip_ext/32	TCP	ALL → 113
20	Drop	ANY	all-nets	all-nets	All	

Le regole 17 e 18 non sono in relazione diretta con la protezione.

Il traffico che non soddisfa nessuna delle regole incluse nel set viene sempre scartato *senza essere registrato*. È per questo motivo che conviene aggiungere una regola finale che oltre a scartare il traffico lo registra.

- La regola 19 è necessaria poiché molti server FTP su Internet eseguono tentativi di apertura di connessioni verso il mittente quando vi si accede. La porta 113 è stata ideata per "ident daemon", che nei sistemi Unix consente al server di determinare l'utente locale che tenta la connessione. Se in questa posizione non è presente una regola Reject, tali server possono ritardare la connessione fino a un minuto nel tentativo di aprire una connessione verso la porta 113. La regola Reject predispose il firewall per la restituzione di un messaggio TCP RESET, il quale notifica immediatamente al server che la connessione alla porta 113 non sarà possibile e che la procedura di accesso proseguirà senza ritardi.

8.5.5 Esempio 5: DMZ-ProxyARP

Il modello di configurazione "DMZ-ProxyARP" si basa sul modello "DMZ". Questo modello presenta le stesse funzionalità di base, ma consente inoltre agli host DMZ di conservare gli stessi indirizzi e allo stesso tempo di non dover creare una rete router tra il router esterno e il firewall.

Ciò è possibile utilizzando la funzione Proxy ARP, che consente di "inserire" il firewall tra il router esterno e le reti protette senza dover apportare delle modifiche a router o a host nella zona demilitarizzata. Gli host nella rete interna, però, dovranno essere riconfigurati per poter utilizzare la nuova estensione dell'indirizzo privato IP.

Differenze:

- La rete "extnet" è scomparsa. Il firewall riceve l'informazione che esiste solo un indirizzo IP connesso direttamente all'adattatore di rete esterno: il router esterno.
- Il percorso extnet è sostituito da "gw-world/32".
- La funzione Proxy ARP viene utilizzata per pubblicare "gw-world" nel settore interno del firewall. In questo modo gli host DMZ non devono modificare il *gateway predefinito* nelle impostazioni di rete.
- Tutti gli indirizzi nella zona demilitarizzata vengono pubblicati mediante Proxy ARP nell'interfaccia esterna del firewall. In questo modo il router esterno non deve essere riconfigurato.
- Non è più necessario effettuare la traduzione dell'indirizzo della comunicazione ai server nella zona demilitarizzata, dal momento che sono accessibili mediante indirizzi pubblici.

8.5.6 Esempio 6: DMZ-Shared-Extnet

Il modello di configurazione "DMZ-Shared-Extnet" si basa sul modello "DMZ-Proxy", ma parte dal presupposto che il firewall esterno sia condiviso con altri clienti o server e che solo alcuni indirizzi siano instradati ai server nella zona demilitarizzata.

Ciò è possibile utilizzando la funzione Proxy ARP, che consente di "inserire" il firewall tra la rete esterna e le reti protette senza dover apportare delle modifiche a router o host nella zona demilitarizzata. Gli host nella rete interna, però, dovranno essere riconfigurati per poter utilizzare la nuova estensione dell'indirizzo privato IP.

Differenze:

- La sezione Routes presenta tre percorsi diversi verso la zona demilitarizzata, una per ciascun server. Tali percorsi vengono pubblicati mediante Proxy ARP nell'interfaccia esterna. In questo modo i server sono ancora accessibili pubblicamente.
- Il percorso "extnet" viene pubblicato nella zona demilitarizzata per consentire agli host di tale zona di conservare la propria configurazione.
- La sezione Access contiene la regola per ciascun server pubblico nella zona demilitarizzata.
- La sezione Rules consente la comunicazione NetBIOS con ciascun server pubblico nella zona demilitarizzata mediante regole diverse per ciascun server.

9. Auditing da EnterNet Firewall

Auditing, ovvero la capacità di monitorare le decisioni prese dal firewall, è una funzione vitale per i dispositivi di sicurezza di rete. EnterNet FireWall offre diverse opzioni per la registrazione delle attività.

EnterNet FireWall supporta tre tipi di auditing:

- log inviati a EnterNet FireWall Logger
- log inviati a destinatari syslog
- Visualizzazione dei log in tempo reale in FireWall Manager

I dati di log non vengono archiviati nel firewall. Nel momento in cui avviene una connessione, i dati di log vengono inviati immediatamente a tutti i loghost.

Il formato di log utilizzato da EnterNet FireWall Logger è estremamente dettagliato ed è l'unico formato supportato dallo strumento di analisi integrato del log di EnterNet FireWall Manager.

Il formato di log utilizzato per la registrazione ai syslog è adatto all'elaborazione e alla ricerca automatizzata e nei contesti in cui il syslog venga utilizzato da altre applicazioni di rete.

9.1 Cosa viene registrato da EnterNet FireWall?

EnterNet FireWall genera e invia dati di log a uno o più ricevitori di log in varie situazioni. Nel corso di questo capitolo ognuna di queste situazioni viene definita *evento* o *evento di log*.

Il caso più ovvio in cui EnterNet FireWall genera tali eventi è, naturalmente, quando il firewall è stato configurato per registrare pacchetti che corrispondono a regole specifiche oppure che non superano i controlli di coerenza.

Esistono comunque altre situazioni in cui EnterNet FireWall genera eventi. Nella tabella che segue vengono elencati i tipi, o *categorie*, più comuni di eventi e le informazioni incluse in ogni categoria. Molti eventi presentano inoltre un'analisi dei contenuti del pacchetto.

Eventi USAGE - Dati statistici periodici

Questo tipo di eventi viene inviato periodicamente e fornisce statistiche relative a connessioni e volume di traffico.

L'intervallo tra un evento e l'altro viene determinato dall'impostazione *UsageLogInterval* nella sezione Settings della configurazione del firewall.

Ciascun evento USAGE contiene le seguenti informazioni

Statistiche della connessione

<code>Connections closed</code>	Numero di connessioni chiuse nel periodo
<code>Connections opened</code>	Numero di connessioni aperte nel periodo
<code>Max connections</code>	Numero massimo di connessioni aperte in un dato momento nel periodo
<code>Min connections</code>	Numero minimo di connessioni aperte in un dato momento nel periodo
<code>Current connections</code>	Numero di connessioni aperte al momento dell'evento

Statistiche per interfaccia

<code>Bits in/sec</code>	Volume medio di traffico ricevuto dall'interfaccia al secondo
<code>Bits out/sec</code>	Volume medio di traffico inviato dall'interfaccia al secondo
<code>Packets in/sec</code>	Volume medio di pacchetti ricevuti dall'interfaccia al secondo
<code>Packets out/sec</code>	Volume medio di pacchetti inviati dall'interfaccia al secondo

Drops/sec

Numero medio di pacchetti scartati al secondo.

Eventi FWD

Questo tipo di eventi viene generato se l'auditing è stata attivato da una regola FwdFast nella sezione Rules oppure da una regola Accept nella sezione Access.

Eventi CONN

Questo tipo di eventi viene generato se l'auditing è stato attivato da una regola Allow o NAT nella sezione Rules.

Una volta stabilita la connessione viene generato un evento che include informazioni relative a protocollo, interfaccia di ricezione, indirizzo IP di origine, porta di origine, interfaccia di destinazione, indirizzo IP di destinazione e porta di destinazione.

Un secondo evento viene generato alla chiusura della connessione. Le informazioni incluse in questo evento sono le stesse presenti nell'evento inviato all'apertura, alle quali si aggiungono però le statistiche relative al traffico inviato e ricevuto.

Se previsto dall'impostazione LogConnections nella sezione Settings, viene inoltre visualizzato il contenuto del pacchetto.

Questi eventi possono includere anche informazioni relative alla traduzione statica dell'indirizzo.

Eventi DROP

Questo tipo di eventi può essere generato da varie funzioni del firewall. La fonte principale è probabilmente l'insieme di regole.

Le informazioni incluse nell'evento sono il nome della regola responsabile dell'eliminazione del pacchetto e del suo contenuto.

DROP: eventi LogOpenFails

Questo tipo di eventi viene generato spesso, di solito a causa del time out della connessione da parte del firewall mentre l'altra estremità continua ad inviare dati dopo la chiusura della connessione.

Tali pacchetti non vengono accettati per i motivi elencati di seguito.

- Il firewall non riconosce l'esistenza della connessione, dal momento che questa in precedenza è stata chiusa e cancellata. In base alla sezione Rules dovrebbe essere consentito il passaggio al pacchetto in arrivo, dal momento che la sua destinazione è la porta 80 del server Web pubblico. Quando il meccanismo di ispezione sullo stato analizza il pacchetto, rileva che il flag SYN non è attivo e che non è possibile aprire una nuova connessione.
- Una delle parti invia un messaggio di errore ICMP che viene (erroneamente) accettato dalla sezione Rules. I messaggi di errore ICMP non consentono mai di aprire nuove connessioni e vengono quindi bloccati dal meccanismo di ispezione sullo stato.
- È in atto un tentativo di eseguire una scansione invisibile dei server e/o del firewall inviando pacchetti TCP senza averne attivato il flag SYN. In questo caso verranno registrate più o meno simultaneamente numerose voci di log relative ad un elevato numero di porte.

Eventi NETCON

Gli eventi NETCON vengono generati nel momento in cui gli amministratori effettuano la connessione al firewall per controllarlo o visualizzare le statistiche in remoto.

9.2 EnterNet FireWall Logger

EnterNet FireWall Logger viene eseguito come servizio su una workstation Windows NT o Windows 2000. Sono in preparazione degli adattamenti per poter eseguire il firewall logger sotto vari linguaggi Unix. Il servizio riceve dati UDP da EnterNet FireWall sulla porta 999.

I dati vengono quindi ordinati e salvati con una struttura gerarchica, nella quale ciascun firewall è rappresentato da una singola directory. I file di registro sono in formato binario per consentire una analisi più rapida.

9.2.1 Installazione di FireWall Logger

9.2.1.1 Dove installare FireWall Logger

EnterNet FireWall Manager viene utilizzato come interfaccia utente per tutte le operazioni FireWall Logger, compresa la configurazione e l'analisi dei dati di log. In questo modo il computer e la directory in cui è installato FireWall Logger devono essere accessibili mediante la condivisione di file Windows dalle workstation di gestione che devono avere accesso ai log. È possibile consentire la scrittura selettivamente in base a ogni singolo utente. Per il file "fwlogger.cfg" questa proprietà deve essere assegnata agli amministratori che gestiscono il ricevitore di log.

Notare che solo il canale NetBIOS deve essere unidirezionale, ovvero Firewall Logger può essere installato su un server in una zona demilitarizzata, con regole di firewall che consentono l'accesso ai file condivisi NetBios dalle reti interne.

9.2.1.2 Installazione del servizio

Inserire il CD di EnterNet FireWall nel computer dal quale verrà eseguito FireWall Logger, ovvero la macchina a cui EnterNet FireWall invierà i dati di log. Il software di installazione si avvierà automaticamente.

In caso contrario, selezionare **Run** dal menu di avvio e digitare `D:\setup.exe` (dove `D`: rappresenta la lettera dell'unità CD-ROM).

Selezionare l'installazione di FireWall Logger e seguire le istruzioni sullo schermo.

Una volta completata l'installazione, la procedura guidata avvierà automaticamente il servizio.

È necessario sottolineare che FireWall Logger, come tutti i servizi di Windows NT, non può essere installato mediante una condivisione in rete, ma solo su dischi rigidi locali. Questo perché i servizi solitamente vengono eseguiti come utenti locali senza accesso alle risorse di rete.

9.2.1.3 Maggiore sicurezza locale per FireWall Logger

Per una maggiore sicurezza nella rete locale, si consiglia di adottare le misure necessarie per proteggere il sistema di registrazione dagli accessi non autorizzati.

Le impostazioni per il servizio EnterNet FireWall Logger devono venire modificate in modo che possa essere eseguito come utente locale con diritti minimi di accesso al resto del sistema. In Logger sono necessarie le autorizzazioni in scrittura solo nella gerarchia della directory locale dove vengono archiviati i log.

Si consiglia di proteggere la directory che contiene il file eseguibile di Firewall Logger in modo che solo gli utenti autorizzati possano avere accesso ai file in essa contenuti.

9.2.2 Configurazione di EnterNet FireWall Logger

La configurazione di FireWall Logger viene effettuata mediante EnterNet FireWall Manager.

Tutte le impostazioni di configurazione vengono salvate in un file denominato *fwlogger.cfg*, che risiede nella directory di installazione di FireWall Logger. Il file viene generato automaticamente con impostazioni predefinite al momento dell'installazione di FireWall Logger, ma in seguito dovrà essere configurato utilizzando EnterNet FireWall Manager.

Il file non deve essere modificato manualmente.

9.2.2.1 Collegamento a FireWall Logger

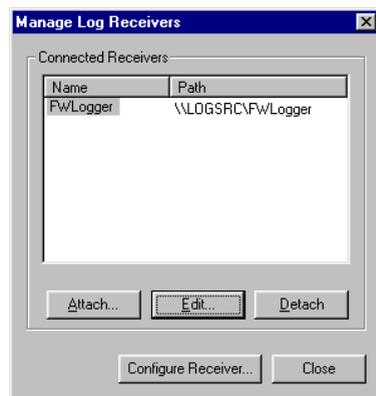
Avviare EnterNet FireWall Manager.

Dalla barra dei menu selezionare **Log** e quindi **Manage Log Receivers**.

In questo modo si apre una finestra di dialogo da utilizzare per effettuare il collegamento alla gestione di un numero qualsiasi di FireWall Logger. Inizialmente l'elenco **Connected Receivers** sarà vuoto.

Scegliere il pulsante **Attach**.

Digitare un nome simbolico per il nuovo FireWall Logger nel campo **Name** della finestra di dialogo.



Il percorso digitato nel campo **Path** viene utilizzato da FireWall Manager per individuare la directory di installazione di FireWall Logger. È bene sottolineare ancora una volta che questo percorso deve possedere le proprietà di scrittura e lettura per potere configurare il ricevitore di log.

Ad esempio, se FireWall Logger è installato su un server denominato *LOGSRV* in una directory condivisa come *FWLogger*, il percorso da digitare è *\\LOGSRV\FWLogger*. Naturalmente può essere utilizzata anche la notazione "X:\Directory" nel caso in cui la condivisione sia già stata mappata.

9.2.2.2 Configurazione del ricevitore

Per evitare di ricevere dati di log imprevisti o dannosi, ciascun firewall configurato per inviare dati di log a un EnterNet FireWall Logger deve essere autorizzato nella configurazione di quello specifico FireWall Logger.

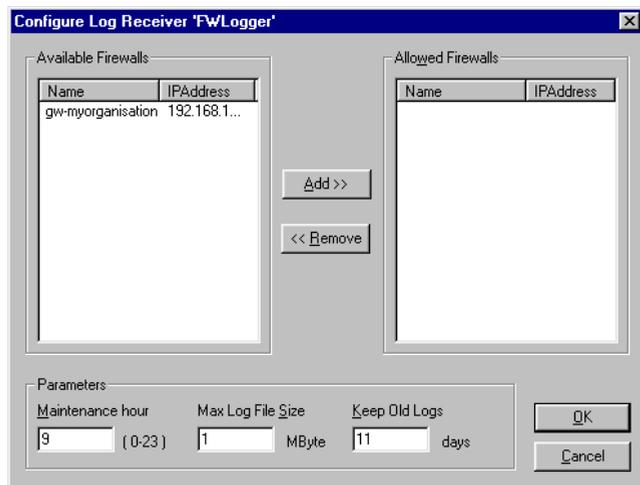


I dati di log provenienti da un firewall non specificato nella configurazione verranno respinti. Questi tentativi vengono riassunti nel log degli eventi del server ogni 10 minuti.

Selezionare il Firewall Logger da configurare dall'elenco dei ricevitori connessi.

Scegliere il pulsante **Configure Receiver**.

In questo modo si apre la finestra di dialogo sottostante:



Le impostazioni presenti in questa finestra di dialogo influiscono direttamente sul comportamento in funzione di FireWall Logger. Dopo avere modificato le impostazioni non è necessario riavviare Logger, dal momento che il servizio controlla di continuo il file di configurazione per rilevare eventuali modifiche.

La parte superiore destra della finestra di dialogo controlla quali sono i firewall autorizzati ad inviare log a questo specifico FireWall Logger. L'elenco **Available Firewalls** visualizza tutti i firewall presenti nel database di gestione che non sono stati ancora autorizzati a comunicare con questo specifico FireWall Logger.

L'elenco **Allowed Firewalls** contiene tutti i firewall accettati da questo FireWall Logger.

Per assegnare un firewall disponibile a questo Logger, selezionare il firewall dall'elenco **Available Firewalls** e fare clic su **Add**.

Per rimuovere un firewall, selezionarlo dall'elenco **Allowed Firewalls** e fare clic su **Remove**.

Notare che in entrambi gli elenchi sono consentite selezioni multiple.



Nel caso in cui l'IP mittente di un firewall sia diverso quando comunica con un ricevitore di log e quando comunica con la workstation di gestione, è necessario modificare l'indirizzo IP autorizzato a comunicare con FireWall Logger. Per effettuare tale modifica fare doppio clic sulla voce relativa nell'elenco **Allowed Firewalls** e modificare l'indirizzo IP nella finestra di dialogo che si apre. Questo procedimento è valido anche per i firewall i cui IP sono stati modificati.

La sezione **Parameters** della finestra di dialogo viene utilizzata per controllare le funzioni amministrative di FireWall Logger. Queste impostazioni possono essere lasciate immutate.

Il campo **Maintenance hour** indica l'ora in cui FireWall Logger è stato programmato per eseguire le operazioni di manutenzione. Queste operazioni includono la compressione dei file di registro, la rimozione di vecchi file di registro e così via.

Nel campo **Max Log File Size** vengono indicate le dimensioni massime di un singolo file di log. Quando un file di log supera il limite prefissato, viene archiviato e sostituito da un file vuoto.

Firewall Logger conserva i file di log per il numero di giorni indicato dall'impostazione **Keep Old Logs**. Al momento della manutenzione giornaliera, i file che superano il limite di giorni consentito vengono eliminati.

9.2.2.3 Avvio e arresto di FireWall Logger

Il servizio viene avviato e arrestato utilizzando il pannello di controllo Service del computer sul quale è stato installato FireWall Logger.

In Windows NT 4.0:

Scegliere il menu **Start**.

Scegliere **Settings -> Control Panel**.

Fare doppio clic sull'icona **Services**.

Per fermare FireWall Logger, selezionare la riga che contiene "EnterNet FireWall Logger" e fare clic su **Stop**.

Per avviare FireWall Logger, selezionare la riga che contiene "EnterNet FireWall Logger" e fare clic su **Start**.

9.3 Strumento di analisi dei log

Lo strumento di analisi dei log è un programma integrato in FireWall Manager utilizzato per effettuare ricerche e query rapide nei dati di log ricevuti da EnterNet FireWall Logger.

Questo strumento consente di ottenere rapidamente e in maniera semplice una panoramica degli eventi del firewall generati nel corso di un determinato periodo. Sono inoltre presenti funzioni di filtro che consentono di isolare eventi interessanti in base a parametri specifici.

Lo strumento di analisi dispone di un sistema avanzato di analisi dei pacchetti che può essere utilizzato per visualizzare e analizzare il contenuto dei pacchetti che portano alla generazione degli eventi di log.

Per rendere lo strumento di analisi estremamente flessibile, viene utilizzato un linguaggio di query denominato E-SQL, ovvero un adattamento del linguaggio SQL effettuato da Enternet. Questo linguaggio di query è molto simile a quello utilizzato in SQL per le query dei database, anche se presenta caratteristiche specifiche per i firewall. Per ulteriori informazioni su E-SQL, consultare la sezione, 9.4, Riferimenti E-SQL.

È possibile digitare query E-SQL direttamente nello strumento di analisi, ma è disponibile anche una procedura guidata intuitiva che può essere utilizzata per le query meno avanzate.

Lo strumento di analisi dei log viene attivato dal menu **Log** di EnterNet FireWall Manager.

Dalla barra dei menu scegliere **Log** e quindi fare clic su **Query Log Receiver**.

In questo modo si apre una finestra simile a quella sottostante.



La parte inferiore della finestra presenta tre schede da utilizzare per alternare le tre diverse visualizzazioni dello strumento: **Results**, **Wizard** ed **E-SQL**.

9.3.1 Visualizzazione Wizard

Questo wizard è utilizzato come procedura guidata per creare in modo semplice una query di log selezionando le origini e i filtri appropriati dai menu a discesa. Altre righe vengono aggiunte automaticamente al momento dell'inserimento dei dati nella procedura guidata.

È possibile eliminare e aggiungere manualmente righe utilizzando il pulsante destro del mouse o il menu **Logger** dalla barra dei menu.

9.3.1.1 Definizione delle sorgenti dei log

In questa sezione sorgenti, della procedura guidata, vengono specificati i firewall e il periodo di tempo per ciascun firewall a cui si riferisce ad una query.



Dal menu a discesa sulla sinistra selezionare il firewall per cui si desidera effettuare una query. Nel menu sono elencati tutti i firewall definiti come **Allowed Firewalls** nella sezione **Configure Receiver** della configurazione di FireWall Logger.

Il menu a discesa al centro offre quattro alternative per la definizione del periodo di tempo:

- Selezionare **Times** per inserire un intervallo di tempo nelle due caselle di testo vuote sulla destra. È necessario indicare le date nel formato standard ISO, ovvero aaaa-mm-gg HH:MM:SS, interrotto in qualunque punto. Ad esempio, se si desidera è possibile omettere la parte relativa all'ora del giorno.
- Scegliere **Last days** per limitare la ricerca agli ultimi n giorni, dove n è indicato nella casella di testo sulla destra.
- Selezionare **Last full days** per ottenere una ricerca simile alla precedente, con la differenza che la ricerca comincia all'inizio di un determinato giorno e include solo gli eventi fino alle 23:59:59 di ieri.
- Selezionare **Last hours** per limitare la ricerca alle ultime n ore, dove n è indicato nella casella di testo sulla destra.
- Selezionare **Last full hours** per ottenere una ricerca simile alla precedente, con la differenza che la ricerca comincia all'inizio di una determinata ora, in maniera simile all'opzione "full days".

Sui dati di log dei vari firewall è possibile eseguire query simultanee, aggiungendo più righe alla sezione Source.

9.3.1.2 Definizione di filtri sugli eventi

La sezione **Filter** fornisce funzioni che includono o escludono le voci dei log che corrispondono a determinati criteri.



The screenshot shows a 'Filter' configuration window with three rows of criteria. Each row has a dropdown menu for 'Exclude/Include', a dropdown for a parameter name, a dropdown for an operator, and a text input field for the value.

Exclude/Include	Parameter	Operator	Value
Include	srcip	IN	192.168.123.5
Include	category	=	DROP
Include	srcip	IN	

Il menu a discesa sulla sinistra consente di determinare se includere o escludere una voce di log che corrisponde ai criteri indicati nella riga.

Il secondo menu a discesa consente di specificare i parametri dei filtri. Per ulteriori informazioni sui vari parametri, consultare la sezione, 9.4, Riferimenti E-SQL.

Il terzo menu a discesa consente di determinare l'operatore da utilizzare nel caso di filtro basato sui parametri specificati in precedenza.

Il menu a discesa sulla destra permette di specificare i criteri.

La query viene eseguita selezionando **Run Query** dal menu **Logger** sulla barra dei menu (o nel menu che appare facendo clic con il pulsante destro del mouse), oppure premendo **Ctrl-E**. Se non vengono rilevati errori di sintassi, la query ha inizio e si apre una finestra nella quale viene visualizzato l'avanzamento della ricerca.

La visualizzazione **Results** viene aperta automaticamente una volta terminata la ricerca.

Le schermate di seguito mostrano due esempi diversi di query.

The screenshot shows the LogQuery - FWLogger application window. The 'Source' section has two rows, both with 'Source' set to 'gw-myorganisati'. The first row has 'Last days' set to '5'. The 'Filter' section has four rows: 'Exclude/Include' set to 'Include', 'category' set to 'DROP'; 'Exclude/Include' set to 'Include', 'ipproto' set to 'TCP'; 'Exclude/Include' set to 'Include', 'destport' set to '137'; and 'Exclude/Include' set to 'Include', 'srcip' set to 'IN'. At the bottom, there are tabs for 'Results', 'Wizard', and 'E-SQL'.

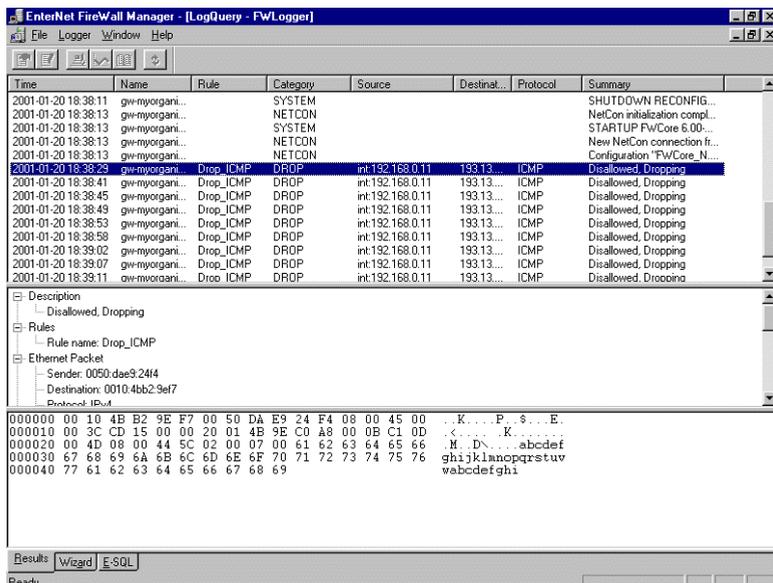
Query di esempio: Le impostazioni descritte nell'esempio eseguiranno una query che cercherà nei file di registro del firewall gw-nomeazienda gli eventi di log ricevuti nel corso degli ultimi 5 giorni. La ricerca include solo gli eventi registrati a causa di pacchetti scartati e destinati alla porta TCP 137.

The screenshot shows the LogQuery - FWLogger application window. The 'Source' section has two rows: the first with 'Source' 'gw-sample1' and 'Times' '2000-06-01' to '2000-07-01'; the second with 'Source' 'gw-sample2' and 'Times' '2000-06-01' to '2000-07-01'. The 'Filter' section has two rows: 'Exclude/Include' set to 'Include', 'syn' set to '1'; and 'Exclude/Include' set to 'Include', 'urg' set to '1'. At the bottom, there are tabs for 'Results', 'Wizard', and 'E-SQL'.

Query di esempio: Le impostazioni descritte nell'esempio eseguiranno una query che cercherà nei file di registro dei firewall gw-sample1 e gw-sample2 gli eventi di log ricevuti tra il 2000-06-01 e il 2000-07-01. Verranno inclusi solo gli eventi registrati a causa di uso illegale delle flag TCP SYN e URG.

9.3.2 Visualizzazione Results

La visualizzazione **Results** mostra i risultati di una precedente ricerca e può essere utilizzata anche per creare determinati tipi di query basate sui risultati. La visualizzazione è divisa in tre sezioni, ciascuna con un diverso livello di dettagli e contenuti.



La visualizzazione Results, divisa in tre sezioni separate con diversi livelli di dettagli.

La sezione superiore visualizza tutti gli eventi di log che fanno parte dei risultati della ricerca, ordinati in base alla data dal più vecchio al più recente.

Time	Name	Rule	Category	Source	Destinat...	Protocol	Summary
2001-01-20 18:38:11	gw-myorgani...		SYSTEM				SHUTDOWN RECONFIG...
2001-01-20 18:38:13	gw-myorgani...		NETCON				NetCon initialization compl...
2001-01-20 18:38:13	gw-myorgani...		SYSTEM				STARTUP FWCore 6.00...
2001-01-20 18:38:13	gw-myorgani...		NETCON				New NetCon connection fr...
2001-01-20 18:38:13	gw-myorgani...		NETCON				Configuration "FwCore_N...
2001-01-20 18:38:45	gw-myorgani...	Drop_ICMP	DROP	int:192.168.0.11	192.13...	ICMP	Disallowed, Dropping
2001-01-20 18:38:41	gw-myorgani...	Drop_ICMP	DROP	int:192.168.0.11	192.13...	ICMP	Disallowed, Dropping
2001-01-20 18:38:45	gw-myorgani...	Drop_ICMP	DROP	int:192.168.0.11	192.13...	ICMP	Disallowed, Dropping
2001-01-20 18:38:45	gw-myorgani...	Drop_ICMP	DROP	int:192.168.0.11	192.13...	ICMP	Disallowed, Dropping

Le colonne visualizzate sono, da sinistra a destra:

- Data e ora dell'evento
- Nome del firewall in cui si è registrato l'evento
- Il nome della regola che ha generato questa voce di log
- Categoria dell'evento. Per un elenco delle categorie e descrizioni, consultare la sezione, 9.4, Riferimenti E-SQL.
- L'origine del pacchetto che ha generato l'evento. Vengono visualizzate informazioni diverse sull'origine a seconda del tipo di pacchetto:
 - Per pacchetti TCP o UDP: *interfaccia, indirizzo IP e porta*
 - Per altri pacchetti IP: *interfaccia e indirizzo IP*
 - Per pacchetti ARP: *interfaccia e indirizzo MAC*
- La destinazione del pacchetto che ha generato l'evento. Le informazioni visualizzate dipendono dal tipo di pacchetto, come descritto in precedenza.
- Il protocollo del pacchetto che ha generato l'evento.
- Un breve riepilogo dell'evento

Selezionando un determinato evento ne verrà evidenziata la riga e nelle due sezioni inferiori della visualizzazione verranno mostrate informazioni dettagliate relative all'evento.



Nella sezione centrale della visualizzazione dei risultati vengono visualizzate informazioni dettagliate relative ad un evento.

Le informazioni vengono visualizzate con un struttura ad albero. Ulteriori dettagli possono essere visualizzati espandendo i rami dell'albero contrassegnati dal simbolo "+".

Se si seleziona un evento che contiene un dump di pacchetto, come un evento DROP, nella sezione superiore della visualizzazione dei risultati, la sezione inferiore visualizza un dump di byte dei primi 150 byte del pacchetto scartato. Il dump viene visualizzato in formato esadecimale.

```

000000 00 10 4B E2 9E F7 00 50 DA E9 24 F4 08 00 45 00  . .K . . P . $ . . E .
000010 00 3C CD 15 00 00 20 01 4B 9E C0 A8 00 0B C1 0D  < . . . . . K . . . . .
000020 00 4D 08 00 44 5C 02 00 07 00 61 62 63 64 65 66  . M . DN . . . . . abcdef
000030 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76  ghijklmnopqrstuv
000040 77 61 62 63 64 65 66 67 68 69  wabdefghi

```

Dump a byte esadecimale di un pacchetto che ha avviato un evento di log.

Come detto all'inizio della presente sezione, la visualizzazione dei risultati può essere utilizzata anche per creare determinati tipi di query basate sui risultati di una query precedente.

Questo è possibile facendo doppio clic su un evento specifico nella sezione superiore della visualizzazione. L'evento selezionato deve disporre delle informazioni relative a sorgente e destinazione. Selezionare **New Query** dal menu visualizzato e quindi selezionare una delle alternative dal sottomenu.

Viene quindi aperto un nuovo strumento di query, nel quale è preimpostata una query con l'indirizzo selezionato e un intervallo di tempo che va da un'ora prima a un'ora dopo l'evento registrato.

9.3.3 Visualizzazione E-SQL

La visualizzazione E-SQL consente di scrivere manualmente query utilizzando E-SQL. Il vantaggio maggiore deriva dalla possibilità di creare query molto più avanzate rispetto a quelle che si ottengono utilizzando la visualizzazione Wizard.

Come accade anche nella visualizzazione Wizard, la query viene eseguita selezionando **Run Query** dal menu **Logger** sulla barra dei menu oppure premendo **Ctrl-E**.

Tutte le query eseguite in precedenza vengono visualizzate nella sezione **Old E-SQL queries** della visualizzazione E-SQL, che include anche quelle generate dalla visualizzazione Wizard. È possibile riutilizzare queste query facendo clic su di esse con il pulsante destro del mouse e selezionando Copy, quindi incollandole nella sezione query di E-SQL.

Nota: le query create con la visualizzazione Wizard possono essere mostrate nella visualizzazione E-SQL, mentre le query scritte manualmente nella visualizzazione E-SQL non possono essere mostrate nella visualizzazione Wizard. Passando alla visualizzazione Wizard verranno mostrate le impostazioni dell'ultima query generata da Wizard.

9.4 Riferimenti E-SQL

E-SQL, acronimo di EnterNet Structured Query Language, è il linguaggio di query utilizzato per effettuare le ricerche nei log. In termini di formato e sintassi E-SQL è molto simile al linguaggio SQL tradizionale utilizzato come linguaggio di query nei sistemi di database. Naturalmente E-SQL presenta numerose parole chiave e istruzioni specifiche per EnterNet FireWall.

La sintassi fondamentale di una query E-SQL è la seguente:

```
SELECT <outputtype> [, <outputtype>]  
FROM <firewall_and_time_statement>  
[WHERE <logical_statement>]
```

Ogni query E-SQL deve iniziare con la parola chiave SELECT.

Dopo SELECT vengono specificati uno o più tipi di output (consultare la sezione Tipi di output) separati da una virgola. Lo strumento integrato di analisi dei log si attende dati binari non elaborati, quindi utilizzare "SELECT BINARY" per le query nel riquadro E-SQL del visualizzatore dei log.

Dopo la parola chiave FROM vengono specificate una o più istruzioni di firewall e di ora (consultare la sezione Istruzioni di firewall e di ora).

È possibile specificare come opzione la parola chiave WHERE seguita da un'istruzione logica.

Operatori logici

Gli operatori logici possono essere utilizzati all'interno dell'istruzione WHERE. Attualmente sono supportati i seguenti operatori logici:

AND

OR

NOT

Gli operatori logici hanno la stessa priorità degli equivalenti di C/C++. L'utilizzo di parentesi attorno all'espressione può modificarne la priorità.

Esempio:

```
srcip = '10.0.0.1' and (destip = '192.168.123.1' or  
destip = '192.168.123.2')
```

Operatori di comparazione

Gli operatori di comparazione vengono utilizzati per confrontare le variabili con i valori specificati dall'utente. Sono supportati i seguenti operatori:

=

>=

<=

>

<

IN (range expression)

Tutti i valori specificati dall'utente devono essere riportati entro i caratteri '.

Esempio:

```
srcip = '10.0.0.1' and destip = '192.168.123.1'  
srcip IN (10.0.0.1 - 10.0.0.255) and destip IN  
(192.168.123.1 - 192.168.123.255, 1.2.3.4)
```

Variabili predefinite

Nelle istruzioni logiche è possibile utilizzare numerose variabili predefinite.

Nella seguente tabella sono elencate le variabili attualmente definite

Variabile	Tipo di valore	Descrizione
Srcip	Indirizzo IPv4	Indirizzo IP sorgente in formato: a.b.c.d
Destip	Indirizzo IPv4	Indirizzo IP di destinazione
Srcenet	Indirizzo Ethernet	Indirizzo Ethernet sorgente
Destenet	Indirizzo Ethernet	Indirizzo Ethernet di destinazione
Category	Stringa	Categoria dell'evento registrato Esempio: SYSTEM, NETCON, USAGE, CONN, DROP
Srcport	PAROLA	Porta sorgente (da 0 a 65535)
Destport	PAROLA	Porta di destinazione (da 0 a 65535)
Ipproto	BYTE	Protocollo IP (da 0 a 255 o il nome) Esempio: TCP, UDP, ICMP, 99
Recviface	Stringa	Nome dell'interfaccia di ricezione Esempio: ext, int, dmz
Destiface	Stringa	Nome dell'interfaccia di destinazione
Icmptype	Stringa	Tipo di messaggio ICMP (da 0 a 255) Esempio: ECHO_REQUEST
Icmsrcip	Indirizzo IPv4	Indirizzo IP sorgente in pacchetto IP incapsulato ICMP
Icmpdestip	Indirizzo IPv4	Indirizzo IP di destinazione in pacchetto IP incapsulato ICMP
Icmsrcport	PAROLA	Porta sorgente (da 0 a 65535) in pacchetto IP incapsulato ICMP

Icmpdestport	PAROLA	Porta di destinazione (da 0 a 65535) in pacchetto IP incapsulato ICMP
icmpproto	Stringa	Protocollo IP (da 0 a 255) in pacchetto IP incapsulato ICMP
description	Stringa	Descrizione dell'evento
Fin	Booleano	Flag TCP FIN (0 o 1)
Syn	Booleano	Flag TCP SYN
rst	Booleano	Flag TCP RST
psh	Booleano	Flag TCP PSH
ack	Booleano	Flag TCP ACK
urg	Booleano	Flag TCP URG
xmas	Booleano	Flag TCP XMAS
ymas	Booleano	Flag TCP YMAS
enetproto	PAROLA	Numero di protocollo Ethernet (da 0 a 65535)
rule	Stringa	Nome della regola
satsrcrule	Stringa	Nome regola di origine SAT
satdestrule	Stringa	Nome regola di destinazione SAT
enet[index]	BYTE	Valore a [index] byte oltre l'intestazione Ethernet
ip[index]	BYTE	Valore a [index] byte oltre l'intestazione IP
tcp[index]	BYTE	Valore a [index] byte oltre l'intestazione TCP
udp[index]	BYTE	Valore a [index] byte oltre l'intestazione UDP

Tipi di output

Vari tipi di output definiti vengono utilizzati nella definizione dei dati che la query deve restituire.

Tutti i tipi di output restituiscono dati in solo testo, tranne il tipo *binario* che restituisce i dati nel formato binario utilizzato dallo strumento di query. Il tipo di output binario è *l'unico* tipo di output consentito quando si utilizza lo strumento di analisi delle query e non può essere combinato con i tipi di output in solo testo.

Sono definiti i seguenti tipi di output:

Nome	Descrizione
Binary	Output in formato binario utilizzato solo all'interno dello strumento di query
Srcip	Indirizzo IP sorgente
Destip	Indirizzo IP di destinazione
Srcport	Porta sorgente
Destport	Porta di destinazione
Srcenet	Indirizzo Ethernet sorgente
Destenet	Ethernet di destinazione
Ihl	Lunghezza dell'intestazione IP
Idl	Lunghezza dei dati IP
Itl	Lunghezza totale IP (dati e intestazione)
Udl	Lunghezza dei dati UDP
Utl	Lunghezza totale dei dati UDP
Firewall	Nome del firewall che ha inviato i dati
Time	L'ora in cui è avvenuto l'evento
Recviface	Interfaccia di ricezione
Destiface	Interfaccia di destinazione
Ttl	Campo Time To Live nell'intestazione IP

date	La data in cui il pacchetto ha raggiunto il Firewall Logger
description	Descrizione dell'evento
arp	Tipo di pacchetto ARP
arpdesthw	Indirizzo hardware di destinazione negli eventi ARP
arpsrchw	Indirizzo hardware sorgente negli eventi ARP
ipproto	Protocollo IP
icmptype	Tipo ICMP
icmproip	IP sorgente in pacchetto IP incapsulato ICMP
icmprodestip	IP di destinazione in pacchetto IP incapsulato ICMP
icmproport	Porta sorgente di pacchetto UDP/TCP incapsulato ICMP
icmprodestport	Porta di destinazione di pacchetto UDP/TCP incapsulato ICMP
icmproipproto	Protocollo IP di pacchetto IP incapsulato ICMP
tcpflags	Flag TCP
enetproto	Protocollo Ethernet
usage	Throughput dell'interfaccia
connusage	Statistiche della connessione
rule	Nome della regola a cui corrisponde questa voce di log
satsrcrule	Nome della regola di origine SAT a cui corrisponde questa voce di log
satdestrule	Nome della regola di destinazione SAT a cui corrisponde questa voce di log
origsent	Volume di dati inviati dal mittente (lato client) della connessione
termsent	Volume di dati inviati dal terminatore (lato server) della connessione
conn	Tipo di evento conn

Istruzione di firewall

Le istruzioni di firewall vengono utilizzate per specificare il firewall per il quale cercare gli eventi di log.

La sintassi dell'istruzione di firewall è.

```
<firewall> [, <firewall>] [<time_statement>] [ AND  
<firewall> [, <firewall> ] [<time_statement>]]
```

Istruzione di ora

L'istruzione di ora viene utilizzata per specificare l'intervallo di tempo per i dati richiesti.

Un'istruzione di ora può essere una delle seguenti:

```
TIMES yyyy-mm-dd HH:MM:SS TO yyyy-mm-dd HH:MM:SS  
LAST DAYS n  
LAST FULL DAYS n  
LAST HOURS n  
LAST FULL HOURS n
```

(dove n è un valore numerico compreso tra 1 e 1000)

Se viene utilizzata l'istruzione TIME, ora e data devono venire specificate nel formato standard ISO, come descritto in precedenza e che può essere interrotto in qualunque punto, ad esempio "TIMES 2000-01 TO 2000-02" è un'istruzione valida.

9.5 Log inviati a destinatari syslog

EnterNet FireWall può inviare dati di log a destinatari syslog. Syslog è un protocollo standard per l'invio dei dati di log a loghost, sebbene non esista un formato standardizzato di tali messaggi. Il formato utilizzato da EnterNet FireWall è adatto ad operazioni automatiche di elaborazione, filtro e ricerca.

Nonostante il formato esatto di ogni voce di log dipenda dal funzionamento del destinatario syslog, spesso sono molto simili. Inoltre, anche la lettura dei log dipende dal funzionamento del destinatario syslog. Un daemon syslog su server Unix generalmente legge i log come file di testo, riga per riga.

La maggior parte dei destinatari syslog premettono ad ogni voce di log un indicatore di data e ora, nonché l'indirizzo IP della macchina che ha inviato i dati di log:

```
Feb 5 2000 09:45:23 gateway.ourcompany.com
```

Segue il testo scelto dal mittente. Tutte le voci di log provenienti da EnterNet FireWall sono precedute da "EFW:" e da una categoria, ad esempio "DROP:".

```
Feb 5 2000 09:45:23 gateway.ourcompany.com EFW: DROP:
```

Il testo che segue dipende dall'evento registrato.

Per facilitare l'elaborazione automatica di tutti i messaggi, EnterNet FireWall trascrive tutti i dati di log in un'unica riga di testo. Tutti i dati che seguono il testo iniziale vengono presentati nel formato *name=value*. In questo modo i filtri automatici possono trovare facilmente i valori cercati senza dover presupporre che un determinato dato si trovi in una certa posizione nella voce di log.

I nomi e i valori utilizzati negli eventi syslog sono più o meno uguali a quelli presenti nelle espressioni E-SQL di FireWall Logger. Per ulteriori informazioni, consultare la sezione, 9.4, Riferimenti E-SQL.

9.6 Visualizzazione Real-Time dei Log

EnterNet FireWall Manager consente di visualizzare in tempo reale i messaggi di log provenienti dai firewall selezionando il firewall desiderato e scegliendo **Realtime Log** dal menu **FireWall**.

Questo formato degli eventi log presentato nel visualizzatore dei log è un ibrido dei formati di FireWall Logger e syslog, dal momento che vengono visualizzate frasi in cui viene descritto il motivo che ha causato un evento, mentre i dump di pacchetto e le descrizioni delle connessioni vengono registrati nel formato syslog.

Il visualizzatore in tempo reale non può mostrare i messaggi di log meno recenti, ma solo quelli che giungono nel momento in cui il visualizzatore è attivo.



La visualizzazione Real-Time Log comunica tramite la stessa connessione crittografata utilizzata da altre funzioni di gestione remota. Per questo i FireWall Manager che desiderano visualizzare in tempo reale i dati di log *non* devono necessariamente comparire nell'elenco dei ricevitori di log nella sezione di configurazione Loghosts.

10. Configurazione del traffico

Prima di iniziare, sono necessarie alcune precisazioni. Modellare il traffico, limitare e garantire la larghezza di banda è **difficile**. Non è possibile aggiungere in un secondo tempo qualità di servizio ad una rete, ma è necessario invece pianificare accuratamente e comprendere che diversi tipi di traffico necessitano di diversi tipi di controllo, per poter elaborare un buon piano per implementare la QoS (Quality of Service, qualità del servizio) in una rete.

Il sistema di configurazione del traffico su EnterNet FireWall offre uno strumento eccezionale per l'implementazione di QoS.

Si tenga presente che le dimensioni del presente Manuale utente probabilmente raddoppierebbero se venissero trattati anche i vari contesti e le strategie di QoS. In questa sede, invece, viene approfondito il funzionamento, dal punto di vista tecnico, di EnterNet FireWall e vengono forniti alcuni esempi che illustrano il normale utilizzo delle funzioni di configurazione del traffico.

Verranno ora esaminati nel dettaglio gli strumenti presenti su EnterNet FireWall che consentono di implementare QoS.

10.1 Premessa

Uno dei maggiori inconvenienti del protocollo TCP/IP è la mancanza di una reale funzionalità QoS. Nelle reti, QoS (Quality of Service) indica la capacità di garantire e limitare la larghezza di banda per determinati servizi e utenti.

Sebbene esistano protocolli come DiffServ e altre soluzioni che hanno come scopo quello di offrire QoS nelle grandi reti, nessuna di queste ha raggiunto uno standard sufficientemente elevato per l'utilizzo su vasta scala.

Inoltre, la maggior parte delle soluzioni QoS è basata sulle applicazioni, ovvero funziona mediante applicazioni che forniscono alla rete le informazioni QoS. Dal punto di vista della sicurezza, naturalmente, è inaccettabile che le applicazioni (ovvero gli utenti) decidano la priorità del proprio traffico in una rete. Nei contesti in cui la sicurezza riveste una particolare importanza e nei quali non è possibile dare fiducia agli utenti, solo l'hardware di rete deve avere la possibilità di decidere in merito a priorità e allocazioni della larghezza di banda.

I punti elencati consentono di comprendere il motivo per cui sia quasi impossibile ordinare in base alla priorità e garantire una limitazione del traffico nelle reti vaste e complesse nelle quali coesistono standard e prodotti differenti. Un esempio di questo genere di topologia di rete è Internet.

Al contrario, in reti delimitate, esistono ottime possibilità di utilizzare diversi metodi per il controllo del traffico. Una rete delimitata è definita per la maggior parte da limiti amministrativi e non dalle sue dimensioni. Il traffico in una rete MAN (Metropolitan Area Network) e persino in una rete WAN (Wide Area Network) potrebbe essere gestito in maniera ottimale a patto che la rete sia stata progettata in maniera omogenea.

EnterNet FireWall offre funzionalità QoS applicando limiti e garanzie al traffico di rete invece di lasciare che siano le applicazioni e gli utenti ad effettuare queste scelte. Per tale motivo risulta adatto per la gestione della larghezza di banda di una piccola rete LAN (Local Area Network) e in uno o più punti di congestione nelle grandi reti MAN o WAN.

10.1.1 Nozioni di base su Traffic Shaping

Il modo più semplice per ottenere QoS in una rete, sia dal punto di vista della sicurezza che della funzionalità, è affidare ai componenti di rete, non alle applicazioni, il compito di controllare il traffico in determinati punti di congestione.

Traffic shaping si ottiene misurando e accodando i pacchetti IP in transito rispetto a vari parametri configurabili. È possibile creare valori limite della velocità e garanzie di traffico differenziate in base alla sorgente, alla destinazione ed ai parametri di protocollo nello stesso modo in cui vengono implementate le regole sui firewall. Traffic shaping consente di:

- Applicare limiti di larghezza di banda accodando i pacchetti che superano i limiti stabiliti nella configurazione e inviandoli in seguito quando la larghezza di banda necessaria è inferiore.
- Scartare pacchetti se i buffer del pacchetto sono pieni. È consigliabile scegliere il pacchetto da scartare tra quelli che causano la “congestione”.
- Ordinare il traffico in base alla priorità a seconda delle scelte dell’amministratore. Se il traffico ad alta priorità aumenta quando la linea è occupata, è necessario limitare momentaneamente il traffico a bassa priorità per lasciare spazio al traffico ad alta priorità.
- Offrire garanzie di larghezza di banda. Ciò è possibile se si considera ad elevata priorità un determinato volume di traffico (il volume garantito), mentre il traffico che supera la garanzia ha la stessa priorità di “tutto il resto del traffico”, ovvero deve competere con il resto del traffico non ordinato in base alla priorità.

Una buona implementazione di traffic shaping generalmente non accoda elevati volumi di dati per poi ordinare il traffico in base alla priorità ed inviarlo prima del rimanente traffico, ma cerca di misurare il volume di traffico ordinato in base alla priorità e quindi limita quello rimanente in modo che non interferisca con il flusso di traffico ordinato in base alla priorità.

EnterNet FireWall dispone di un modulo di traffic shaping flessibile e integrato nel software del firewall. Dal momento che il firewall è una parte centrale e vitale della rete, si possono ottenere numerosi vantaggi affidando al firewall il controllo del traffico.

Il modulo di traffic shaping di EnterNet FireWall ha le seguenti caratteristiche:

Basato su pipe

La gestione del traffico in EnterNet FireWall viene gestita con un concetto basato su "pipe", nel quale ogni pipe ha varie capacità di ordinamento in base alla priorità, di limitazione e di raggruppamento. È possibile concatenare i singoli pipe in vari modi per creare unità di gestione della larghezza di banda con capacità decisamente superiori a quelle di un solo pipe.

Piena integrazione con l'insieme di regole del firewall

Ciascuna regola del firewall può essere assegnata singolarmente a uno o più pipe.

Ordinamento del traffico in base alla priorità e limitazione della larghezza di banda

Ogni pipe presenta vari livelli di priorità, ciascuno dei quali con un proprio limite di larghezza di banda specificato in kilobit per secondo e/o pacchetti per secondo. E' possibile inoltre specificare il limite complessivo del pipe.

Raggruppamento

È possibile raggruppare automaticamente il traffico che attraversa un pipe in "utenti di pipe" e ciascun utente di pipe, o "pipe di utente", può essere configurato con gli stessi parametri del pipe principale.

È possibile raggruppare il traffico in base a vari parametri, ad esempio rete IP, indirizzo IP o porta di origine o destinazione.

Bilanciamento dinamico della larghezza di banda

È possibile utilizzare il modulo di traffic shaping per il bilanciamento dinamico dell'allocazione della larghezza di banda di diversi utenti di pipe se l'intero pipe ha superato i propri limiti.

Ciò significa che la larghezza di banda disponibile viene bilanciata in maniera uniforme in base al raggruppamento scelto per il pipe.

Concatenazione dei pipe

È possibile concatenare sino ad otto pipe assegnati a regole, in modo da gestire filtri e limitazioni in maniera estremamente complessa.

Garanzie di traffico

Grazie a una configurazione di pipe corretta è possibile utilizzare la modellazione del traffico in EnterNet FireWall per *garantire* la larghezza di banda (e quindi la qualità) per il traffico che attraversa il firewall.

Integrazione IPsec

Se si utilizza il modulo opzionale VPN IPsec nel firewall, è possibile configurare larghezza di banda e priorità per i tunnel VPN e per le regole comuni del firewall.

10.2 Configurazione del traffico su Enternet FireWall

Le operazioni di misurazione, limitazione, garanzia e bilanciamento vengono eseguite nei *pipe*. Un *pipe* in sé, però, non ha alcun significato se non viene attivato nella sezione Rules. Ciascuna regola può consentire il passaggio di traffico attraverso uno o più *pipe* in base a una determinata precedenza (priorità).

Per configurare il traffico è necessario effettuare i seguenti passaggi.

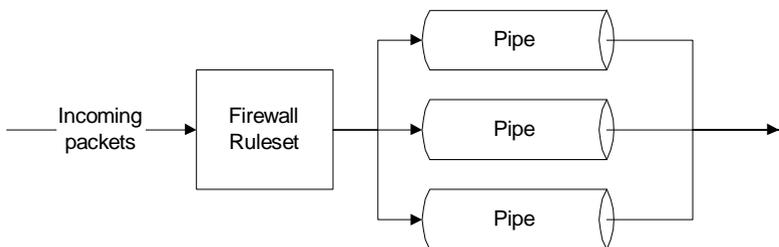
- *Pianificare* i requisiti di traffic shaping. È probabile che il processo di configurazione risulti non particolarmente chiaro se non si è a conoscenza di come limitare, ordinare in base a priorità, garantire o distribuire il traffico.
- Nella sezione Pipes configurare i pipe che descrivono le diverse classi di traffico.
- Nella sezione Rules assegnare tipi specifici di comunicazione ai vari pipe. Ciò potrebbe portare ad un aumento dell'insieme di regole. È probabile che una regola che in precedenza stabiliva "NAT everything from the inside out" debba essere estesa a numerose regole che utilizzano diversi limiti o priorità per diversi protocolli e/o porte.
- Verificare che la configurazione scelta funzioni nella maniera desiderata. Due opzioni consentono di capire cosa realmente accade nel proprio ambiente attivo: Il comando "pipes" (per ulteriori informazioni consultare la Guida in linea nella sezione "Pipes") e il grafico Pipes nella visualizzazione delle statistiche.

10.2.1 Nozioni di base sui pipe

Il *Pipe* è uno dei concetti fondamentali della funzionalità di traffic shaping dell'EnterNet FireWall ed è alla base del controllo della larghezza di banda. I pipe vengono configurati nella sezione Pipes del firewall. Consultare la sezione 7.3.5, Scheda Pipes.

I pipe sono piuttosto semplici, dal momento che non contengono informazioni sul tipo di traffico che li attraversa né sulla sua direzione. Un pipe si limita a misurare il traffico che lo attraversa e ad applicare i limiti configurati in ciascuna precedenza e/o gruppo di utenti.

Il traffico di rete in entrata viene prima filtrato dall'insieme di regole del firewall e quindi viene inviato al pipe indicato nella regola corrispondente. Nel pipe il traffico viene limitato in base alla configurazione dello stesso e viene quindi inoltrato alla sua destinazione o al pipe successivo in una concatenazione.



EnterNet FireWall è in grado di gestire contemporaneamente centinaia di pipe, ma in realtà la maggior parte delle configurazioni ne richiede solo pochi. L'unico caso in cui possono risultare necessari molti pipe sono i contesti in cui vengono creati pipe individuali per ciascun servizio (protocollo o client nei casi ISP)

10.2.1.1 Gestione della larghezza di banda

L'utilizzo più comune del pipe è la creazione di controlli della larghezza di banda. Si tratta inoltre dell'unico contesto in cui non è necessaria una pianificazione particolarmente complessa.

Nel primo esempio che segue viene applicato un limite di larghezza di banda in una sola direzione, ovvero quella del traffico in entrata, che generalmente crea i maggiori problemi in una connessione a Internet.

Si consideri la creazione di un pipe con le seguenti caratteristiche:

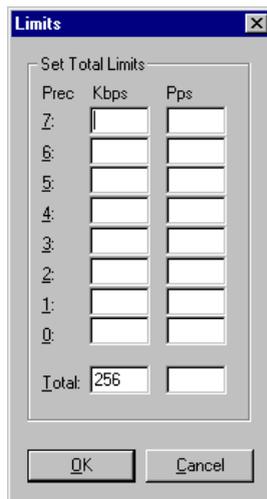
	Name	Min...	Def...	Max...	Grouping	Net ...	Total Limits	Per-User Limits	Dyn...	Comments
1	std-in	0	0	7	None		Total: 256Kb			
2		0	0	7	None					

In questo modo viene creato un pipe molto semplice che limita tutto il traffico che lo attraversa a 256 kilobit per secondo, indipendentemente dal tipo di traffico.

I limiti basati sulla priorità verranno trattati in seguito. Per il momento, *tutto* il traffico che attraversa il pipe viene limitato a 256 kbps.

Tuttavia, la sola creazione di un pipe non porta a grandi risultati, dal momento che è necessario consentire il passaggio del traffico *attraverso* il pipe. Per questo bisogna assegnare i pipe nella colonna Pipes della sezione Rules.

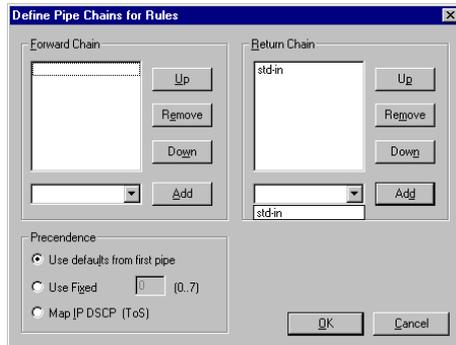
Il pipe indicato nell'esempio verrà utilizzato per limitare il traffico in entrata, ovvero i *pacchetti* e non le connessioni. Ciò che è realmente importante nella gestione del traffico è la direzione in cui viene spostato il traffico e non il computer che ha avviato la connessione.



Viene creata una semplice regola che consente il passaggio di tutti gli elementi dall'interno verso l'esterno:

	Action	Pipes	Src If...	Source Net	Dest If...	Dest Net	Proto	Ports/Params
1	Allow	Ret: std-in...	int	intnet	ext	all-nets	Standard	
2								

Il pipe creato è stato aggiunto alla *concatenazione di ritorno*. In questo modo i pacchetti che si spostano nella *direzione di ritorno* di questa connessione devono attraversare il pipe "std-in".



Con questo tipo di configurazione viene limitato tutto il traffico proveniente dall'esterno (da Internet) a 256 kilobit per secondo, come se una connessione Internet a 256 kbps rappresentasse il collo di bottiglia. Non è stata applicata alcuna priorità o bilanciamento dinamico.

10.2.1.2 Controllo bidirezionale della larghezza di banda

La configurazione esaminata nel precedente esempio limita la larghezza di banda solo per il traffico in entrata. Questa scelta è stata dettata dal fatto che, nella maggior parte delle configurazioni, la direzione in entrata è la prima a riempirsi. Se si desidera limitare la larghezza di banda in entrambe le direzioni,

è necessario applicare il limite di 256 kbps anche nella direzione di inoltro. Vediamo come.



Inserire "std-in" nella concatenazione di inoltro **non sortisce alcun effetto**, o almeno non gli effetti voluti, soprattutto se si desidera che i 256 kbps del traffico in uscita siano separati da quelli del traffico in entrata.

Questa soluzione non può funzionare perché i pipe, che sono estremamente semplici, consentono il passaggio di soli 256 kbps di traffico. Se si aggiunge il passaggio di 256 kbps di traffico in uscita ai 256 kbps di traffico in entrata, si raggiunge un totale di 512 kbps. Dal momento che il limite è di 256 kbps, si ottengono 128 kbps in entrambe le direzioni.

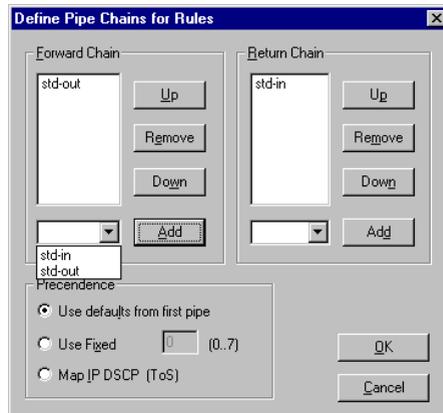
Tuttavia non è possibile elevare semplicemente il limite totale a 512 kbps e sperare che funzioni. Perché? Bisogna ricordare che i pipe sono semplici. Un pipe non è in grado di comprendere che si desiderano 256 kbps in entrata e 256 kbps in uscita, per cui si potrebbero ottenere 64 kbps in uscita e 448 kbps in entrata, dal momento che il totale è comunque di 512 kbps.

Per poter controllare correttamente la larghezza di banda in entrambe le direzioni è necessario utilizzare *due* pipe, uno per il traffico in entrata e uno per il traffico in uscita, entrambi con un limite di 256 kbps.

	Name	Min...	Def...	Max...	Grouping	Net...	Total Limits	Per-User Limits	Dyn...	Comments
1	std-in	0	0	7	None		Total: 256Kb			
2	std-out	0	0	7	None		Total: 256Kb			
3		0	0	7	None					

Una volta creato il pipe per il controllo della larghezza di banda in uscita, è sufficiente aggiungerlo alla concatenazione di pipe di inoltro della regola creata nell'esempio precedente.

In questo modo tutte le connessioni in uscita saranno limitate a 256 kbps in entrambe le direzioni e si otterrà un risultato molto simile a una normale connessione Internet a 256 kbps.



Naturalmente è anche possibile utilizzare un solo pipe per entrambe le direzioni, se si desidera un totale di 256 kbps divisi indifferentemente tra dati di inoltro e dati di ritorno. Esistono connessioni Internet di questo tipo, ma generalmente si acquista la stessa quantità di larghezza di banda in entrambe le direzioni, in modo che il flusso di dati in una direzione non influenzi quello dell'altra.

10.2.1.3 Utilizzo di concatenazioni per la creazione di limiti differenziati

Negli esempi precedenti è stato applicato un limite di traffico statico per tutte le connessioni in uscita. Se si desidera limitare maggiormente l'esplorazione del Web rispetto al resto del traffico, è necessario configurare due pipe "surf", uno in entrata ed uno in uscita. Tuttavia è probabile che il traffico in uscita non debba essere limitato in maniera consistente, dal momento che l'esplorazione consiste generalmente di brevi richieste in uscita seguite da lunghe risposte in entrata.

Si proceda quindi alla creazione di un solo pipe speciale "surf" per il traffico in entrata:

	Name	Min...	Def...	Max...	Grouping	Net ...	Total Limits	Per-User Limits	Dyn...	Comments
1	std-in	0	0	7	None		Total: 256Kb			
2	std-out	0	0	7	None		Total: 256Kb			
3	surf-in	0	0	7	None		Total: 128Kb			
4		0	0	7	None					

Una volta definito il pipe è necessario configurare un insieme di regole relative all'esplorazione e porle prima della regola relativa a tutto il resto del traffico. In questo modo è possibile consentire il passaggio del traffico di esplorazione attraverso i pipe desiderati, ma lasciare che tutto il resto del traffico venga gestito dai pipe predefiniti creati in precedenza.

	Action	Pipes	Src If...	Source Net	Dest If...	Dest Net	Proto	Ports/Params
1	Allow	Fwd: std-o...	int	intnet	ext	all-nets	TCP	ALL -> 80
2	Allow	Fwd: std-o...	int	intnet	ext	all-nets	Standard	
3								

Copiare le impostazioni della concatenazione di inoltro dalla regola relativa a tutti i protocolli "Standard".

Ora è necessario consentire il passaggio del traffico di ritorno attraverso il pipe "surf-in" definito in precedenza.

Come prima cosa, si può provare a consentire il passaggio del traffico di esplorazione attraverso il pipe "surf-in" nella concatenazione di ritorno.

Sfortunatamente, però, questo non consentirà di ottenere gli effetti desiderati.

In questo modo si ottiene il passaggio del traffico in entrata attraverso due pipe, uno che inoltra 256 kbps e l'altro che inoltra 128 kbps, per un totale di 384 kbps di traffico in entrata.

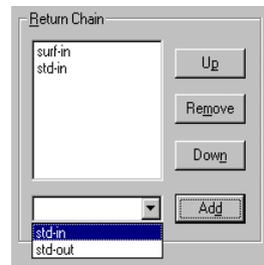
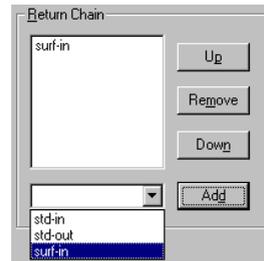
Per limitare il traffico di esplorazione a 128 kbps senza dover riconfigurare i limiti totali è sufficiente consentire il passaggio di tale traffico in entrata anche attraverso il pipe std-in.

In questo modo, il traffico di esplorazione in entrata passa prima attraverso il pipe "surf-in", che lo limita a 128 kbps, *quindi* viene fatto passare attraverso il pipe "std-in" insieme al resto del traffico in entrata, raggiungendo il limite totale di 256 kbps. Perciò, se l'esplorazione occupa 128 kbps di larghezza di banda, quei 128 kbps occupano metà del pipe std-in, lasciando solo 128 kbps per il resto del traffico, soluzione che probabilmente soddisfa maggiormente l'utente.

Se non è in corso alcuna attività di esplorazione, tutti i 256 kbps a cui è consentito il passaggio attraverso il pipe std-in sono disponibili per il resto del traffico.

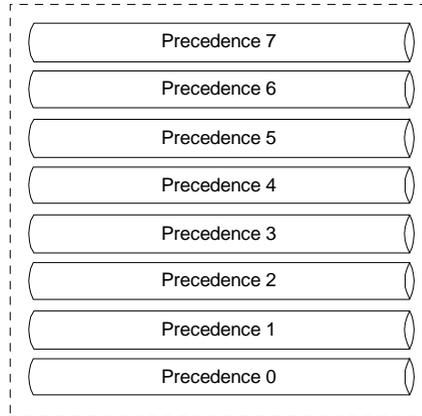


Notare tuttavia che *non* si tratta di una garanzia di traffico per l'esplorazione del Web. Potrebbe essere considerata come una garanzia di traffico da 128 kbps per tutti gli elementi *tranne* l'esplorazione del Web, anche se in quest'ultimo caso la competizione per la larghezza di banda segue la normale regola "first-come, first-served". È *possibile* poter raggiungere i 128 kbps, ma potrebbe anche trattarsi dell'equivalente di un modem a 2400 baud se la connessione è intasata.



10.2.2 Precedenze

Ogni pipe contiene otto *precedenze*, o livelli di priorità, numerati da 0 a 7. Ciascuna precedenza può essere considerata come una coda separata nella quale è possibile controllare il traffico di rete. La precedenza 0 è la precedenza di minore importanza, mentre la precedenza 7 è quella di maggiore importanza.



Le rispettive precedenze non hanno alcun carattere "speciale". Il loro significato viene definito esclusivamente dai limiti e dalle garanzie configurate. L'unica differenza è nell'importanza relativa, dal momento che al traffico con precedenza 1 viene consentito il passaggio prima del traffico con precedenza 0, al traffico con precedenza 2 prima del traffico con precedenza 1 e così via.

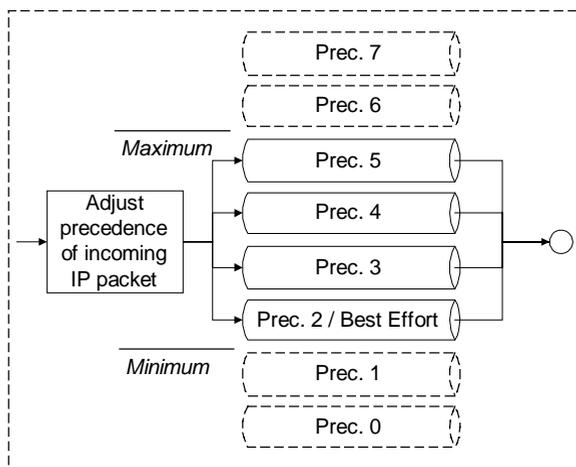
Per determinare a quale precedenza appartenga il traffico di rete, viene assegnato un numero di precedenza a ciascun buffer a pacchetto prima di venire inviato a un pipe. La sezione Rules controlla la precedenza assegnata. In questo modo è possibile ordinare il traffico per priorità in base a estensione IP, numero di protocollo, numero di porta e così via, allo stesso modo in cui normalmente viene filtrato il traffico. Questo argomento verrà comunque trattato in maniera più approfondita nel seguito del capitolo.

Una volta configurato il pipe, è possibile definire il numero di precedenze nel pipe indicando una *precedenza minima* (*Minimum precedence*) e una *precedenza massima* (*Maximum precedence*). I pacchetti in entrata vengono regolati automaticamente dal pipe in modo che siano rispettati tali limiti. Se la priorità di un pacchetto è troppo bassa, viene adeguata alla precedenza minima, viceversa se è troppo alta. Se un pacchetto non ha precedenza, viene assegnata la *precedenza predefinita* (*Default precedence*).

La limitazione della larghezza di banda viene eseguita all'interno di ciascuna precedenza. È possibile specificare limiti diversi di larghezza di banda per ciascuna precedenza. Tali limiti saranno espressi in kilobit per secondo e/o in pacchetti per secondo.



La precedenza indicata come minima ha un ruolo particolare nel pipe, dal momento che agisce da precedenza di *massimo carico*. **Il traffico che supera il limite della precedenza più elevata viene automaticamente trasferito nella precedenza di massimo carico**, a patto che tale precedenza possa accogliere ancora traffico.



Pipe definito con precedenza minima 2 e precedenza massima 5.

Come mostra questo esempio, oltre al limite in base alla precedenza è possibile definire un limite per l'intero pipe. Quando la larghezza di banda totale nel pipe raggiunge il limite totale, il traffico viene ordinato in base alla priorità a seconda della precedenza a cui appartiene. Il traffico con precedenza più elevata ha maggiori possibilità di attraversare il pipe senza la necessità di essere accodato. Tuttavia, se si utilizzano solo due precedenze, scegliere 6 e 7 piuttosto che 0 e 1 oppure 0 e 7 non comporta alcuna differenza. Una precedenza ha significato solo in relazione al traffico a cui è consentito il passaggio nelle altre precedenze e non a fattori esterni quali, ad esempio, il traffico nella LAN esterna al firewall o all'altra estremità della connessione Internet.

10.2.2.1 Gestione delle priorità

Vediamo come utilizzare le precedenze per rendere determinati tipi di traffico più importanti di altri. Si riprenda l'esempio precedente, assegnando al traffico SSH e telnet una priorità più elevata rispetto al rimanente traffico che attraversa i pipe.

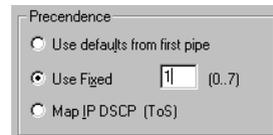
Per questo primo esempio non è necessario aggiungere o modificare nulla nella sezione Pipes. Innanzitutto viene aggiunta una regola relativa al traffico SSH e telnet:

	Action	Pipes	Src If...	Source Net	Dest If...	Dest Net	Proto	Ports/Params
1	Allow	Fwd: std-o...	int	inrnet	ext	all-nets	TCP	ALL -> 22-23
2	Allow	Fwd: std-o...	int	inrnet	ext	all-nets	TCP	ALL -> 80
3	Allow	Fwd: std-o...	int	inrnet	ext	all-nets	Standard	
4								

Copiare le impostazioni del pipe dalla regola "Standard".

Le precedenze erano già state impostate su "Use defaults from first pipe". Questo significa che la regola non prevede l'applicazione di una precedenza specifica, ma lascia che sia la configurazione del primo pipe in ciascuna concatenazione a decidere.

Le precedenze predefinite di tutti i pipe configurati sino ad ora corrispondono a 0, perciò, per ordinare il traffico in base alla priorità, è necessario predisporre la regola per il passaggio del pacchetto alla concatenazione di pipe con una precedenza più elevata, ad esempio 1.



Grazie a questa configurazione è possibile ordinare il traffico SSH e telnet in base alla priorità prima di tutti gli altri tipi di traffico. Grazie a questi due protocolli a flusso debole, l'operazione non presenta alcun problema.

Tuttavia, se si trattasse di audio in tempo reale, probabilmente la larghezza di banda disponibile verrebbe interamente utilizzata dai flussi audio e non ne rimarrebbe altra per esplorazione, DNS, FTP e tutti gli altri protocolli.

10.2.2.2 Suggestimenti sulla configurazione delle priorità e larghezza di banda

Prima di proseguire con la serie di esempi parlando di larghezza di banda garantita, raggruppamento e bilanciamento dinamico, è necessario soffermarsi su alcuni importanti punti da ricordare.

Le garanzie non servono solo a "garantire". Il traffico garantito ordinato in base alla priorità funziona *limitando* tutto ciò che *non* è ordinato in base alla priorità. Come vengono calcolati questi limiti? In ogni pipe, i limiti delle priorità più basse vengono calcolati sottraendo al limite totale il flusso corrente di precedenze più elevate.

Questo ha molte più implicazioni di quanto si potrebbe pensare a prima vista. Se si ha la necessità di impostazioni più avanzate dei limiti semplici, si consiglia di leggere attentamente i seguenti punti.

Impostazione di un limite totale

La larghezza di banda nelle precedenze più basse non viene regolata finché attraverso il pipe non passa tutto il traffico stabilito dal limite totale. D'altronde, per quale motivo regolarla prima di quel momento. Se si dispone di un pipe di 512 kbps attraverso il quale avviene il passaggio di 400 kbps di traffico a bassa priorità e 100 kbps di traffico ad elevata priorità, non c'è motivo di regolare nulla, dal momento che rimangono liberi ancora 12 kbps di larghezza di banda.

Per conoscere il limite da applicare alle precedenze più basse, quindi, è necessario conoscere il limite totale del pipe

I limiti totali non possono superare la larghezza di banda disponibile per la connessione

Se si imposta come limite di pipe un valore superiore alla larghezza di banda realmente disponibile, il pipe non si renderà mai conto che la connessione non ha più spazio disponibile. Se si dispone di una connessione a 512 kbps ma i limiti totali di pipe sono impostati a 600 kbps, il pipe non rileverà che la connessione è piena e quindi non regolerà le precedenze più basse.

Gestione del traffico all'ingresso di un punto di congestione

Se si protegge "l'ingresso" di un collo di bottiglia della rete, ad esempio i dati in uscita dal firewall, è possibile impostare il limite totale in modo che corrisponda approssimativamente alla larghezza di banda della connessione.

Gestione del traffico all'uscita di un punto di congestione

Se si protegge "l'uscita" di un collo di bottiglia della rete, ad esempio i dati in entrata dal firewall, probabilmente è necessario impostare il limite in modo che risulti inferiore alla larghezza di banda della connessione. Impostare i limiti in modo che corrispondano esattamente alla larghezza di banda in entrata comporta però due rischi:

- Nell'ipotesi peggiore, si potrebbero avere alcuni pacchetti per secondo vaganti che consumano una frazione della larghezza di banda della connessione. Di conseguenza i pipe non rilevano di aver raggiunto il limite.
- Esiste inoltre il rischio molto più concreto che gli adeguamenti impieghino troppo tempo, dal momento che il pipe rileva solo un "leggero" sovraccarico. Se il sovraccarico è leggero verranno effettuati solo piccoli adeguamenti e per questo l'adattamento alle distribuzioni delle nuove precedenze può avvenire molto lentamente, a volte addirittura in mezzo minuto.



Naturalmente esiste anche il rischio di sovraccarico della connessione. Dal momento che la gestione del traffico riguarda l'uscita del collo di bottiglia, non si ha il controllo su ciò che vi entra. Se la gestione riguarda normali TCP, il modulo di gestione del traffico non incontrerà grossi problemi e anche se i client interni sollecitano la connessione inviando ACK, o altro, non otterranno grossi risultati, dal momento che il modulo di gestione del traffico continua ad accodare i pacchetti destinati a loro.

La gestione del traffico all'uscita di un collo di bottiglia, però, *non* protegge dalle violazioni che provocano esaurimento delle risorse, quali DDoS o altri intasamenti. In caso di bombardamento di traffico, può verificarsi un sovraccarico della connessione e la gestione del traffico, in questo caso, non può intervenire. Naturalmente impedisce ai pacchetti estranei di raggiungere i computer situati dietro al gestore del traffico, ma *non* può proteggere la connessione e se questa viene intasata il pirata informatico ha vinto.

Alcuni provider di servizi Internet consentono il co-posizionamento, perciò, se l'intasamento diventa un rischio concreto, può essere necessario prendere in considerazione la possibilità di posizionare la gestione del traffico nell'estremità Internet della connessione.

Per garantire la larghezza di banda è necessario conoscere sempre la larghezza di banda disponibile.

Affinché la gestione del traffico funzioni correttamente, è necessario conoscere la larghezza di banda che attraversa il punto di congestione che si deve proteggere.

Se si condivide la connessione Internet con altri utenti o server che *non* vengono controllati dal firewall, è praticamente impossibile garantire, ordinare in base alla priorità o bilanciare la larghezza di banda, dal momento che il firewall non è in grado di rilevare la larghezza di banda disponibile per la *propria* rete. Naturalmente il semplice limite della larghezza di banda funzionerà, a differenza della banda garantita, delle priorità e del bilanciamento dinamico.

Attenzione alle dispersioni

Se si decide di proteggere e gestire il traffico di un collo di bottiglia della rete, è necessario assicurare il passaggio di *tutto* il traffico del collo di bottiglia attraverso i propri pipe. Se parte del traffico di una connessione a Internet non attraversa i pipe, questi non saranno mai in grado di rilevare quando la connessione Internet è piena.

I casi appena descritti illustrano i problemi derivanti dalle dispersioni. Il traffico che "si disperde" attraverso il firewall senza essere misurato dai pipe produce lo stesso effetto dato dal consumo di larghezza di banda da parte di utenti al di fuori del vostro controllo ma che condividono la vostra stessa connessione.

10.2.2.3 Banda garantita

Il concetto di banda garantita è abbastanza simile all'ordinamento di certi tipi di traffico in base alla priorità. Ciò che rimane da fare è limitare la quantità di larghezza di banda ad elevata priorità che può essere utilizzata. Il modo più semplice ma meno flessibile per ottenere questo risultato è limitare il passaggio del traffico nelle preferenze più elevate dei pipe predefiniti.

Per modificare il traffico SSH e telnet ordinato in base alla priorità del precedente esempio con garanzia di 96 kbps, è sufficiente modificare il pipe "std-in" in modo che includa un limite di 96 kbps per la precedenza 1.

Ciò significa che il traffico SSH e telnet in entrata è *limitato* a 96 kbps?

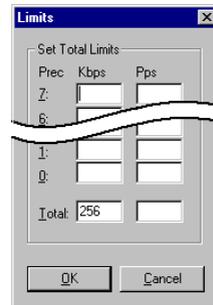
Naturalmente no.

Come affermato in precedenza, il traffico in eccesso nelle precedenze superiori alla precedenza di massimo carico viene passato in quest'ultima, che, in questo esempio, è 0.



È bene ricordare che i limiti nelle precedenze superiori alla precedenza di massimo carico *non* limitano il traffico. Questi limiti agiscono solo sul volume di traffico che attraversa la precedenza specifica.

In questo caso, il limite di 96 kbps nella precedenza 1 indica che è possibile consentire il passaggio di 96 kbps di traffico con precedenza 1 nel pipe std-in e che questo traffico in effetti *passerà*, a meno che, ovviamente, non si abbia altro traffico con precedenze più elevate.



Se si prova a consentire il passaggio di oltre 96 kbps di traffico con precedenza 1, il traffico in eccesso deve contendere la rimanente larghezza di banda al resto del traffico ed affrontare una competizione del tipo "first-come, first-served", come tutte le connessioni a Internet. Nel corso del capitolo verranno descritti il raggruppamento e il bilanciamento, due soluzioni che possono migliorare la situazione.

10.2.2.4 Banda garantita differenziata

Come è già stato detto, il metodo appena illustrato per l'implementazione della banda garantita presenta un piccolo problema, ovvero non è particolarmente flessibile.

Se, ad esempio, si desidera assegnare una specifica banda di 32 kbps al traffico telnet e una banda di 63 kbps al traffico SSH, è *possibile* impostare un limite da 32 kbps per la precedenza 1, un limite da 64 kbps per la precedenza 2 e consentire il passaggio dei diversi tipi di traffico attraverso le rispettive precedenze. Questo approccio, tuttavia, presenta due problemi evidenti:

- Quale traffico è da considerare più importante? Questa domanda non pone grossi problemi in questo caso, ma diventa più difficile mano a mano che il contesto di gestione del traffico diventa più complesso.
- Il numero di precedenze è estremamente limitato. Con otto precedenze è possibile creare solo otto garanzie differenziate. Anche superando il problema dell'importanza del traffico, questo rimarrebbe comunque un grosso limite.

Per risolvere questo problema è necessario creare due nuovi pipe: uno per il traffico telnet e l'altro per il traffico SSH, simile al pipe "surf" creato in precedenza.

Innanzitutto è necessario *rimuovere* il limite da 96 kbps dal pipe std-in e quindi creare due nuovi pipe che verranno denominati "ssh-in" e "telnet-in". Impostare la precedenza predefinita per entrambi i pipe a 1 e i limiti di precedenza 1 rispettivamente a 32 e 64 kbps.

	Name	Min...	Def...	Max...	Grouping	Net ...	Total Limits	Per-User Limits	Dyn...	Comments
1	std-in	0	0	7	None		Total: 256Kb			
2	std-out	0	0	7	None		Total: 256Kb			
3	surf-in	0	0	7	None		Total: 128Kb			
4	ssh-in	0	1	7	None		P1: 64Kb			
5	telnet-in	0	1	7	None		P1: 32Kb			
6		0	0	7	None					

Dividere quindi la regola definita in precedenza relativa alle porte 22 e 23 in due regole, una per ciascuna porta.

	Action	Pipes	Src If...	Source Net	Dest If...	Dest Net	Proto	Ports/Params
1	Allow	Fwd: std:...	int	intnet	ext	all-nets	TCP	ALL -> 22
2	Allow	Fwd: std:...	int	intnet	ext	all-nets	TCP	ALL -> 23
3	Allow	Fwd: std:...	int	intnet	ext	all-nets	TCP	ALL -> 80
4	Allow	Fwd: std:...	int	intnet	ext	all-nets	Standard	
5								

Mantenere la concatenazione di inoltro di entrambe le regole solo come "std-out". Per semplificare questo esempio, l'attenzione viene focalizzata solo sul traffico in entrata, ovvero la direzione che tende a riempirsi prima nelle configurazioni client-oriented.

Impostare la concatenazione di ritorno della regola della porta 22 su "ssh-in" seguito da "std-in". Impostare la concatenazione di ritorno della regola della porta 23 su "telnet-in" seguito da "std-in". Impostare l'assegnazione della priorità per entrambe le regole su "Use defaults from first pipe", dove la precedenza predefinita sia per il pipe ssh-in sia telnet-in è 1. Utilizzando questo approccio invece della precedenza 1 "hard-coding" nell'insieme di regole, è possibile modificare la precedenza di tutto il traffico ssh e telnet semplicemente modificando la precedenza dei pipe "ssh-in" e "telnet-in".

Notare che non è stato impostato un limite totale per i pipe ssh-in e telnet-in. Infatti non è necessario, dal momento che il limite totale viene imposto dal pipe "std-in" che si trova all'estremità delle rispettive concatenazioni.

I pipe ssh-in e telnet-in funzionano da "filtri per la priorità", ovvero controllano che solo il volume riservato rispettivamente di 64 e 32 kbps di traffico con precedenza 1 raggiunga std-in. Il traffico SSH e telnet che supera le rispettive garanzie raggiunge std-in con precedenza 0, la precedenza di massimo carico dei pipe std-in e ssh-in.



In questo caso è importante ordinare i pipe nella concatenazione di ritorno. Se std-in viene posto prima di ssh-in e telnet-in, il traffico raggiunge std-in solo come precedenza 0 e deve perciò competere come il resto del traffico per i 256 kbps di larghezza di banda disponibile.

10.2.3 Raggruppamento degli utenti di un pipe

Se le funzionalità dei pipe fossero ristrette a quanto descritto sino ad ora, il traffico sarebbe limitato indipendentemente dall'origine e dalla destinazione. Questa modalità operativa può essere sufficiente per la semplice gestione del traffico e banda garantita.

EnterNet FireWall, però, è in grado di raggruppare il traffico in ogni pipe. In questo modo il traffico viene classificato e raggruppato in base alla sorgente o alla destinazione di ciascun pacchetto che attraversa il pipe.

È possibile effettuare il raggruppamento in base alla rete, all'indirizzo IP oppure alle porte sorgente o destinazione. Nel caso di raggruppamento in base alla rete, è possibile specificarne le dimensioni. I casi di raggruppamento in base alla porta includono anche l'indirizzo IP, dal momento che la porta 1024 del computer A *non* appartiene allo stesso "gruppo" della porta 1024 del computer B.

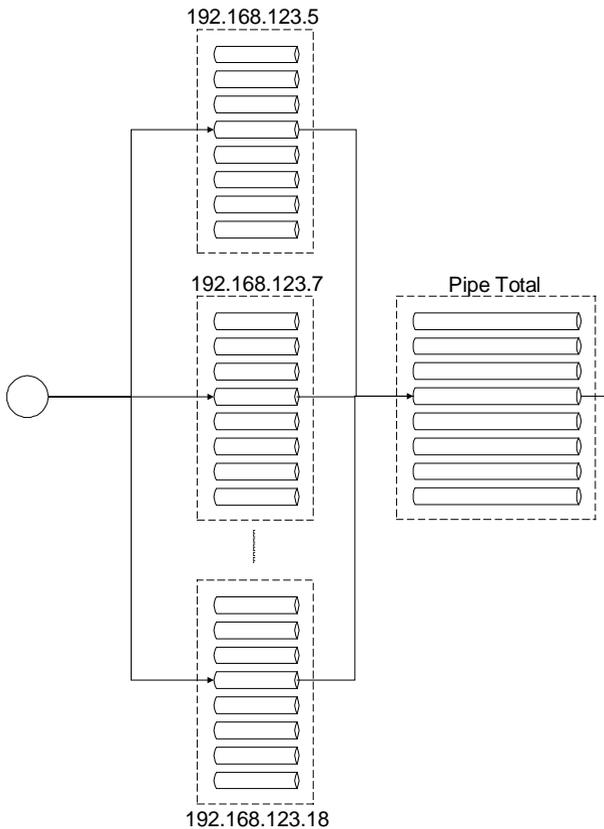
Il raggruppamento offre il vantaggio di poter applicare ulteriori controlli di larghezza di banda a ciascun gruppo. Ciò significa che se il raggruppamento viene effettuato, ad esempio, sull'indirizzo IP, il firewall può limitare e garantire la larghezza di banda in base all'indirizzo IP che comunica attraverso il pipe.

Anche nei gruppi utenti è possibile applicare precedenze. È possibile limitare la larghezza di banda sia in base alla precedenza che per ciascun gruppo intero.



In molti casi i gruppi verranno definiti utenti, sia che il gruppo rappresenti una persona fisica, una connessione sola o un'intera rete di classe C.

Il controllo della larghezza di banda viene dapprima applicato ad ogni singolo utente e quindi all'intero pipe. Il disegno qui di seguito illustra un pipe nel quale è stato abilitato il raggruppamento.



Esempio di pipe con traffico in precedenza 4 raggruppato in base all'indirizzo IP.

10.2.3.1 Applicazione di limiti e garanzie in base a ogni singolo utente

Dopo aver raggruppato gli utenti di un pipe, si possono inserire limitazioni di banda, sia garantirla a ciascun utente così come vengono applicate all'intero pipe.

Per ampliare l'esempio precedente, è possibile limitare la quantità di larghezza di banda che ciascun utente interno riceve per il traffico SSH in entrata. In questo modo si evita che un singolo utente esaurisca tutta la larghezza di banda ad elevata priorità disponibile.

Innanzitutto è necessario decidere come raggruppare gli utenti del pipe ssh-in per poter applicare delle limitazioni a ciascun utente sulla rete interna. Dal momento che si tratta di pacchetti *in entrata*, il raggruppamento avverrà in base all'IP di destinazione, perciò è necessario modificare il raggruppamento "ssh-in" in "Per DestIP".

	Name	Min...	Def...	Max...	Grouping	Net ...	Total Limits	Per-User ...	Dyn...	Comments
1	std-in	0	0	7	None		Total: 256Kb			
2	std-out	0	0	7	None		Total: 256Kb			
3	surf-in	0	0	7	None		Total: 128Kb			
4	ssh-in	0	1	7	Per DestIP		P1: 64Kb	P1: 16Kb	<input type="checkbox"/>	
5	telnet-in	0	1	7	None		P1: 32Kb			
6		0	0	7	None					

Dopo avere impostato il raggruppamento si possono impostare le limitazioni in base a ciascun singolo utente. In questo caso, il limite per la precedenza 1 viene impostato a 16 kbps per utente, in modo che ciascuno di essi abbia una banda garantita di soli 16 kbps per il traffico SSH. Se si desidera, è possibile limitare anche la larghezza di banda totale per ciascun utente, impostandola ad esempio su 40 kbps.

Appare evidente che sorgono problemi se più di quattro utenti inviano o ricevono contemporaneamente molto traffico SSH, dal momento che 16 kbps per cinque dà un totale che supera i 64 kbps. Il limite totale per il pipe è ancora attivo e ciascun utente deve competere per la larghezza di banda disponibile con precedenza 1 così come devono competere per la larghezza di banda con precedenza 0. Nel corso del capitolo verrà trattato il bilanciamento dinamico, una soluzione che può migliorare la situazione.



Per una maggiore comprensione di quello che avviene in una configurazione attiva, si consiglia di provare il comando "pipe -u <pipename>", che permette di visualizzare l'elenco degli utenti correntemente attivi su ciascun pipe.

10.2.4 Bilanciamento dinamico della larghezza di banda

Come detto in precedenza, è possibile limitare la larghezza di banda ad ogni singolo utente consentendo il raggruppamento all'interno di un pipe, in modo da assicurare che un utente non esaurisca tutta la larghezza di banda disponibile.

Cosa accade se si imposta un limite della larghezza di banda per il pipe intero e *questo* limite viene superato?

Nell'esempio precedente, il limite di larghezza di banda con precedenza 1 per ciascun utente è di 16 kbps, mentre il limite con precedenza 1 per il pipe è di 64 kbps. In questo modo la larghezza di banda ad elevata precedenza viene distribuita equamente fino a quattro utenti.

Se un quinto utente genera traffico SSH, il limite di 64 kbps viene superato, generando risultati non prevedibili, dal momento che alcuni utenti riceveranno comunque i 16 kbps mentre altri no.

Per prevenire situazioni di questo genere, EnterNet FireWall dispone di una funzione denominata *Dynamic Bandwidth Balancing* (*Bilanciamento dinamico della larghezza di banda*). Questo algoritmo garantisce l'abbassamento (e l'innalzamento) dinamico dei limiti di larghezza di banda in base a ciascun singolo utente per bilanciare in maniera uniforme tra gli utenti del pipe la larghezza di banda disponibile.

Riprendendo l'esempio precedente, quando un altro utente comincia a generare traffico SSH, il limite per utente viene abbassato a circa 13 kbps (64 kbps divisi tra 5 utenti). Le restrizioni temporanee come questa vengono gradualmente rimosse sino a raggiungere il limite configurato *oppure* sino a superare i limiti del pipe. A quel punto i limiti per gli utenti vengono abbassati di nuovo. Questi adeguamenti dinamici avvengono circa 20 volte al secondo e si adattano rapidamente alle modifiche apportate alla distribuzione di larghezza di banda.

Il bilanciamento dinamico di larghezza di banda avviene individualmente in ciascuna precedenza di un pipe. In questo modo, se agli utenti viene assegnata una quantità ridotta di traffico ad elevata priorità e una quantità maggiore di traffico di massimo carico, tutti gli utenti riceveranno la loro parte di traffico ad elevata precedenza e la parte di traffico di massimo carico.

10.3 Esempi pratici di utilizzo dei pipe

Nel presente capitolo è stato illustrato il funzionamento dal punto di vista tecnico del sottosistema di gestione del traffico di EnterNet FireWall.

Ma pipe, gruppi di utenti e precedenze sono semplici elementi di base che possono essere utilizzati come si ritiene meglio. I contesti di gestione del traffico che si possono creare applicando diversi limiti e precedenze e concatenando diversi pipe tra loro, è limitato solo dalla propria immaginazione e dalle proprie capacità di progettazione.

Vediamo due esempi di utilizzo.

Utilizzo dei pipe come misuratori di traffico

Se si creano pipe senza alcun tipo di limite, è possibile consentire il passaggio del traffico in una o più regole di particolare interesse e ottenere un grafico della larghezza di banda nella visualizzazione delle statistiche in FireWall Manager oppure dal prompt dei comandi.

Implementazione di protezione contro gli intasamenti SYN per le regole FwdFast

EnterNet FireWall non dispone di una protezione speciale contro gli intasamenti SYN attraverso le regole FwdFast, a differenza delle regole Allow e NAT.

Utilizzando i pipe, è possibile configurare valori limite per i pacchetti TCP SYN, realizzando quindi una protezione rudimentale contro gli intasamenti SYN.

A tale scopo è necessario creare due regole che consentono il passaggio dei pacchetti verso una porta di server. Le due regole devono essere quasi identiche, l'unica differenza è che nella prima deve essere selezionata la casella di controllo "Only Established Connections", mentre nell'altra no.

In questo modo la prima regola riceve tutti i pacchetti in arrivo alla porta di server *tranne* i pacchetti SYN, che vengono invece ricevuti dalla seconda regola. Immaginiamo cosa accadrebbe se si applicasse la seconda regola a un pipe con un limite, ad esempio, di 10 pacchetti per secondo.

Purtroppo non è possibile riportare numerosi esempi pratici sull'utilizzo della gestione del traffico in questo Manuale utente.

Per consultare altri esempi di gestione del traffico, visitate il nostro sito all'indirizzo <http://www.enternet.net>.

Il sito include numerosi esempi di configurazione per i contesti di gestione del traffico ed esempi di normale utilizzo di firewall e VPN. Questi esempi illustrano anche strutture di rete e descrizioni guidate dei file di configurazione.

11. Internet e TCP/IP

11.1 Numeri di protocollo IP

Le informazioni sono tratte dal sito all'indirizzo <http://www.isi.edu/in-notes/iana/assignments/protocol-numbers>, che rappresenta la fonte più aggiornata di numeri di protocollo registrati.

Per un breve riepilogo dei protocolli utilizzati più frequentemente, consultare la fine della presente sezione.

N.	Nome	Descrizione	RFC
0	HOPOPT	Hop-by-Hop Option IPv6	1883
1	ICMP	Internet Control Message	792
2	IGMP	Internet Group Management	1112
3	GGP	Gateway-to-Gateway	823
4	IP	IP in IP (incapsulamento)	2003
5	ST	Stream	1190
6	TCP	Transmission Control	793
7	CBT	CBT	
8	EGP	Exterior Gateway	888
9	IGP	Gateway interno privato (utilizzato da Cisco per IGRP)	
10	BBN-RCC-MON	BBN RCC Monitoring	
11	NVP-II	Network Voice Protocol	741
12	PUP	Xerox PARC Universal Protocol	
13	ARGUS	ARGUS	
14	EMCON	EMCON	
15	XNET	Cross Net Debugger	

16	CHAOS	Chaos	
17	UDP	User Datagram	768
18	MUX	Multiplexing	
19	DCN-MEAS	DCN Measurement Subsys	
20	HMP	Host Monitoring	869
21	PRM	Packet Radio Measurement	
22	XNS-IDP	Xerox NS IDP	
23	TRUNK-1	Trunk-1	
24	TRUNK-2	Trunk-2	
25	LEAF-1	Leaf-1	
26	LEAF-2	Leaf-2	
27	RDP	Reliable Data Protocol	908
28	IRTP	Internet Reliable Transaction	938
29	ISO-TP4	ISO Transport Protocol Class 4	905
30	NETBLT	Bulk Data Transfer Protocol	969
31	MFE-NSP	MFE Network Services Protocol	
32	MERIT-INP	MERIT Internodal Protocol	
33	SEP	Sequential Exchange Protocol	
34	3PC	Third Party Connect Protocol	
35	IDPR	Inter-Domain Policy Routing	
36	XTP	XTP	
37	DDP	Datagram Delivery Protocol	
38	IDPR-CMTP	IDPR Control Message	
39	TP++	TP++ Transport Protocol	
40	IL	IL Transport Protocol	
41	IPv6	IPv6	
42	SDRP	Source Demand Routing	
43	IPv6-Route	Routing Header per IPv6	
44	IPv6-Frag	Fragment Header per IPv6	

45	IDRP	Inter-Domain Routing Protocol	
46	RSVP	Reservation Protocol	
47	GRE	General Routing Encapsulation	
48	MHRP	Mobile Host Routing Protocol	
49	BNA	BNA	
50	ESP	Encap Security Payload IPv6	1827
51	AH	Authentication Header IPv6	1826
52	I-NLSP	Integrated Net Layer Security	
53	SWIPE	IP con Encryption	
54	NARP	NBMA Address Resolution	1735
55	MOBILE	IP Mobility	
56	TLSP	Transport Layer Security che utilizza gestione delle chiavi Kryptonet	
57	SKIP	SKIP	
58	IPv6-ICMP	ICMP per IPv6	1883
59	IPv6-NoNxt	No Next Header per IPv6	1883
60	IPv6-Opts	Destination Options IPv6	1883
61		Protocollo interno di host	
62	CFTP	CFTP	
63		Rete locale	
64	SAT-EXPAK	SATNET / Backroom EXPAK	
65	KRYPTOLAN	Kryptolan	
66	RVD	MIT Remote Virtual Disk	
67	IPPC	Internet Pluribus Packet Core	
68		File system distribuito	
69	SAT-MON	SATNET Monitoring	
70	VISA	VISA Protocol	
71	IPCV	Internet Packet Core Utility	
72	CPNX	Computer Proto Net Executive	

73	CPHB	Computer Proto Heart Beat	
74	WSN	Wang Span Network	
75	PVP	Packet Video Protocol	
76	BR-SAT-MON	Backroom SATNET Monitoring	
77	SUN-ND	SUN ND Protocol	
78	WB-MON	WIDEBAND Monitoring	
79	WB-EXPAK	WIDEBAND EXPAK	
80	ISO-IP	ISO Internet Protocol	
81	VMTP	VMTP	
82	SECURE-VMTP	SECURE-VMTP	
83	VINES	VINES	
84	TTP	TTP	
85	NSFNET	NSFNET-IGP	
86	DGP	Dissimilar Gateway Protocol	
87	TCF	TCF	
88	EIGRP	EIGRP	
89	OSPFIGP	Open Shortest Path First IGP	1583
90	Sprite-RPC	Sprite RPC Protocol	
91	LARP	Locus Address Resolution	
92	MTP	Multicast Transport Protocol	
93	AX.25	AX.25 Frames	
94	IPIP	IP-within-IP Encapsulation	
95	MICP	Mobile Internetworking Control	
96	SCC-SP	Semaphore Comms Security	
97	ETHERIP	Ethernet-within-IP Encap	
98	ENCAP	Encapsulation Header	1241
99		Schema privato di crittografia	
100	GMTP	GMTP	
101	IFMP	Ipsilon Flow Management	

102	PNNI	PNNI over IP	
103	PIM	Protocol Independent Multicast	
104	ARIS	ARIS	
105	SCPS	SCPS	
106	QNX	QNX	
107	A/N	Active Networks	
108	IPComp	IP Payload Compressions	2393
109	SNP	Sitara Networks Protocol	
110	Compaq-Peer	Compaq Peer Protocol	
111	IPX-in-IP	IPX in IP	
112	VRRP	Virtual Router Redundancy	
113	PGM	PGM Reliable Transport	
114		Protocollo 0-hop	
115	L2TP	Layer 2 Tunnelling Protocol	
116	DDX	D-II Data Exchange (DDX)	
117	IATP	Interactive Agent Transfer	
118	STP	Schedule Transfer Protocol	
119	SRP	Spectralink Radio Protocol	
120	UTI	UTI	
121	SMP	Simple Message Protocol	
122	SM	SM	
123	PTP	Performance Transparency	
124	ISIS-IPv4	ISIS over IPv4	
125	FIRE		
126	CRPT	Combat Radio Transport	
127	CRUDP	Combat Radio User Datagram	
128	SSCOPMCE		
129	IPLT		

Solo alcuni dei numeri di protocollo elencati sono di uso comune nelle reti odierne.

Protocolli IP utilizzati molto frequentemente:

- | | | |
|----|------|-----------------------------------|
| 1 | ICMP | Internet Control Message Protocol |
| 6 | TCP | Transmission Control Protocol |
| 17 | UDP | User Datagram Protocol |

Protocolli IP utilizzati frequentemente:

- | | | |
|-----|--------|--|
| 47 | GRE | Generic Routing Encapsulation. Utilizzato da PPTP. |
| 50 | ESP | Encapsulation Security Payload di IPsec e IPv6. |
| 51 | AH | Authentication Header di IPsec e IPv6. |
| 57 | SKIP | Standard VPN progettato originariamente da SUN. |
| 89 | OSPF | Open Shortest Path First. Utilizzato dai router. |
| 94 | IPIP | IP-in-IP. Utilizzato dal punto di arresto VPN-1. |
| 108 | IPComp | Compressione dei dati IPsec e IPv6. |
| 115 | L2TP | Layer 2 Tunneling Protocol |

11.2 Numeri di porta utilizzati comunemente

Le informazioni sono tratte dal sito all'indirizzo <http://www.isi.edu/in-notes/iana/assignments/port-numbers>, che rappresenta la fonte più aggiornata di numeri di porta registrati.

L'elenco che segue ha dimensioni dieci volte inferiori rispetto all'elenco originale. Sono stati aggiunti alcuni protocolli, anche se non registrati.

echo	7/tcp	Echo
echo	7/udp	Echo
discard	9/tcp	Discard (Sink)
discard	9/udp	Discard (Sink)
systat	11/tcp	Active Users
systat	11/udp	Active Users
daytime	13/tcp	Daytime
daytime	13/udp	Daytime
qotd	17/tcp	Quote of the Day
qotd	17/udp	Quote of the Day
chargen	19/tcp	Character Generator
chargen	19/udp	Character Generator
ftp-data	20/tcp	File Transfer [Default Data]
ftp-data	20/udp	File Transfer [Default Data]
ftp	21/tcp	File Transfer [Control]
ftp	21/udp	File Transfer [Control]
ssh	22/tcp	Secure Shell
ssh	22/udp	Secure Shell
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
smtp	25/tcp	Simple Mail Transfer

smtp	25/udp	Simple Mail Transfer
time	37/tcp	Time
time	37/udp	Time
nicname	43/tcp	Who Is
nicname	43/udp	Who Is
auditd	48/tcp	Digital Audit Daemon
auditd	48/udp	Digital Audit Daemon
login	49/tcp	Login Host Protocol
login	49/udp	Login Host Protocol
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
sql*net	66/tcp	Oracle SQL*NET
sql*net	66/udp	Oracle SQL*NET
bootps	67/tcp	Bootstrap Protocol Server
bootps	67/udp	Bootstrap Protocol Server
bootpc	68/tcp	Bootstrap Protocol Client
bootpc	68/udp	Bootstrap Protocol Client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	Gopher
gopher	70/udp	Gopher
finger	79/tcp	Finger
finger	79/udp	Finger
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
objcall	94/tcp	Tivoli Object Dispatcher
objcall	94/udp	Tivoli Object Dispatcher
hostname	101/tcp	NIC Host Name Server
hostname	101/udp	NIC Host Name Server

3com-tsmux	106/tcp	3COM-TSMUX
3com-tsmux	106/udp	3COM-TSMUX
rtelnet	107/tcp	Remote Telnet Service
rtelnet	107/udp	Remote Telnet Service
pop2	109/tcp	Post Office Protocol – Version 2
pop2	109/udp	Post Office Protocol – Version 2
pop3	110/tcp	Post Office Protocol – Version 3
pop3	110/udp	Post Office Protocol – Version 3
sunrpc	111/tcp	SUN Remote Procedure Call
sunrpc	111/udp	SUN Remote Procedure Call
auth	113/tcp	Authentication Service
auth	113/udp	Authentication Service
uucp-path	117/tcp	UUCP Path Service
uucp-path	117/udp	UUCP Path Service
sqlserv	118/tcp	SQL Services
sqlserv	118/udp	SQL Services
nntp	119/tcp	Network News Transfer Protocol
nntp	119/udp	Network News Transfer Protocol
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
pwdgen	129/tcp	Password Generator Protocol
pwdgen	129/udp	Password Generator Protocol
cisco-fna	130/tcp	cisco FNATIVE
cisco-fna	130/udp	cisco FNATIVE
cisco-tna	131/tcp	cisco TNATIVE
cisco-tna	131/udp	cisco TNATIVE
cisco-sys	132/tcp	cisco SYSMaint
cisco-sys	132/udp	cisco SYSMaint
statsrv	133/tcp	Statistics Service

statsrv	133/udp	Statistics Service
netbios-rpc	135/tcp	NETBIOS Remote Procedure Call
netbios-rpc	135/udp	NETBIOS Remote Procedure Call
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap4	143/tcp	Internet Mail Access Protocol v4
imap4	143/udp	Internet Mail Access Protocol v4
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
pcmail-srv	158/tcp	PCMail Server
pcmail-srv	158/udp	PCMail Server
snmp	161/tcp	SNMP
snmp	161/udp	SNMP
snmptrap	162/tcp	SNMPTRAP
snmptrap	162/udp	SNMPTRAP
print-srv	170/tcp	Network PostScript
print-srv	170/udp	Network PostScript
xmcp	177/tcp	X Display Manager Control Protocol
xmcp	177/udp	X Display Manager Control Protocol
nextstep	178/tcp	NextStep Window Server
nextstep	178/udp	NextStep Window Server
bgp	179/tcp	Border Gateway Protocol
bgp	179/udp	Border Gateway Protocol

audit	182/tcp	Unisys Audit SITP
audit	182/udp	Unisys Audit SITP
prospero	191/tcp	Prospero Directory Service
prospero	191/udp	Prospero Directory Service
irc	194/tcp	Internet Relay Chat Protocol
irc	194/udp	Internet Relay Chat Protocol
at-rtmp	201/tcp	AppleTalk Routing Maintenance
at-rtmp	201/udp	AppleTalk Routing Maintenance
at-nbp	202/tcp	AppleTalk Name Binding
at-nbp	202/udp	AppleTalk Name Binding
at-3	203/tcp	AppleTalk Unused
at-3	203/udp	AppleTalk Unused
at-echo	204/tcp	AppleTalk Echo
at-echo	204/udp	AppleTalk Echo
at-5	205/tcp	AppleTalk Unused
at-5	205/udp	AppleTalk Unused
at-zis	206/tcp	AppleTalk Zone Information
at-zis	206/udp	AppleTalk Zone Information
at-7	207/tcp	AppleTalk Unused
at-7	207/udp	AppleTalk Unused
at-8	208/tcp	AppleTalk Unused
at-8	208/udp	AppleTalk Unused
ipx	213/tcp	IPX
ipx	213/udp	IPX
dbase	217/tcp	dBASE Unix
dbase	217/udp	dBASE Unix
imap3	220/tcp	Interactive Mail Access Protocol v3
imap3	220/udp	Interactive Mail Access Protocol v3
fln-spx	221/tcp	Berkeley rlogind with SPX auth

fln-spx	221/udp	Berkeley rlogind with SPX auth
rsh-spx	222/tcp	Berkeley rshd with SPX auth
rsh-spx	222/udp	Berkeley rshd with SPX auth
pdap	344/tcp	Prospero Data Access Protocol
pdap	344/udp	Prospero Data Access Protocol
ulistserv	372/tcp	Unix Listserv
ulistserv	372/udp	Unix Listserv
hp-collector	381/tcp	hp performance data collector
hp-collector	381/udp	hp performance data collector
hp-managed- node	382/tcp	hp performance data managed node
hp-managed- node	382/udp	hp performance data managed node
hp-alarm-mgr	383/tcp	hp performance data alarm manager
hp-alarm-mgr	383/udp	hp performance data alarm manager
ibm-app	385/tcp	IBM Application
ibm-app	385/tcp	IBM Application
aurp	387/tcp	Appletalk Update-Based Routing Prot.
aurp	387/udp	Appletalk Update-Based Routing Prot.
ldap	389/tcp	Lightweight Directory Access Protocol
ldap	389/udp	Lightweight Directory Access Protocol
synoptics- relay	391/tcp	SynOptics SNMP Relay Port
synoptics- relay	391/udp	SynOptics SNMP Relay Port
synoptics- broker	392/tcp	SynOptics Port Broker Port
synoptics- broker	392/udp	SynOptics Port Broker Port
netware-ip	396/tcp	Novell Netware over IP

netware-ip	396/udp	Novell Netware over IP
ups	401/tcp	Uninterruptible Power Supply
ups	401/udp	Uninterruptible Power Supply
genie	402/tcp	Genie Protocol
genie	402/udp	Genie Protocol
prm-sm	408/tcp	Prospero Resource Manager Sys. Man.
prm-sm	408/udp	Prospero Resource Manager Sys. Man.
prm-nm	409/tcp	Prospero Resource Manager Node Man.
prm-nm	409/udp	Prospero Resource Manager Node Man.
synoptics-trap	412/tcp	Trap Convention Port
synoptics-trap	412/udp	Trap Convention Port
mobileip-agent	434/tcp	MobileIP-Agent
mobileip-agent	434/udp	MobileIP-Agent
mobilip-mn	435/tcp	MobilIP-MN
mobilip-mn	435/udp	MobilIP-MN
decvms- sysmgt	441/tcp	decvms-sysmgt
decvms- sysmgt	441/udp	decvms-sysmgt
https	443/tcp	https Mcom
https	443/udp	https Mcom
microsoft-ds	445/tcp	Microsoft-DS
microsoft-ds	445/udp	Microsoft-DS
as-servermap	449/tcp	AS Server Mapper
as-servermap	449/udp	AS Server Mapper
exec	512/tcp	esecuzione remota del processo; l'autenticazione viene eseguita utilizzando le password e i nomi di accesso UNIX

biff	512/udp	utilizzato dal sistema di posta per notificare agli utenti la ricezione della posta; attualmente riceve messaggi solo da processi dello stesso computer
login	513/tcp	remote login a la telnet; autenticazione automatica eseguita sulla base dei numeri di porta con privilegi e delle basi dati distribuite che identificano i "domini di autenticazione"
who	513/udp	mantiene le basi dati che mostrano l'utente connesso ai computer di una rete locale, nonché il carico medio del computer.
cmd	514/tcp	analogo ad exec, ma l'autenticazione automatica viene eseguita per quanto riguarda il server di accesso
syslog	514/udp	
printer	515/tcp	Spooler
printer	515/udp	Spooler
talk	517/tcp	analogo al collegamento tenex, ma tramite computer
talk	517/udp	
ntalk	518/tcp	
ntalk	518/udp	
utime	519/tcp	Unixtime
utime	519/udp	Unixtime

timed	525/tcp	Timeserver
timed	525/udp	Timeserver
netnews	532/tcp	Readnews
netnews	532/udp	Readnews
netwall	533/tcp	per trasmissioni di emergenza
netwall	533/udp	per trasmissioni di emergenza
uucp	540/tcp	Uucpd
uucp	540/udp	Uucpd
uucp-rlogin	541/tcp	uucp-rlogin
uucp-rlogin	541/udp	uucp-rlogin
klogin	543/tcp	
klogin	543/udp	
kshell	544/tcp	Krcmd
kshell	544/udp	Krcmd
new-rwho	550/tcp	new-who
new-rwho	550/udp	new-who
remotefs	556/tcp	rfs server
remotefs	556/udp	rfs server
ipcserver	600/tcp	Sun IPC server
ipcserver	600/udp	Sun IPC server
doom	666/tcp	doom Id Software
doom	666/udp	doom Id Software
netviewdm1	729/tcp	IBM NetView DM/6000 Server/Client
netviewdm1	729/udp	IBM NetView DM/6000 Server/Client
netviewdm2	730/tcp	IBM NetView DM/6000 send/tcp
netviewdm2	730/udp	IBM NetView DM/6000 send/tcp
netviewdm3	731/tcp	IBM NetView DM/6000 receive/tcp
netviewdm3	731/udp	IBM NetView DM/6000 receive/tcp
fujitsu-dev	747/tcp	Fujitsu Device Control

fujitsu-dev	747/udp	Fujitsu Device Control
kerberos-adm	749/tcp	kerberos administration
kerberos-adm	749/udp	kerberos administration
tell	754/tcp	Send
tell	754/udp	Send
quotad	762/tcp	
quotad	762/udp	
puprouter	999/tcp	PARC Universal Protocol Router
puprouter	999/udp	PARC Universal Protocol Router
enetfw	999/tcp	EnterNet FireWall
enetfw	999/udp	EnterNet FireWall
socks	1080/tcp	Socks
socks	1080/udp	Socks
netware-csp	1366/tcp	Novell NetWare Comm Service Platform
netware-csp	1366/udp	Novell NetWare Comm Service Platform
fc-cli	1371/tcp	Fujitsu Config Protocol
fc-cli	1371/udp	Fujitsu Config Protocol
fc-ser	1372/tcp	Fujitsu Config Protocol
fc-ser	1372/udp	Fujitsu Config Protocol
apple-licman	1381/tcp	Apple Network License Manager
apple-licman	1381/udp	Apple Network License Manager
novell-lu6.2	1416/tcp	Novell LU6.2
novell-lu6.2	1416/udp	Novell LU6.2
autodesk-lm	1422/tcp	Autodesk License Manager
autodesk-lm	1422/udp	Autodesk License Manager
ms-sql-s	1433/tcp	Microsoft-SQL-Server
ms-sql-s	1433/udp	Microsoft-SQL-Server
ms-sql-m	1434/tcp	Microsoft-SQL-Monitor
ms-sql-m	1434/udp	Microsoft-SQL-Monitor

eicon-server	1438/tcp	Eicon Security Agent/Server
eicon-server	1438/udp	Eicon Security Agent/Server
eicon-x25	1439/tcp	Eicon X25/SNA Gateway
eicon-x25	1439/udp	Eicon X25/SNA Gateway
eicon-slp	1440/tcp	Eicon Service Location Protocol
eicon-slp	1440/udp	Eicon Service Location Protocol
ms-sna-server	1477/tcp	Microsoft SNA server
ms-sna-server	1477/udp	Microsoft SNA server
ms-sna-base	1478/tcp	Microsoft SNA base
ms-sna-base	1478/udp	Microsoft SNA base
watcom-sql	1498/tcp	Watcom-SQL
watcom-sql	1498/udp	Watcom-SQL
orasrv	1525/tcp	Oracle
orasrv	1525/udp	Oracle
tlisrv	1527/tcp	Oracle
tlisrv	1527/udp	Oracle
coauthor	1529/tcp	Oracle
coauthor	1529/udp	Oracle
licensedaemon	1986/tcp	cisco license management
licensedaemon	1986/udp	cisco license management
tr-rsrb-p1	1987/tcp	cisco RSRB Priority 1 port
tr-rsrb-p1	1987/udp	cisco RSRB Priority 1 port
tr-rsrb-p2	1988/tcp	cisco RSRB Priority 2 port
tr-rsrb-p2	1988/udp	cisco RSRB Priority 2 port
tr-rsrb-p3	1989/tcp	cisco RSRB Priority 3 port
tr-rsrb-p3	1989/udp	cisco RSRB Priority 3 port
stun-p1	1990/tcp	cisco STUN Priority 1 port
stun-p1	1990/udp	cisco STUN Priority 1 port
stun-p2	1991/tcp	cisco STUN Priority 2 port

stun-p2	1991/udp	cisco STUN Priority 2 port
stun-p3	1992/tcp	cisco STUN Priority 3 port
stun-p3	1992/udp	cisco STUN Priority 3 port
snmp-tcp-port	1993/tcp	cisco SNMP TCP port
snmp-tcp-port	1993/udp	cisco SNMP TCP port
stun-port	1994/tcp	cisco serial tunnel port
stun-port	1994/udp	cisco serial tunnel port
perf-port	1995/tcp	cisco perf port
perf-port	1995/udp	cisco perf port
tr-rsrb-port	1996/tcp	cisco Remote SRB port
tr-rsrb-port	1996/udp	cisco Remote SRB port
gdp-port	1997/tcp	cisco Gateway Discovery Protocol
gdp-port	1997/udp	cisco Gateway Discovery Protocol
x25-svc-port	1998/tcp	cisco X.25 service (XOT)
x25-svc-port	1998/udp	cisco X.25 service (XOT)
tcp-id-port	1999/tcp	cisco identification port
tcp-id-port	1999/udp	cisco identification port
ccmail	3264/tcp	cc:mail/lotus
ccmail	3264/udp	cc:mail/lotus
dec-notes	3333/tcp	DEC Notes
dec-notes	3333/udp	DEC Notes
aol	5190/tcp	America-Online
aol	5190/udp	America-Online
x11	6000- 6063/tcp	X Window System
x11	6000- 6063/udp	X Window System

12. Domande frequenti (FAQ)

È possibile consultare una knowledge base con domande frequenti all'indirizzo <http://www.enternet.net>, da cui è possibile anche scaricare le versioni più recenti del presente Manuale utente.



- Come è possibile importare i contenuti di un disco di avvio di EnterNet FireWall nel database di amministrazione di FireWall Manager?

Per importare tutti i dati del firewall da un disco di avvio nel database di amministrazione è necessario seguire un procedimento suddiviso in tre fasi:

- Creare un nuovo firewall in FireWall Manager con lo stesso indirizzo IP del firewall esistente. Inserire il relativo disco di avvio nella workstation di FireWall Manager.
- Se si desidera continuare ad utilizzare la stessa chiave di crittografia del firewall presente, selezionare il firewall nell'elenco e dal menu **FireWall** scegliere **Advanced/Load Key from Disk**. In questo modo viene copiata la chiave di crittografia dal disco di avvio nel database di amministrazione.
- È stata copiata la configurazione attuale. Dal menu **FireWall** selezionare **Configure**. In questo modo si apre la visualizzazione della configurazione. Dal menu **File** selezionare **Advanced/Open from Disk**. In questo modo la configurazione viene aperta e i file trasferiti alla RAM. Scegliere OK per salvare la configurazione nel database di amministrazione. Rispondere No alla richiesta di caricamento della configurazione nel firewall.



- Perché la configurazione non viene trasferita automaticamente dal firewall a FireWall Manager se è stata aggiornata manualmente sul disco di avvio o se il firewall è stato aggiornato da un FireWall Manager connesso ad un altro database di amministrazione?

Per ragioni di sicurezza. Se, nonostante tutto, qualcuno riuscisse ad entrare nel firewall, la configurazione corretta rimarrebbe comunque nel database di amministrazione.

Nei caso in cui il firewall stesso fosse in grado di determinare con certezza quale può essere considerata una "buona" configurazione, il trasferimento potrebbe avvenire automaticamente. Tuttavia la tecnologia necessaria non è al momento disponibile. Se lo fosse, il problema non si porrebbe, dal momento che il firewall stesso sarebbe in grado di configurarsi senza dover ricorrere ad un intervento esterno.

È possibile scaricare la configurazione dal firewall, selezionando il comando **Download Configuration** dal menu **Firewall, Advanced**. Si consiglia però di analizzare attentamente la configurazione scaricata prima di salvarla nel database di gestione.



- Perché non è possibile utilizzare nomi IP dal DNS nelle regole di firewall? Quando i server vengono spostati è necessario effettuare un doppio lavoro per modificare gli indirizzi sia nel DNS che nel firewall.

Il DNS non è una struttura affidabile. Se non si è in grado di controllare cosa contiene il DNS del proprio dominio o, ad esempio, se il server DNS dovesse essere temporaneamente fuori servizio, il firewall sarebbe costretto a recuperare i dati da fonti esterne alla sua protezione.

Se succedesse questo, un intruso indesiderato potrebbe riuscire ad ottenere un passaggio nel firewall e avere accesso con il suo computer. La comunicazione che normalmente viene consentita ad un server accessibile pubblicamente oltre il firewall potrebbe venire deviata lungo le stesse linee verso una macchina completamente diversa e non accessibile pubblicamente.



- Il firewall traduce gli indirizzi delle connessioni utilizzando NAT e ora FTP funziona solo con Internet Explorer e Netscape, ma non con i software client FTP più comuni quali WS_FTP. Perché?

FTP funziona utilizzando due connessioni: una per inviare i comandi dal client al server e una per trasferire i file. FTP può funzionare sia in Active Mode o Passive Mode (modalità attiva o passiva), a seconda del comportamento del server FTP. Passive Mode viene generalmente abbreviata in PASV Mode.

FTP viene normalmente utilizzato in Active Mode, nella quale la seconda connessione (canale dei dati) viene aperta *dal* server FTP al client, cosa non consentita dal firewall.

Passive Mode fa sì che il client apra entrambe le connessioni al server e questo viene consentito dal firewall. Internet Explorer e Netscape vengono generalmente impostati per funzionare in Passive Mode, mentre il software FTP viene spesso impostato per funzionare in Active Mode.

Queste impostazioni possono essere cambiate nella maggior parte dei software FTP, ma non nel caso del client FTP fornito con Windows.

Consultare i file della guida del software FTP per ulteriori informazioni sul passaggio alla modalità Passive (PASV).



La versione più recente di Internet Explorer 5 utilizza Active Mode se viene impostato per visualizzare i siti FTP come se fossero unità disco rigido. Se però viene impostato su "Display FTP as a web page", utilizza FTP in Passive Mode.



Molti firewall utilizzano un proxy o Application Layer Gateway per consentire al server FTP di aprire la seconda connessione verso il client. EnterNet ha dimostrato recentemente che tutti i firewall con FTP Application Layer Gateway posso subire violazioni che fanno sì che il firewall apra una porta attraverso la quale è possibile ottenere accesso a macchine su reti protette. Il sospetto di questa possibilità è emerso nel 1998. EnterNet implementerà un FTP Application Layer Gateway nel proprio firewall solo quando sarà stato scoperto un modo per combattere questa vulnerabilità.

 - **FTP funziona con tutte le versioni di Netscape e Internet Explorer sino alla versione 4, ma non con la versione 5. Qual è il problema?**

Per consentire a FTP di funzionare in EnterNet FireWall mediante traduzione dinamica degli indirizzi è necessario utilizzare FTP in Passive Mode.

Internet Explorer 5 utilizza Active Mode solo se viene configurato per visualizzare FTP come disco rigido locale. Se però viene impostato su "Show FTP as a web page", utilizza FTP in Passive Mode.

È impossibile dire perché ciò accada, dal momento che non esiste un motivo per cui Internet Explorer passi da una modalità all'altra in questo modo.

 - **Desidero utilizzare NAT dinamico per nascondere i miei indirizzi. Che intervalli di indirizzi privati posso utilizzare?**

È possibile utilizzare tre diverse aree nell'estensione dell'indirizzo IP per gli indirizzi privati:

10.0.0.0-10.255.255.255 (16 milioni di indirizzi)

172.16.0.0-172.31.255.255 (16 x 65536 indirizzi)

192.168.0.0-192.168.255.255 (256 x 256 indirizzi)

Molte voci infondate sostengono che è possibile utilizzare anche altre reti. *False*. Le tre reti indicate sono le uniche che devono venire utilizzate se non si vogliono avere problemi imprevisti lungo la linea. Consultare RFC1918, Address Allocation for Private Internets (allocazione indirizzi privati per Internet).

 - **Che conseguenze comporta l'utilizzo di indirizzi privati in una rete protetta di proprietà di terzi?**

Nella migliore delle ipotesi, niente. Dal momento che la maggior parte degli utenti decide di implementare la traduzione dinamica degli indirizzi delle loro reti protette, il traffico di ritorno può tornare all'esterno del firewall, dove viene ripristinato e inviato alla rete protetta.

Bisogna però tenere presente cosa accadrebbe se si utilizzassero indirizzi altrui e si tentasse di comunicare con quella rete. Il risultato sarebbe che niente di quello che viene inviato raggiungerebbe la sua destinazione e che verrebbe instradato invece sulla propria rete.



- Perché EnterNet FireWall viene eseguito sotto DOS? Questo non riduce le sue prestazioni?

Una convinzione errata ma molto diffusa è che le prestazioni dei software vengono ridotte se il software viene eseguito in un ambiente DOS. Invece il software eseguito sotto DOS spesso ha prestazioni *migliori* dei software che vengono eseguiti sotto "veri" sistemi operativi. Ciò è dovuto al fatto che le funzioni di multitasking di un sistema operativo sottraggono tempo al software per eseguire altre funzioni. Sebbene sia vero che DOS ha capacità limitate, dal momento che consente l'esecuzione di un solo programma per volta, è l'ambiente ideale per gli scopi di EnterNet Firewall poiché consente il funzionamento ottimale del software. In realtà, una volta avviato il software del firewall, DOS non ha più alcun fine pratico, dal momento che il software del firewall diventa il sistema operativo in tempo reale.

- È stato scelto di utilizzare DOS invece di scrivere i file di avvio per poter ottenere "gratuitamente" un file system standard che può essere letto e gestito facilmente dalla maggior parte dei computer e dei sistemi operativi.
- Scegliendo DOS come piattaforma da cui eseguire il software del firewall è possibile utilizzare anche altri driver ODI per schede di rete non supportate dai driver integrati. Si tratta di uno standard che viene comunemente accettato dal mercato. Praticamente tutte le schede di rete sono fornite di driver ODI. In questo modo non è necessario scrivere i driver per altre schede di rete e aggiornarle ogni volta che vengono messe in vendita nuove schede. Questo consente di offrire alla clientela un miglior supporto per l'hardware del firewall.

- Inoltre, l'utilizzo di DOS invece di altri sistemi operativi più grandi consente di aumentare la sicurezza e la stabilità di EnterNet FireWall. Molte violazioni di altri firewall, infatti, sono dovute alle debolezze di implementazione della rete del sistema operativo che sta alla base. DOS non può essere violato dal momento che non dispone di uno stack di rete
- DOS non ha grandi requisiti hardware. Utilizzando DOS invece di un "vero" sistema operativo, i requisiti hardware per eseguire EnterNet FireWall sono notevolmente inferiori rispetto ad altri firewall che per la loro funzionalità si basano su sistemi operativi più vasti e complessi. In questo modo è possibile ridurre i costi che devono sostenere gli utenti finali.



- Dopo aver utilizzato uno scanner di porte per rilevare quali porte siano accessibili esternamente sui server pubblici, risulta che sono aperti intervalli casuali di porte UDP. Queste porte "aperte" variano ogni volta che viene eseguito lo scanner. Cosa accade di preciso?

Uno scanner di porte non può mai verificare che una specifica porta UDP su una macchina protetta sia veramente aperta. Ciò che può fare è inviare uno o più pacchetti *nella direzione* della macchina in questione. Ciò che accade ai pacchetti prima che raggiungano la macchina è un'altra questione.

Molti scanner di porte attendono la ricezione di pacchetti Destination Unreachable ICMP EnterNet FireWall restituisce tali pacchetti se sono stati scartati perché corrispondenti a una regola Reject, ma ne invia solo alcuni al secondo. Se la velocità dei pacchetti a cui è stato negato l'accesso è maggiore, questi vengono scartati definitivamente, ma il firewall non invierà più messaggi ICMP Destination Unreachable. La corrispondenza a regole Drop non porta mai all'invio di messaggi Destination Unreachable. Se, per uno dei due motivi appena elencati, lo scanner non riceve nessun messaggio di questo tipo, riterrà erroneamente che la porta è aperta.

Per scoprire realmente a cosa viene consentito il passaggio attraverso il firewall, è possibile collegare alla rete uno "Sniffer", un analizzatore di rete che visualizza il contenuto dei pacchetti. Utilizzare uno scanner per analizzare un flusso di pacchetti presso tutte le porte dell'indirizzo che interessa e controllare se alcuni di essi attraversano il firewall.

 - **Molti firewall consentono il passaggio di *tutti* i pacchetti per un breve periodo di tempo durante l'avvio, prima che venga caricato il software del firewall. Anche EnterNet FireWall presenta questo problema?**

No. Questo problema si presenta solo nel caso di sistemi operativi che hanno i propri stack di IP, mentre DOS non implementa l'instradamento. Quando il software di EnterNet FireWall viene avviato, sono immediatamente disponibili *tutte* le funzionalità, compreso l'insieme di regole. In questo modo non si ha alcun momento iniziale di vulnerabilità.

 - **È possibile installare EnterNet FireWall su un disco rigido?**

Sì. Con questa versione, però, è possibile che si presentino alcuni inconvenienti. Non è possibile importare o esportare in maniera semplice i file di configurazione da/a floppy. Ciò significa che è necessario copiare manualmente tutti i dati al disco e dal disco. Detto questo, eseguire un firewall da un'installazione su disco rigido funziona in maniera eccellente, in particolare per quanto riguarda l'amministrazione e l'aggiornamento del software in remoto e la riduzione del tempo di avvio.

 - **È possibile installare EnterNet FireWall su un disco Flash?**

Sì. Un disco Flash da 2 MB è sufficiente per installare EnterNet FireWall v6.0 e un disco da 4 MB dovrebbe essere sufficiente per le future espansioni. Al momento di andare in stampa il loro costo si aggira sui 30-40 dollari USA. Si consiglia di utilizzare unità disco su modulo, dal momento che sono di facile installazione e non presentano praticamente alcun problema. Per ulteriori informazioni sull'utilizzo di EnterNet FireWall in questa modalità, consultare la sezione relativa all'installazione su disco rigido.



- Cosa sono i parametri /0, /24 and /32 che si presentano nella configurazione del firewall?

Si tratta di maschere di rete utilizzate da CIDR, lo standard Classless InterDomain Routing. Per una spiegazione più dettagliata delle loro funzioni, consultare la voce CIDR del glossario nel capitolo 13.



- Non è possibile far funzionare in maniera corretta le regole SAT (Static Address Translation, traduzione statica di indirizzo). Dov'è l'errore?

Errori comuni che vengono commessi nella configurazione delle regole SAT:

- Dimenticare che la regola SAT di per sé non ha alcuna azione su un pacchetto. Quando un pacchetto coincide con una regola SAT, nel firewall viene attivata l'opzione per portare a termine una traduzione statica di indirizzo successiva, mentre si continua a cercare una regola corrispondente FwdFast, Allow, NAT, Drop o Reject.

Il motivo è che dovrebbe essere necessario impostare una sola regola SAT anche se si usano più di due interfacce. Se, ad esempio, si ha una zona demilitarizzata su una terza interfaccia, è probabile che vengano utilizzate regole diverse per il traffico dalle reti esterne (generalmente regole Allow) e la rete protetta (generalmente regole NAT).

- Se si utilizzano regole FwdFast, è necessario configurarle anche per il traffico di ritorno. Di conseguenza, anche per queste è necessario utilizzare due insiemi di regole SAT, una per il traffico in ciascuna direzione.



- La traduzione statica dell'indirizzo non avviene finché non è stata incontrata una regola FwdFast, Allow o NAT. Questo indica che una regola SAT che traduce gli indirizzi di destinazione 1.1.1.1 in 2.2.2.2 deve avere corrispondenza con una regola FwdFast o NAT con un indirizzo di destinazione 1.1.1.1, *non* 2.2.2.2.

Consultare la sezione 8.1, Traduzione degli indirizzi.



- Perché EnterNet FireWall non supporta protocolli di instradamento quali RIP o OSPF?

EnterNet intende implementare il supporto al protocollo di instradamento non appena sarà stato sviluppato un algoritmo sufficientemente sicuro che possa identificare le informazioni di instradamento sicure.

Accettare informazioni di instradamento senza verificare che siano sicure toglierebbe il significato al concetto di firewall, dal momento che intrusi indesiderati potrebbero reindirizzare a se stessi comunicazioni che dovrebbero viaggiare solo tra due interfacce "protette".



- Il mio server di posta è un server Microsoft Exchange / Lotus Notes / Novell GroupWise / altro. Se lo si colloca in una zona demilitarizzata, i computer non avranno accesso alle funzioni avanzate che offre. È possibile collocarlo in una rete protetta e consentire comunque la ricezione di e-mail da Internet?

Sì. Esistono quattro possibili soluzioni a questo problema:

- È possibile collocare un sistema di inoltro della posta nella zona demilitarizzata e renderlo accessibile da Internet. Questo, a sua volta, può comunicare con il server di posta interno mediante SMTP. Questa è la soluzione più sicura. Un sistema di inoltro della posta può anche verificare la presenza di virus e implementare altre misure di sicurezza sulla posta in entrata.
- Se il server di posta interno dispone solo di un indirizzo IP privato, è possibile impostare nel firewall una regola NAT che traduca il traffico destinato all'indirizzo IP esterno del firewall, porta 25, all'indirizzo del server di posta interno, porta 25. È necessario aggiungere una regola corrispondente Allow per consentire effettivamente il passaggio del traffico attraverso il firewall.
- Se il server di posta dispone di un indirizzo IP pubblico è possibile consentire semplicemente il passaggio del traffico SMTP alla porta 25.

- Se il server di posta non dispone di un indirizzo pubblico e non si desidera utilizzare la traduzione statica di indirizzo, è possibile selezionare un indirizzo IP dall'intervallo esterno e aggiungerlo alla configurazione di rete del server di posta. Il procedimento richiede l'aggiunta di un percorso separato nel firewall per l'indirizzo IP che si sta "prendendo in prestito", indirizzato all'interfaccia interna del firewall. Inoltre è necessario attivare la funzione Proxy ARP per il percorso sull'interfaccia da cui è stato "preso in prestito" l'indirizzo. Consentire quindi il passaggio del traffico all'indirizzo come indicato.

Consultare la sezione 8.1, Traduzione degli indirizzi.



- Selezionando la funzione Show Log in FireWall Manager non è possibile visualizzare eventi precedenti, ma solo ciò che accade *in quel momento*. Questo non va contro la logica di un registro?

Selezionando Show Log in FireWall Manager si apre una finestra in cui vengono visualizzati in tempo reale i dati di log generati dal firewall. Per visualizzare eventi precedenti, è necessario cercare tra i log creati da EnterNet FireWall Logger oppure dal destinatario syslog. Per ulteriori informazioni, consultare il capitolo, 9, Auditing da EnterNet Firewall.



- I file di registro generati da FireWall Logger/syslog sono vuoti.

È necessario predisporre il firewall per l'invio di messaggi di log al vostro loghost. Nella sezione Loghosts è possibile specificare fino a otto indirizzi a cui il firewall deve inviare i dati di log. Per ulteriori informazioni, consultare il paragrafo 7.3.11, Scheda Loghosts..



- Ho installato un firewall e ho utilizzato uno dei modelli di configurazione, ma non sono in grado di stabilire un contatto con il firewall. Dal momento che non ho effettuato alcuna modifica all'insieme di regole, può essere possibile che il problema sia dato da un errore del modello?

Provare ad utilizzare la guida per la risoluzione dei problemi che si trova al punto 6.7. Se il firewall non funziona.

Se la guida non risolve il problema, contattare il rivenditore di fiducia o, nel caso non possa essere di aiuto, contattare il servizio di assistenza Enternet.

Per consultare la versione aggiornata di questa sezione visitare il sito <http://www.enternet.net>.

13. Glossario

Active Mode	FTP in Active Mode significa che il server FTP crea il canale dei dati nel quale vengono trasferiti i file. Vedere anche <i>FTP</i> e <i>Passive Mode</i> .
Address Resolution Protocol	ARP è il protocollo utilizzato per trovare l'indirizzo hardware corrispondente a uno specifico indirizzo IP in una LAN, ad esempio una Ethernet. ARP non può essere inoltrato attraverso router o firewall.
ALG	Vedere Application Layer Gateway.
ARP	Vedere Address Resolution Protocol.
ASP	Vedere Application Service Provider, anche Active Server Pages.
Active Server Pages	File su server Web con linguaggi procedurali incorporati in documenti HTML. Questi script possono essere scritti in linguaggi quali VB Script, Javascript o simili.
Application Layer Gateway	Un firewall può utilizzare un ALG per esaminare informazioni a livello di applicazione, ad esempio i dati trasportati da TCP, UDP e altri protocolli.
Application Service Provider	Un Application Service Provider è un'azienda che mette a disposizione applicazioni tramite reti. Il costo di questo servizio può essere basato sul tempo o sul numero di utenti contemporanei.
Bastion Host	Il termine Bastion Host è equivalente al termine Firewall, ovvero un sistema disegnato per proteggere uno o più computer da violazioni. Vedere anche <i>Firewall</i> .
CAN	Vedere City Area Network.
CIDR	Vedere Classless InterDomain Routing.

City Area Network	Una rete MAN è costituita solitamente da una rete a dorsale veloce, composta da anelli in fibra, in grado di connettere utenti di una stessa città reciprocamente e ad Internet. Identico a <i>MAN</i> .
Classless InterDomain Routing	<p>CIDR è un metodo di notazione e una tecnologia di instradamento che consente agli intervalli IP di dimensioni diverse da 256, 65536 e 16777216 di venire instradati come singola rete omogenea. La notazione CIDR ha formato "192.168.123.0/24", dove "/24" è la dimensione dell'indirizzo di rete in <i>bit</i>. In altre parole, "/24" rappresenta il numero di uni binari nella maschera di rete, che in questo caso è "255.255.255.0".</p> <p>"/0" corrisponde al percorso predefinito, ovvero 0.0.0.0.</p> <p>"/8" è una rete di classe A, ovvero 255.0.0.0</p> <p>"/16" è una rete di classe B, ovvero 255.255.0.0</p> <p>"/24" è una rete di classe C, ovvero 255.255.255.0</p> <p>"/27" è una rete a 32 indirizzi, ovvero 255.255.255.224</p> <p>"/28" è una rete a 16 indirizzi, ovvero 255.255.255.240</p> <p>"/29" è una rete a 8 indirizzi, ovvero 255.255.255.248</p> <p>"/32" corrisponde a un singolo indirizzo.</p>
ODI	Open Datalink Interface è uno standard per driver di schede di interfaccia di rete quali quelli utilizzati da Novell.

Ethernet	<p>Ethernet è uno standard LAN molto diffuso nel settore. Una rete Ethernet viene generalmente trasportata su cavi Twisted Pair (CAT5), cavi coassiali (BNC) e fibre ottiche. Le reti Ethernet generalmente hanno una velocità di 10 Mbps e 100 Mbps, mentre le reti Gigabit Ethernet hanno una velocità di 1000 Mbps. Se un cavo viene utilizzato solo per collegare due computer tra loro o per collegare un computer a uno switch, la connessione può svolgersi in modalità <i>Full Duplex</i>. La modalità normale di una Ethernet a 10 Mbps è <i>Half Duplex</i>.</p>
File Transfer Protocol	<p>Ftp è un protocollo per il trasferimento dei file. Supporta sia il caricamento che lo scaricamento di file ed è in grado di trasferire più file contemporaneamente. Per quanto riguarda lo scaricamento di file, FTP è stato quasi completamente sostituito da HTTP.</p> <p>FTP funziona utilizzando due connessioni: una alla porta 21 per i comandi e una per il trasferimento dei dati. Se viene utilizzato FTP in <i>Active Mode</i>, il canale dei dati viene aperto dal server al client. Se viene utilizzato FTP in <i>Passive Mode</i>, il canale dei dati viene aperto dal client al server.</p>
Firewall	<p>Una speciale unità o server di rete con insiemi di regole che determinano a quale tipo di traffico può essere consentito il passaggio attraverso le sue varie direzioni. Mentre un router si concentra sull'IP, un firewall generalmente esamina protocolli più specifici quali TCP, UDP e ICMP. In alcuni casi i firewall controllano anche i dati contenuti nei protocolli di applicazione trasportati da TCP, UDP e ICMP.</p> <p>Una seconda definizione del termine Firewall può essere "procedure, politiche e sistemi stabiliti che proteggono una azienda da intrusioni".</p>

Firewalking	Una tecnica utilizzata per rivelare gli indirizzi privati che stanno dietro un firewall che traduce indirizzi. Può essere descritta brevemente come un percorso di rilevamento modificato e specializzato.
Frammentazione	<p>IP può trasportare fino a 65536 byte di dati. La maggior parte dei supporti, però, come ad esempio Ethernet, non è in grado di trasportare pacchetti di queste dimensioni. Lo stack IP risolve questo problema <i>frammentando</i> i dati da inviare in vari pacchetti separati, ognuno dei quali dispone di proprie intestazione e informazioni IP che consentiranno al destinatario di riassemblare correttamente il pacchetto originario.</p> <p>La frammentazione, però, aumenta il pericolo della perdita di pacchetti. Per questo motivo generalmente si cerca di comunicare senza ricorrere alla frammentazione.</p>
FTP	Vedere File Transfer Protocol.
Full Duplex	Full Duplex è una modalità di traffico di rete. In questa modalità il traffico può viaggiare contemporaneamente nelle due direzioni. Per operare in modalità Full Duplex, i cavi devono collegare solamente due computer tra loro oppure un computer a uno switch. In pratica, questa modalità, in confronto a <i>Half Duplex</i> , raddoppia la reale capacità della larghezza di banda di una determinata connessione.
Gateway	Altro termine per Router. Viene utilizzato raramente per indicare un router se non in contesti specifici, ad esempio "il router X è il <i>gateway</i> della rete Y".
Half Duplex	Half Duplex è una modalità di traffico di rete. In questa modalità la comunicazione può viaggiare solo in una direzione per volta. Vedere anche <i>Full Duplex</i> .
HTTP	Vedere HyperText Transfer Protocol.

Hub	Un hub è il centro di una <i>LAN</i> , che connette cavi Multiple Ethernet Twisted Pair. Il traffico inviato a un hub viene inoltrato a tutti gli altri computer (e hub) ai quali è connesso. I computer collegati a un hub non possono utilizzare la comunicazione <i>Full Duplex</i> . Vedere anche <i>Switch</i> .
HyperText Transfer Protocol	HTTP è stato utilizzato originariamente per richiedere lo scaricamento di file HTML dai server Web ma nel tempo si è evoluto ed è diventato un protocollo mediante il quale è possibile trasferire file di qualunque tipo e che, in una certa misura, supporta anche il caricamento di file. Vedere anche <i>FTP</i> .
ICMP	Vedere Internet Control Message Protocol.
IMAP	Vedere Interactive Mail Access Protocol.
Interactive Mail Access Protocol	Il protocollo IMAP, come <i>POP3</i> , viene utilizzato per scaricare e-mail da un server di posta e salvarle in una cassetta postale in un computer non connesso costantemente a Internet. Il protocollo IMAP, però, offre maggiore controllo sulla posta che deve rimanere sul server, consentendo di leggere le cassette postali da varie posizioni. La versione attuale del protocollo IMAP è attualmente la quattro, da cui deriva l'acronimo IMAP4. Vedere anche <i>SMTP</i> e <i>POP3</i> .
Internet Control Message Protocol	ICMP viene utilizzato per diagnosticare situazioni e problemi in una rete, ad esempio Internet. ICMP viene trasportato nell'IP. Viene comunemente utilizzato nelle macchine di Pinging per verificare la loro risposta. Vedere anche <i>IP</i> .
Internet Protocol	IP è il protocollo utilizzato nella comunicazione via Internet. Attualmente la versione utilizzata è la 4, che supporta fino a quattro miliardi di indirizzi. IP agisce da carrier per <i>TCP</i> , <i>UDP</i> e <i>ICMP</i> e altri protocolli.
IP	Vedere Internet Protocol.

IPv4	IPv4 è la versione di IP, Internet Protocol, correntemente in uso. Vedere <i>Internet Protocol</i> .
IPv6	IP versione 6. Standard attualmente non completamente sviluppato. Sarà in grado di supportare molti più indirizzi di IPv4, che è lo standard corrente. Vedere <i>Internet Protocol</i> .
IPsec	IPsec è uno standard IP di crittografia e autenticazione della comunicazione o, più brevemente, uno standard <i>VPN</i> . La maggior parte dei produttori di computer e apparecchiature di rete ha scelto di supportare IPsec nei casi in cui viene richiesta la funzionalità VPN.
ISP	Vedere Internet Service Provider.
Internet Service Provider	Azienda che offre connettività ad Internet a utenti finali. Le connessioni possono assumere qualunque forma, dai modem standard alle connessioni via fibre ottiche ad elevata velocità.
LAN	Vedere Local Area Network.
Local Area Network	Una rete LAN è costituita da sistemi di computer collegati da hub e/o switch. Tutti i computer di una LAN possono comunicare tra loro senza passare per un router o un firewall e possono inviare messaggi Broadcast a tutti gli altri computer connessi. Le LAN funzionano generalmente a velocità di 10 Mbps e 100 Mbps. LAN utilizzate comunemente sono <i>Ethernet</i> e <i>Token Ring</i> .
Mbps	Vedere Megabits per Second.
MAC	Media Adapter Card, un'altra definizione di scheda di interfaccia di rete. Vedere anche <i>NIC</i> .
MAN	Vedere Metropolitan Area Network.

Mail Forwarder	Nei casi in cui un server di posta debba venire posto nella rete interna per offrire funzioni avanzate che non possono attraversare un firewall, la pratica corrente è di collocare un Mail Forwarder in una <i>zona demilitarizzata</i> a cui le reti esterne possono inviare la posta. Il Mail Forwarder invia quindi la posta al server di posta interno.
Maximum Segment Size	MSS TCP è il valore che determina il quantitativo di dati che può essere inviato tramite TCP in ciascun pacchetto. Il valore dovrebbe essere determinato dalle due estremità in modo da non causare <i>frammentazione</i> a livello di IP.
Megabits per Second	La velocità di rete viene misurata in Mbps, il numero di bit (zero e uno) che può attraversare la rete ogni secondo. Un byte, che è l'unità di misura dei file, è costituita da otto bit.
Metropolitan Area Network	Una rete MAN è costituita solitamente da una rete a dorsale veloce, composta da anelli in fibra, in grado di connettere utenti di una stessa città reciprocamente e ad Internet. Identico a CAN.
MSS	Vedere Maximum Segment Size.
MTU	Vedere Maximum Transmission Unit.
NAT	Network Address Translation è un termine che comprende tutte le forme di traduzione di indirizzo. Nell'insieme di regole di EnterNet FireWall, NAT si riferisce alla traduzione dinamica di indirizzo, NAT-hide. Vedere anche SAT.
NetBIOS	Un protocollo di rete utilizzato da Microsoft Windows per condividere file, accedere a domini, che può essere trasportato direttamente su Ethernet mediante NetBEUI ma anche mediante TCP/IP.
NIC	NIC è l'abbreviazione di Network Interface Card, ma anche di Network Information Centre.

OS Finger- printing	OS Fingerprinting è una tecnica che rileva le proprietà dei vari sistemi operativi e le utilizza per determinare quale sistema operativo stia utilizzando una determinata macchina senza conoscere molti altri dettagli. Anche se OS Fingerprinting in sé non rappresenta una minaccia per la sicurezza, può comunque essere utilizzato dai pirati informatici nel corso dei lavori preparatori per scoprire quale forma di violazione potrebbe avere successo.
Open Shortest Path First	OSPF è un protocollo utilizzato in una rete delimitata per lo scambio dinamico di informazioni di instradamento. OSPF sta sostituendo RIP come protocollo standard per questo tipo di scambi. Rispetto a RIP, OSPF può gestire informazioni di instradamento più complesse, ricerca percorsi più rapidi nelle reti complesse e supporta anche un certo livello di sicurezza (autenticazione). EnterNet FireWall attualmente non supporta RIP né OSPF. Consultare la sezione delle domande frequenti (FAQ).
OSPF	Vedere Open Shortest Path First.
Passive Mode	FTP in Passive Mode significa che il client FTP crea il canale dei dati nel quale vengono trasferiti i file. Vedere anche <i>FTP e Active Mode</i> .
POP3	Vedere Post Office Protocol.
Post Office Protocol	POP viene utilizzato per scaricare e-mail da un server di posta e inviarle alla cassetta postale di un computer che non sia costantemente connesso a Internet. La versione corrente di POP è la 3, da cui deriva l'acronimo POP3. Vedere anche <i>SMTP e IMAP4</i> .

Proxy ARP	Un firewall o un router possono utilizzare Proxy ARP per segmentare una rete esistente e consentire ai computer nelle due nuove reti di continuare a comunicare direttamente tra loro senza dover modificare la loro configurazione di rete. Quando un computer in una rete chiede la comunicazione con un computer nell'altra rete mediante ARP, il firewall o router risponde utilizzando l'indirizzo hardware della sua scheda di rete. Quando i computer inviano traffico tra loro, il firewall o il router utilizza la sua tabella di instradamento per determinare la direzione in cui devono venire inviati i pacchetti.
RIP	Vedere Routing Information Protocol.
Router	Una macchina che collega due o più LAN, WAN e/o CAN. Un router generalmente determina in quale direzione va inviato il traffico in entrata utilizzando l'indirizzo di destinazione di ciascun pacchetto e la sua tabella interna di instradamento.
Routing Information Protocol	<p>RIP è un protocollo utilizzato all'interno di reti delimitate per lo scambio dinamico di informazioni di instradamento. Il protocollo è molto limitato in termini di funzionalità e sicurezza e per questo motivo è stato sviluppato il protocollo OSPF.</p> <p>EnterNet FireWall attualmente non supporta né RIP né OSPF. Consultare la sezione delle domande frequenti (FAQ).</p>
SAT	<p>Il tipo di regola utilizzato da EnterNet FireWall per la traduzione statica di indirizzo, NAT statica. Per ulteriori informazioni, consultare la sezione 8.1, <small>Traduzione</small> degli indirizzi.</p>
Simple Mail Transfer Protocol	SMTP viene utilizzato per inviare messaggi e-mail ai server di posta. Richiede la connessione più o meno costante del server di destinazione alla rete e quindi non è particolarmente adatto per inviare e-mail a destinatari finali. Vedere anche <i>POP3</i> e <i>IMAP4</i> .
SMTP	Vedere Simple Mail Transfer Protocol.

Stack	<p>1) Un'area dinamica di dati in un computer. Utilizzata dai programmi per memorizzare temporaneamente dati e altri elementi.</p> <p>2) Uno stack TCP o IP è la parte del software di rete del computer che gestisce rispettivamente TCP e IP. Questa definizione di stack non ha alcuna correlazione con quella data nella definizione 1.</p>
Switch	Uno switch svolge approssimativamente la stessa funzione che svolge un hub in una LAN. La differenza è che lo switch consente il passaggio del traffico che lo raggiunge solo verso il computer a cui è destinato. I computer collegati a uno switch possono utilizzare la comunicazione <i>Full Duplex</i> . Vedere anche <i>hub</i> .
TCP	Vedere Transmission Control Protocol.
TCP/IP	Termine generico per la combinazione più comune di protocolli di rete Internet, TCP viene trasportato all'interno di IP. Vedere anche <i>TCP</i> e <i>IP</i> .
Time To Live	I valori TTL vengono utilizzati da numerosi protocolli di rete. L'utilizzo più comune è un pacchetto IP che comincia in un valore compreso tra 32 e 255, a seconda del sistema operativo che lo invia. Il valore TTL viene diminuito da ciascun router che il pacchetto incontra sul percorso verso la sua destinazione. Se TTL raggiunge lo zero, il pacchetto viene scartato. Il motivo principale è la necessità di prevenire loop infiniti tra due o più router.
Transmission Control Protocol	TCP è un protocollo utilizzato dalla maggior parte delle applicazioni di Internet, ad esempio HTTP, FTP e Telenet. Il protocollo TCP viene trasportato all'interno di IP. Il vantaggio offerto da questo protocollo è che garantisce che un pacchetto inviato da A raggiungerà B aspettando conferme e rinvii. Vedere anche <i>IP</i> e <i>UDP</i> .
TTL	Vedere Time To Live.
UDP	Vedere User Datagram Protocol.

User Datagram Protocol	Udp è un protocollo utilizzato da molte applicazioni in tempo reale su Internet. Il protocollo UDP viene trasportato all'interno di IP. UDP non garantisce automaticamente che un pacchetto inviato da A raggiungerà B, offrendo il vantaggio di non dover attendere conferme o rinvii. Vedere anche <i>IP</i> e <i>TCP</i> .
VPN	Vedere Virtual Private Network.
Virtual Private Network	Una connessione crittografata e autenticata su una rete non sicura come Internet, che collega reti locali o client mobili. VPN rappresenta spesso un'alternativa a costi contenuti alle linee dedicate. Esiste uno standard fissato per VPN denominato IPsec. Dal momento che la maggior parte dei fornitori utilizza IPsec, le apparecchiature dei vari produttori sono (o dovrebbero essere) compatibili.
WAN	Vedere Wide Area Network.
Wide Area Network	Una rete WAN è costituita da due o più LAN collegate mediante una serie di bridge, router o firewall. La velocità dei collegamenti WAN è generalmente inferiore a quella di una LAN. Vedere anche <i>LAN</i> e <i>MAN</i> .