IBM eNetwork Firewall per Windows NT

Guida per l'utente

Versione 3 Rilascio 2

GC13-2748-00

IBM eNetwork Firewall per Windows NT

Guida per l'utente

Versione 3 Rilascio 2

GC13-2748-00

Nota: Prima di utilizzare queste informazioni e il prodotto supportato, consultare “Informazioni particolari” a pagina vii.

Prima edizione (marzo 1998)

Questa pubblicazione si riferisce a IBM eNetwork Firewall per Windows NT Versione 3 Rilascio 2 (numero programma 5765-C16) e a tutti i successivi rilasci di questo prodotto salvo diversa indicazione nelle nuove edizioni.

Richieste di ulteriori copie di questo prodotto o informazioni tecniche sullo stesso vanno indirizzate ad un rivenditore autorizzato o ad un rappresentante commerciale IBM. Le pubblicazioni non sono disponibili all'indirizzo riportato di seguito.

Come ultima pagina del manuale è stato predisposto un foglio riservato ai commenti del lettore. Se il modulo è stato rimosso, indirizzare i commenti a:

SELFIN S.p.A.
Translation Assurance
Via F. Giordani, 7
80122 - NAPOLI

Tutti i commenti ed i suggerimenti inviati potranno essere utilizzati dall'IBM e dalla Selfin e diventeranno esclusiva delle stesse.

Indice

Informazioni particolari

I riferimenti contenuti in questa pubblicazione relativi a prodotti, programmi o servizi IBM non implicano che l'IBM intenda renderli disponibili in tutti i paesi in cui opera.

Qualsiasi riferimento a programmi su licenza d'uso o ad altri prodotti IBM contenuto in questa pubblicazione non significa che soltanto tali programmi e/o prodotti possano essere usati.

In sostituzione a quelli forniti dall'IBM, possono essere usati prodotti, programmi o servizi funzionalmente equivalenti che non comportino violazione dei diritti di proprietà intellettuale o di altri diritti dell'IBM.

È responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri programmi e/o prodotti, fatta eccezione per quelli espressamente indicati dall'IBM.

L'IBM può avere brevetti o domande di brevetto in corso relativi a quanto trattato nella presente pubblicazione. La fornitura di questa pubblicazione non implica la concessione di alcuna licenza su di essi. Chi desiderasse ricevere informazioni relative a licenze può rivolgersi per iscritto a:

Director of Commercial Relations IBM Europe
Schoenaicher Str. 220
D-7030 Boeblingen
Deutschland

Coloro che detengono la licenza su questo programma e desiderano avere informazioni su di esso allo scopo di consentire: (i) uno scambio di informazioni tra programmi indipendenti ed altri (compreso questo) e (ii) l'uso reciproco di tali informazioni, dovrebbero rivolgersi:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Queste informazioni possono essere rese disponibili, secondo condizioni contrattuali appropriate, compreso, in alcuni casi, l'addebito di un canone.

Il programma su licenza descritto in questo manuale e tutto il materiale su licenza ad esso relativo sono forniti dall'IBM nel rispetto delle condizioni previste dalla licenza d'uso.

Questa pubblicazione non deve essere riprodotta e viene fornita senza alcuna garanzia, esplicita o implicita. Essa è inoltre da considerarsi solo una guida generale e a titolo indicativo. La IBM Italia si riserva di modificare le caratteristiche tecniche e fisiche nonché i nomi dei prodotti ivi citati, declinando ogni responsabilità per danni diretti o indiretti derivanti da eventuali modifiche.

Questo prodotto comprende software sviluppato dall'Università della California, di Berkeley e dei suoi collaboratori.

Marchi

I seguenti termini, contrassegnati in questa pubblicazione da un asterisco (*), sono marchi dell'IBM Corporation:

- Common User Access
- DB2
- eNetwork
- IBM
- OS/2

Microsoft, Windows, Windows NT ed il logo di Windows 95 sono marchi della Microsoft Corporation.

Java e HotJava sono marchi della Sun Microsystems, Inc.

Nomi di altri prodotti, società e servizi, che potrebbero essere contrassegnati da un un doppio asterisco (**), possono essere marchi di altre società.

Introduzione

Questo manuale descrive come configurare e gestire IBM eNetwork Firewall su un sistema Windows NT** in modo da prevenire comunicazioni indesiderate o non autorizzate all'interno o all'esterno della rete sicura.

Questo manuale è rivolto ai responsabili della sicurezza di rete o del sistema che installano, gestiscono e utilizzano IBM Firewall. Sebbene venga qui descritto in che modo accedere al firewall utilizzando i programmi client, questa non è una guida per l'utente per i programmi client. Per utilizzare i programmi client, quali Telnet o FTP, consultare la guida per l'utente relativa ai programmi client TCP/IP.

Utilizzare le istruzioni per l'installazione contenute nella custodia del CDROM per installare il prodotto prima di utilizzare questo manuale.

Una volta avviato il client di configurazione, le informazioni dell'aiuto in linea forniscono l'assistenza necessaria per l'immissione dei dati nei campi del client di configurazione e per spostarsi da una casella di dialogo all'altra.

Conoscenze di base

È importante avere una buona conoscenza dell'indirizzamento TCP/IP, delle maschere e della gestione di rete prima di installare e configurare IBM Firewall. Dal momento che si è in procinto di installare e configurare un firewall che controlla gli accessi alla rete in entrata e in uscita, è indispensabile avere una conoscenza di base del funzionamento di una rete. In particolare è necessaria una buona familiarità con i principi fondamentali relativi a indirizzi IP, nomi completi e maschere di sottorete.

Un eccellente manuale su TCP/IP, relativo a netstat, arp, ifconfig, ping, nslookup, DNS, sendmail, routing e molto altro ancora è *TCP/IP Network Administration*. Per ulteriori dettagli, consultare la *Bibliografia*.

Un eccellente manuale per i gestori di UNIX, che fornisce anch'esso una panoramica completa su TCP/IP, instradamento, hardware di rete, DNS, e sendmail è *UNIX System Administration Handbook*. Per ulteriori dettagli, consultare la bibliografia.

Funzioni di questo rilascio

IBM eNetwork Firewall per Windows NT offre una grande varietà di funzioni ed include le tre architetture del firewall:

1. Proxy di applicazione
   - FTP
   - HTTP, incluso Gopher e WAIS
   - Telnet
   - SafeMail

   HTTP, Telnet e FTP hanno funzioni di autenticazione.

2. Gateway a livello di circuito tramite il protocollo Socks, versione 5, un Internet standard
3. Filtro - un completo ed efficace insieme di criteri secondo i quali è possibile negare o consentire il traffico. I criteri includono l'indirizzo TCP/IP, la porta, il protocollo, la direzione, l'adattatore (sicuro/non sicuro) e così via.

   Molti servizi predefiniti rendono più rapida la procedura di impostazione.

Socks Protocol Versione 5

Oltre alla semplicità ed alla flessibilità, Socks Protocol Versione 5 presenta i seguenti vantaggi:

- Sviluppo semplificato dei metodi di autenticazione e crittografia
- Associazione UDP, che crea un circuito proxy virtuale per il passaggio dei circuiti proxy basati su UDP
- Socks V5 Watcher, che consente di visualizzare le informazioni sull'esecuzione di socks in tempo reale

Gestione semplificata

Con l'utilizzo di un'applicazione Java**, che è possibile gestire da una macchina remota, si possono eseguire facilmente gli aggiornamenti alla configurazione del firewall. È possibile assegnare diversi livelli di autorizzazione a vari responsabili per favorire il controllo dell'accesso al firewall. Questa singola GUI (graphical user interface), facile da comprendere, può essere utilizzata per gestire entrambi i firewall Windows NT ed AIX.

Hardening di NT

Quando viene installato il firewall, vengono disabilitati i protocolli non TCP/IP, i servizi di sistema non necessari ed i login locali eseguiti da codici di contabilizzazione di utenti diversi dai responsabili.

Autenticazione più efficace

Viene fornito un supporto per tutti i meccanismi di autenticazione a base token comuni, quali SecurID, SecureNet Key e così via.

Programmi di utilità per prospetti

I programmi di utilità per prospetti consentono di eseguire un'interrogazione SQL relativa al log di sistema una volta che tale log è stato esportato in un processo del database.

Avvisi, controllo e log

Un log completo e dettagliato comprende tutte le attività del firewall più l'indirizzo TCP/IP, gli ID utente, TOD, i nomi file, i numeri di porta e così via. Viene fornito il controllo log per verificare tutte le attività sospette e per avvisare che le soglie sono state superate.

Isolamento di più reti

Utilizzando più NIC (Network Interface Cards) sul firewall, è possibile isolare più sottoreti.

Supporto per la lingua nazionale

Il supporto per lingua nazionale viene offerto per l'inglese, il giapponese, il coreano, il francese, il cinese semplificato, il cinese tradizionale, l'italiano, lo spagnolo ed il portoghese brasiliano.

Immissione degli indirizzi IP

Quando si configura il firewall, viene richiesta l'immissione degli indirizzi IP. È possibile immettere un indirizzo IP decimale con punti, con quattro ottetti, nel formato:

```
nnn.nnn.nnn.nnn
```

dove ogni `nnn` è un insieme di tre numeri compresi nell'intervallo 000–255.

Assistenza tecnica IBM

Il centro di assistenza tecnica IBM fornisce assistenza telefonica per l'individuazione e la risoluzione dei problemi. È possibile chiamare il centro di assistenza tecnica IBM in qualsiasi momento; si riceverà una risposta telefonica entro le successive 8 ore lavorative (lunedì–venerdì, 8:00–17:00, ora locale del cliente). Il numero di telefono da chiamare è il seguente: 167-820094. In alternativa, è possibile contattare il rappresentate IBM o il rivenditore autorizzato IBM.

Capitolo 1. Introduzione a IBM Firewall

IBM eNetwork Firewall è un programma per la sicurezza di rete per AIX e Windows NT**. In pratica, un firewall è un sistema di blocco tra una o più reti interne sicure ed altre reti esterne (non sicure) o la rete Internet. Lo scopo di un firewall è di prevenire comunicazioni indesiderate o non autorizzate in entrata o in uscita dalla rete sicura. Le funzioni del firewall sono tre:

- Rafforzare le politiche di sicurezza della rete Internet
- Consentire agli utenti all'interno della propria rete di utilizzare le risorse autorizzate delle reti esterne senza compromettere i dati della rete e le altre risorse
- Impedire l'accesso alla rete agli utenti non autorizzati

Concetti di firewall

La connettività di tipo aperto di Internet può comportare molti rischi di sicurezza. È necessario proteggere i dati privati e l'accesso alle macchine che fanno parte della propria rete da un uso esterno non autorizzato. Il primo passo per raggiungere questo fine consiste nel limitare il numero di punti in cui la rete privata è collegata ad Internet. Una configurazione secondo la quale la rete privata è collegata ad Internet mediante un singolo gateway, consente di controllare il traffico in entrata ed in uscita da Internet. Questo gateway viene detto firewall.

Il seguente esempio può aiutare a capire il modo in cui funziona un firewall, Si immagini un edificio cui si desidera limitare l'accesso e controllare coloro che vi entrano. L'edificio ha un solo atrio, che è l'unico punto di ingresso. In quest'atrio ci sono degli addetti che danno il benvenuto alle persone che entrano nell'edificio, dei responsabili della sicurezza che li controllano, delle videocamere che registrano le loro azioni e dei lettori di cartellini di identificazione che ne autenticano l'identità.

Questa procedura è molto efficace nel controllo dell'ingresso ad un edificio privato. Ma se una persona non autorizzata riesce a superare l'atrio, non c'è alcun modo per proteggere l'edificio dalle azioni di questa persona. Tuttavia, se si supervisionano gli spostamenti di questa persona, è possibile rilevare eventuali comportamenti sospetti.

Quando si definisce la propria strategia di firewall, si può pensare che sia sufficiente la proibire l'ingresso solo a tutto quanto si ritiene rappresenti un rischio per l'organizzazione. Ma, a causa dei nuovi metodi di attacco, occorre anticipare il modo in cui prevenire questi attacchi e, come nel caso dell'edifico, occorre controllare i segni che possono indicare l'eventuale violazione dei propri sistemi di difesa. È generalmente molto più pericoloso e costoso il ripristino di una violazione che la sua prevenzione.

Tool di IBM Firewall

IBM Firewall rappresenta un insieme di tool utilizzati per implementare le diverse architetture del firewall. Una volta scelta la propria architettura e la propria strategia di sicurezza, vengono selezionati i tool IBM Firewall necessari. Il client di configurazione di IBM Firewall fornisce un'interfaccia utente grafica semplificata. IBM Firewall fornisce funzioni di log complete di tutti gli eventi di rilievo, quali le modifiche alla gestione ed i tentativi di violazione della sicurezza.

Poiché IBM Firewall è, a conti fatti, un gateway IP, esso divide il mondo in due o più reti: una o più reti non sicure e una o più reti sicure. La rete non sicura è, ad esempio, Internet. Le reti sicure sono di solito reti IP aziendali. Alcuni tool offerti da IBM Firewall sono:

- Filtri avanzati
- Server proxy
- Server socks
- Servizi specifici come DNS (domain name service) e SafeMail

Filtri avanzati

I filtri avanzati sono tool che esaminano i pacchetti a livello di sessione in base a più criteri, come l'ora del giorno, l'indirizzo IP e la sottorete. Le regole di filtro utilizzano la funzione gateway IP e pertanto occorre che la macchina abbia due o più interfacce di rete, ognuna delle quali in una rete o sottorete IP diversa. Un insieme di interfacce è dichiarato non sicuro e l'altro insieme è dichiarato sicuro. Il filtro è attivo tra queste due interfacce, come illustrato nella Figura 1.

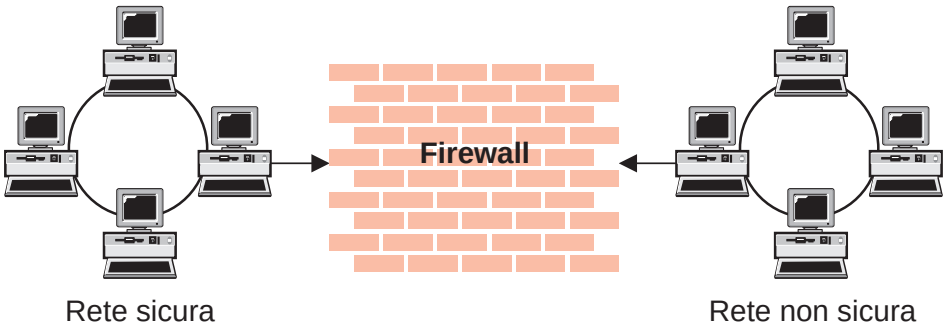

Figura 1. Firewall con filtri avanzati

Funzione dei filtri avanzati

I filtri avanzati forniscono al firewall un meccanismo di protezione di base. Tali filtri consentono all'utente di determinare il traffico sul firewall in base ai dettagli della sessione IP, proteggendo così la rete sicura da minacce esterne, quali la ricerca di server sicuri e l'indicazione di falsi indirizzi IP. La funzione di filtro può essere considerata la base su cui vengono create le altre funzioni.

Server proxy

A differenza dei filtri, che controllano semplicemente i pacchetti in transito, i server proxy sono applicazioni che fanno parte del firewall e che svolgono funzioni TCP/IP specifiche per un utente di rete. L'utente contatta il server proxy utilizzando una delle applicazioni TCP/IP (Telnet o FTP). Il server proxy contatta l'host remoto per conto dell'utente, per poter controllare l'accesso nascondendo allo stesso tempo la struttura della rete agli utenti esterni. La Figura 2 illustra un server proxy telnet che intercetta una richiesta da un utente esterno.

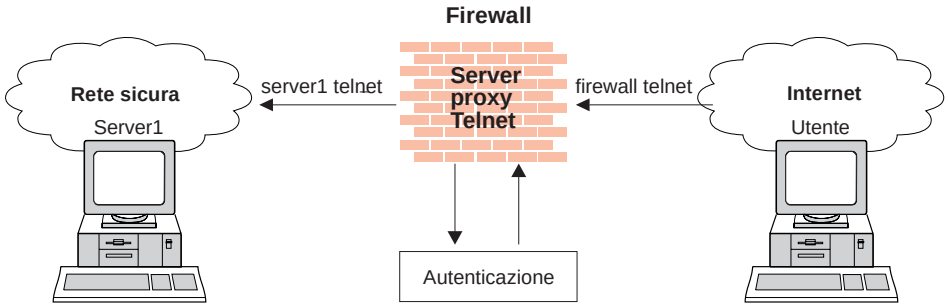

Figura 2. Firewall con un server proxy

I servizi proxy disponibili sono telnet, FTP, HTTP, WAIS, GOPHER, HTTPS e SafeMail.

I server proxy di IBM Firewall possono eseguire l'autenticazione degli utenti mediante una serie di metodi diversi di autenticazione. Gli utenti possono accedere ad informazioni utili su Internet senza compromettere la sicurezza delle loro reti interne.

Obiettivi dei server proxy

Quando ci si collega tramite un server proxy, i collegamenti TCP/IP sul firewall vengono interrotti e pertanto le possibilità di rischio per la rete sicura vengono ridotte. Gli utenti devono inoltre provvedere allo loro autenticazione, utilizzando uno dei metodi di autenticazione.

Uno dei principali vantaggi dei server proxy è la possibilità di nascondere gli indirizzi. Tutti i collegamenti proxy in partenza utilizzano l'indirizzo del firewall. Un altro grande vantaggio dei server proxy è rappresentato dalla sicurezza. Gli esperti IBM hanno sviluppato infatti i server proxy in modo da poter far fronte ai problemi di sicurezza che possono verificarsi sulla macchina client.

Un altro vantaggio del server proxy è che non occorre una versione speciale del programma client sulla macchina client. Pertanto, una volta installato il firewall, ogni utente registrato nel firewall può avere accesso alla rete non sicura senza dover provvedere all'installazione di software aggiuntivo.

Server Socks

Socks è uno standard per i gateway a livello di circuito che fornisce la possibilità di nascondere l'indirizzo senza richiedere il tempo di elaborazione di un server proxy più convenzionale.

Il server Socks è simile ad un server proxy, in quanto per entrambi la sessione viene interrotta sul firewall. La differenza risiede nel fatto che il socks può

supportare tutte le applicazioni, mentre il proxy deve essere univoco per ciascuna applicazione. In modo trasparente, il client Socks avvia una sessione con il servizio Socks di Windows NT sull'host di IBM Firewall e verifica quindi che l'indirizzo di origine e l'ID utente siano autorizzati a stabilire un collegamento nella rete non sicura e crea così la seconda sessione. La Figura 3 illustra un firewall con un server socks.

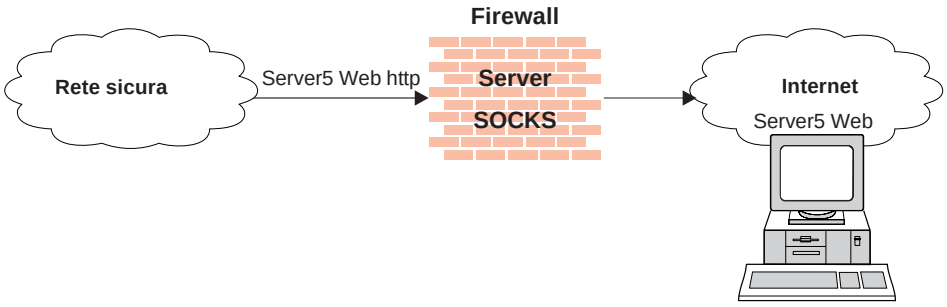

Figura 3. Firewall con un server socks

I client con socks (client che riconoscono i Socks) sono disponibili con molte applicazioni, ad esempio Netscape Navigator** o Microsoft** Internet Explorer, o con il software di TCP/IP vale a dire Aventail** AutoSocks**.

Obiettivi del server socks

Per le sessioni in uscita (da un client sicuro ad un server non sicuro), il server socks ha gli stessi obiettivi di un server proxy: interrompere la sessione sul firewall e fornire una porta sicura per poter accedere alla quale gli utenti devono provare la loro identità. Ciò comporta per l'utente il vantaggio della semplicità ed un minimo di lavoro di gestione supplementare.

DNS (Domain Name Service)

L'accesso ai record dei nomi dominio relativo alla rete sicura aiuta moltissimo gli intrusi, in quanto fornisce loro un elenco degli host da attaccare. Anche un server DNS sovvertito può fornire una via di accesso ad un pirata dell'informatica. Dalla rete esterna, il server nomi del firewall riconosce solo se stesso e non fornisce mai informazioni sulla rete IP interna. Dalla rete interna, questo server nomi riconosce la rete Internet ed è molto utile per accedere per nome a qualsiasi macchina collegata ad Internet.

Obiettivi del server DNS

L'esecuzione del server DNS sul firewall presenta il duplice vantaggio di impedire che le richieste di risoluzione dei nomi passino attraverso il firewall e di nascondere gli host della rete sicura al mondo esterno.

SafeMail

La posta è una delle ragioni principali per cui un'organizzazione desidera accedere ad Internet. SafeMail è un gateway di posta IBM che ha la funzione di nascondere i nomi dominio della rete interna. La funzione SafeMail non memorizza la posta nel gateway e non viene eseguita con l'ID utente root. Il nome dominio pubblico del gateway del firewall sostituisce il nome dominio privato per la posta in uscita per cui la posta sembra provenire dall'indirizzo del firewall e non da quello dell'utente. SafeMail supporta SMTP (Simple Mail Transfer Protocol) e MIME (Multipurpose Internet Mail Extensions).

Utilizzo di Network Security Auditor

Network Security Auditor controlla la rete per rilevare eventuali rischi per la sicurezza o errori di configurazione. Network Security Auditor analizza i server ed i firewall per evidenziarne i problemi ed i punti deboli, ad esempio le porte aperte e compila un elenco per consentire all'utente di eseguire le correzioni. Network Security Auditor può essere utilizzato per l'analisi periodica degli host di particolare importanza oppure come un tool di raccolta delle informazioni. La gestione di Network Security Auditor viene eseguita mediante un'interfaccia della riga comandi facile da utilizzare. Con Network Security Auditor è possibile tenere sotto controllo il firewall.

Le funzioni di Network Security Auditor includono:

- scansione delle porte TCP e UDP
- riconoscimento dei server su porte non standard
- prospetto su servizi pericolosi, punti deboli noti, versioni obsolete del server e server o servizi che violano la politica di sito personalizzata
- creazione di prospetti in formato HTML per una facile visualizzazione tramite browser

Capitolo 2. Pianificazione

Prima di configurare IBM Firewall, utilizzare l'elenco di controllo ed i fogli di lavoro per la pianificazione per un aiuto nella configurazione della rete.

Elenco di controllo per la pianificazione

1. Definire lo scopo che si intende raggiungere. Si desidera:
   - Accedere ad Internet (telnet, FTP anonimo e così via)?
   - Eseguire una partizione della rete interna?
   - Consentire l'accesso *esterno* alla propria rete?
2. Valutare la topologia della rete a livello di sottorete IP.
   - Si ritiene che un'interfaccia sicura ed una non sicura costituiscano una configurazione corretta?
   - Gli indirizzi di cui si dispone supportano le maschere di sottorete presenti nelle regole?
3. Stabilire in quale modo si desidera utilizzare DNS. Fare riferimento al Capitolo 6, “Gestione del DNS (Domain Name Service)” a pagina 31.
4. Stabilire in che modo si desidera utilizzare safemail. Fare riferimento al Capitolo 7, “SafeMail” a pagina 39.
5. Se si desidera utilizzare il socks, accertarsi che siano installati i client con socks, ad esempio il browser Netscape Navigator o Microsoft. Per informazioni sull'utilizzo di socks, fare riferimento al Capitolo 11, “Configurazione del server Socks” a pagina 69.
6. Qual'è il tipo di autenticazione richiesto?
   - Se si prevede di utilizzare Security Dynamics** ACE/Server** per l'autenticazione degli utenti, installare il codice del client ACE/Server sull'host del firewall. Si consiglia di installare il codice del server ACE/Server su un altro host all'interno della rete sicura.

     Per informazioni sull'installazione e l'uso di Security Dynamics ACE/Server e della scheda SecurID**, fare riferimento alle informazioni fornite dalla Security Dynamics Technologies Inc.
   - Se si prevede di utilizzare la scheda SecureNet Key** della AssureNet Pathways**, acquistare le schede separatamente da IBM Firewall.
   - Se si utilizza un proprio metodo di autenticazione, fare riferimento al capitolo Metodi di autenticazione personalizzati in *IBM eNetwork Firewall - Manuale di riferimento*.
   - È necessario configurare il codice del client Windows, mediante il quale è possibile ricercare i domini Windows NT sicuri per scopi di autenticazione, all'uso di TCP invece di NETBIOS. NETBIOS viene disabilitato. I server Windows NT sicuri devono conoscere i nomi e gli indirizzi degli host TCP/IP e deve esistere un collegamento TCP/IP fra i server Windows NT ed il firewall. Per poter consentire il traffico, è necessario che il responsabile del firewall crei i collegamenti tra il firewall ed i server NT sicuri.

     Impostare il collegamento mediante i servizi predefiniti di seguito riportati:

a. Autenticazione Domain Controller - che consente l'uso di Domain Controller per l'autenticazione dell'utente

b. NetBT Name Services broadcasts - che consente trasmissioni broadcast NetBIOS su servizi di nome TCP/IP

Programmi di utilità per la configurazione NT per definire relazioni sicure.

7. Se si fa uso dei filtri, cominciare con regole di filtro semplici e renderle estremamente restrittive. Acquisire familiarità con porte e protocolli utilizzati dai servizi di cui si ha bisogno.
8. Stabilire un metodo per l'archiviazione dei file di log. L'archiviazione rappresenta il metodo ideale per un lavoro pianificato nel servizio Windows NT Scheduler. Fare riferimento al Capitolo 15, “Gestione dei file di log e di archivio” a pagina 107.

Foglio di lavoro per la pianificazione della configurazione di rete

Completare il foglio di lavoro con le informazioni come parte del processo di pianificazione della configurazione di IBM Firewall.

Nome host del firewall _____

Interfacce di rete sicure (collegate alla rete sicura interna)

Indirizzo IP _____ Maschera di sottorete _____

Indirizzo IP _____ Maschera di sottorete _____

Indirizzo IP _____ Maschera di sottorete _____

Indirizzo IP _____ Maschera di sottorete _____

Interfacce di rete non sicure (collegate alla rete non sicura)

Indirizzo IP _____ Maschera di sottorete _____

Indirizzo IP _____ Maschera di sottorete _____

Indirizzo IP _____ Maschera di sottorete _____

Indirizzo IP _____ Maschera di sottorete _____

Nome del router _____

Indirizzo del router _____

Nome dominio sicuro _____

Indirizzo IP del DNS (domain name server) sicuro _____

Indirizzo IP dei DNS (Domain Name Server) non sicuri _____

Server di posta sicuro _____

Nome Dominio Pubblico _____

Indirizzo IP del client di configurazione _____

Indirizzo IP dei client remoti

Indirizzario root del firewall Windows NT _____
(Viene indicato come ROOTDIR nell'intera documentazione)

c:\winnt (Si presume che Windows NT sia installato in questo indirizzario)

Capitolo 3. Impostazione del server di configurazione e del client di configurazione

Questo capitolo descrive come impostare il server di configurazione ed il client di configurazione, vale a dire l'interfaccia utente grafica (GUI) per IBM Firewall.

Impostazione del server di configurazione

Il server di configurazione è l'interfaccia del client di configurazione con il firewall. Il server di configurazione elabora le richieste del client di configurazione. Tale server viene eseguito sulla macchina firewall ed è in grado di gestire le richieste dei client di configurazione presenti sulle macchine locali o remote. Una volta impostato, il server diventa parte della macchina firewall.

Il numero di porta del server di configurazione è specificato nel file services di NT, presente nell'indirizzario in cui è stato installato il sistema operativo Windows: `c:\winnt\system32\drivers\etc\services`. Il numero di porta viene impostato per valore assunto su 1014 ma è possibile modificare tale valore, per motivi di sicurezza, arrestando il servizio del server di configurazione, modificando il file dei servizi e riavviando il servizio del server di configurazione.

Il server di configurazione viene inizialmente impostato in modo da accettare solo le richieste dei client di configurazione presenti sulla macchina locale. Le richieste iniziali non vengono crittografate. Per modificare queste opzioni, utilizzare `fwcfgsrv cmd=change` dalla riga comandi.

localonly= Indica se il firewall può essere gestito soltanto da una macchina locale.

- **localonly=yes** La configurazione può essere eseguita solo dalla macchina locale; questo è il valore assunto.
- **localonly=no** La configurazione può essere eseguita da qualsiasi macchina.

encryption Indica se il server di configurazione prevede che i dati in arrivo vengano crittografati o meno mediante ssl (secure sockets layer).

Se le opzioni encryption o sslfile vengono modificate, è necessario arrestare e riavviare il servizio del server di configurazione.

- **encryption=none** Non verrà eseguita alcuna crittografia; questo è il valore assunto.
- **encryption=ssl** Verrà eseguita la crittografia SSL.

sslfile= Indica il nome del file di chiavi SSL da utilizzare con la crittografia SSL; il valore assunto è `ROOTDIR\config\fwkey.kyr`. *ROOTDIR* è l'indirizzario selezionato durante il processo di installazione come ubicazione di destinazione per IBM Firewall. Per informazioni su come creare il file di chiavi, consultare *IBM eNetwork Firewall - Manuale di riferimento.*

Se un client di configurazione non può collegarsi alla macchina firewall e si trova su una macchina diversa, utilizzare `fwcfgsrv cmd=list` per controllare che sia impostato il valore `localonly=no`. È necessario inoltre che il client ed il server utilizzino la stessa lingua. Accertarsi, infine, che il servizio del server di configurazione sia in esecuzione portando in primo piano il pannello dei servizi e controllandone lo stato. Per fare ciò, andare al pannello di controllo e fare doppio clic sull'icona Servizi per controllare lo stato di ciascun servizio. Se il servizio non è in esecuzione, è necessario riavviarlo.

Impostazione del client di configurazione (GUI)

Quando si installa IBM Firewall, il client di configurazione viene installato automaticamente. Il client di configurazione può anche essere installato separatamente su una macchina Windows NT senza il firewall, il che consente di eseguire la gestione remota. Per avviare il client di configurazione, fare doppio clic sull'icona del client di configurazione nel gruppo di programmi IBM Firewall. Una volta avviato il client di configurazione, è necessario collegarsi al firewall utilizzando il codice di contabilizzazione del responsabile di Windows NT.

Solo i responsabili Windows NT ed i responsabili del firewall che dispongono dell'autenticazione di gestione adeguata possono utilizzare il client di configurazione per collegarsi al firewall.

Una volta installato il firewall, tutti i responsabili Windows NT vengono designati come responsabili principali del firewall. Utilizzare il client di configurazione per collegarsi al server di configurazione come responsabile principale del firewall e, se necessario, definire altri nomi utente dei responsabili del firewall. Per ulteriori informazioni su come definire i responsabili del firewall utilizzando il client di configurazione, consultare il Capitolo 12, “Gestione degli utenti del firewall” a pagina 75.

Per impostare il valore di timeout del collegamento relativo a macchine più voloci o più lente, apportare la seguente modifica facendo clic sull'icona del client di configurazione di IBM Firewall, e successivamente su **Caratteristiche**. Modificare le caratteristiche utilizzando la scheda di **accesso rapido**. Impostare il parametro `timeout` su *20*, dove 20 è il numero di secondi da attendere per stabilire il collegamento. Per le macchine più veloci è possibile impostare questo valore su 10 mentre per quelle più lente si consiglia di accettare il valore assunto.

Per aumentare il livello delle informazioni di debug nella console JAVA, eseguire `ibmfw.bat` in `ROOTDIR\cfgcli\gui` invece di utilizzare l'icona del client di configurazione. L'abilitazione del log di console può tuttavia ridurre le prestazioni.

Collegamento al client di configurazione

Per il collegamento al client di configurazione (sulla macchina locale o remota):

- L'utente deve essere un responsabile del firewall
- Il responsabile del firewall deve possedere uno schema di autenticazione definito. Fare riferimento alla sezione “Metodi di autenticazione utente” a pagina 81.
- L'utente deve essere in possesso dell'autorizzazione ad eseguire funzioni di configurazione specifiche

Abilitazione della configurazione remota tramite il client di configurazione

Per abilitare la configurazione remota tramite il client di configurazione, assicurarsi che sulla macchina firewall del responsabile che sta per eseguire il collegamento siano definiti i seguenti attributi:

- Se il responsabile si trova sul lato sicuro della rete e sta utilizzando un'interfaccia sicura sulla macchina firewall, deve essere definito con il metodo di autenticazione corretto per la gestione sicura (non può essere impostato su "deny all"). Questa condizione è valida per i collegamenti locali al firewall.
- Analogamente, se il responsabile si trova sul lato non sicuro e sta utilizzando un'interfaccia non sicura sulla macchina firewall, deve essere definito con il metodo di autenticazione corretto per la gestione non sicura (non può essere impostato su "deny all").

È possibile impostare tutti gli attributi utente mediante la casella di dialogo Modificare Utente del client di configurazione o mediante il comando `fwuser`. Per tutti i responsabili del firewall tutti i campi indicati precedentemente saranno adeguatamente impostati dopo l'installazione del firewall. Per ulteriori informazioni, consultare il Capitolo 12, “Gestione degli utenti del firewall” a pagina 75.

Esempio di un'emissione di log relativa al server di configurazione remoto

Di seguito viene riportato un esempio dell'emissione di log relativa al server di configurazione remoto:

```
Feb 03 13:52:15 1998 mr16n18: ICA9005i: Avvio del server di configurazione remoto in corso.

Feb 03 13:52:21 1998 mr16n18: ICA2024i: Utente responsabile autenticato
correttamente mediante l'autenticazione NT dalla rete sicura:127.0.0.
Feb 03 13:52:21 1998 mr16n18: ICA2169i: Utente responsabile autenticato
correttamente per il server di gestione remoto mediante NT dalla rete sicura:127.0.0.1.
```

Capitolo 4. Utilizzo del client di configurazione

Utilizzare il client di configurazione, vale a dire un'interfaccia utente grafica, per configurare e gestire IBM Firewall.

Quando si installa per la prima volta, IBM Firewall viene inizialmente impostato in modo da accettare solo le richieste dei client di configurazione presenti sulla macchina locale. È possibile tuttavia installare il client di configurazione su un'altra macchina e gestire il firewall in modo remoto. Per ulteriori informazioni, consultare la sezione “Impostazione del server di configurazione” a pagina 11.

Per impostare il client di configurazione in modo che venga avviato nella lingua relativa alla 'locale' specificata, fare clic sull'icona del client di configurazione di IBM Firewall, quindi fare clic su **Caratteristiche**. Modificare le caratteristiche utilizzando la scheda di **accesso rapido**. Per valore assunto, viene utilizzata la 'locale' della macchina host. IBM Firewall supporta queste 'locale':

- en_US - Inglese americano
- ja_JP - Giapponese EUC
- Ja_JP - Giapponese PC
- ko_KR - Coreano
- zh_CN - Cinese semplificato EUC
- zh_TW - Cinese tradizionale (lingua Taiwanese)
- Zh_TW - Cinese tradizionale [Big 5]
- fr_FR - Francese
- it_IT - Italiano
- pt_BR - Portoghese brasiliano
- es_ES - Spagnolo
- Es_ES - Spagnolo PC

Per utilizzare il client di configurazione è necessario un mouse.

Nella parte superiore del pannello principale del client di configurazione si trova un pulsante **Aiuto**. Fare clic su **Aiuto** per informazioni sulle varie funzioni.

Collegamento al client di configurazione

1. Per Tipo di collegamento, selezionare Locale se si utilizza la stessa macchina su cui è installato il firewall. Locale è il valore assunto. Selezionare Remoto se si desidera accedere in modo remoto ad un altro firewall. Il collegamento di tipo Remoto richiede l'immissione di un nome host.
2. Se è stato selezionato il collegamento Remoto, è necessario immettere il nome host o l'indirizzo IP della macchina firewall a cui ci si desidera collegare.
3. In base al tipo di crittografia utilizzato per il firewall, selezionare SSL o Nessuno. Per il client, il valore assunto per l'opzione Locale è Nessuno mentre per l'opzione Remoto è SSL.

4. Immettere il nome utente di un responsabile del firewall o di un responsabile di Windows NT.
5. Immettere il numero di porta su cui è in ascolto il server. Il valore assunto è 1014.
6. Per Modo, selezionare Host se si desidera configurare la macchina firewall Windows NT cui ci si sta collegando. Con una gestione host, il responsabile può aggiornare, in modo locale o remoto, un firewall alla volta. Selezionare Enterprise per la gestione EFM (Enterprise Firewall Management) dei firewall AIX.
7. Una volta eseguito il collegamento, verranno visualizzati dei messaggi di autenticazione e, se questo è il metodo di autenticazione impostato per il proprio nome utente, è possibile che venga richiesta l'immissione di una parola d'ordine. Se richiesta, immettere la parola d'ordine nel campo Risposta Utente e premere Invio oppure fare clic su Inviare. Se la parola d'ordine immessa non è corretta, viene visualizzato un messaggio. Fare clic su Chiudere e riavviare il processo di collegamento. Se non viene richiesta alcuna parola d'ordine, il metodo di autenticazione dell'utente può essere Consentire tutto. In questo caso, viene immediatamente visualizzato il pannello del client di configurazione di IBM Firewall.
8. Una volta eseguita correttamente l'autenticazione, verrà visualizzato il pannello di configurazione principale.

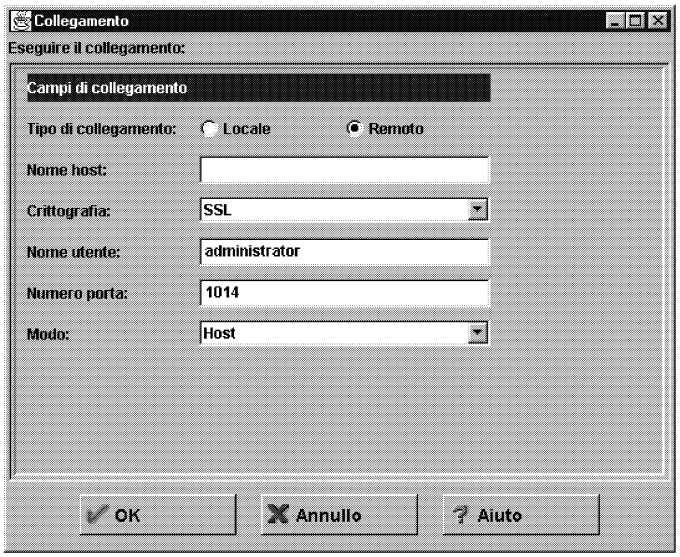

Figura 4. Pannello di collegamento al client di configurazione

Albero di navigazione

Il client di configurazione presenta sul lato sinistro un pannello riducibile con struttura ad albero di ausilio per la navigazione , come illustrato nella Figura 5 a pagina 17.

Se un nodo o una funzione contengono delle voci, a sinistra del nodo o delle funzioni viene visualizzata un'icona di cartella di file. Per visualizzare le funzioni secondarie è possibile espandere la vista facendo doppio clic sull'icona. Facendo di

nuovo doppio clic sull'icona la vista del nodo viene nuovamente ridotta e riportata alle dimensioni originarie.

Se si fa clic su una funzione, quella funzione viene ritenuta selezionata e viene evidenziata. È possibile espandere e ridurre i nodi senza modificare la vista della finestra a destra. Quando l'albero supera lo spazio verticale disponibile, sulla destra dell'albero di navigazione viene visualizzata una barra di scorrimento. Se un nome funzione non rientra nell'albero di navigazione, viene visualizzata una barra di scorrimento orizzontale.

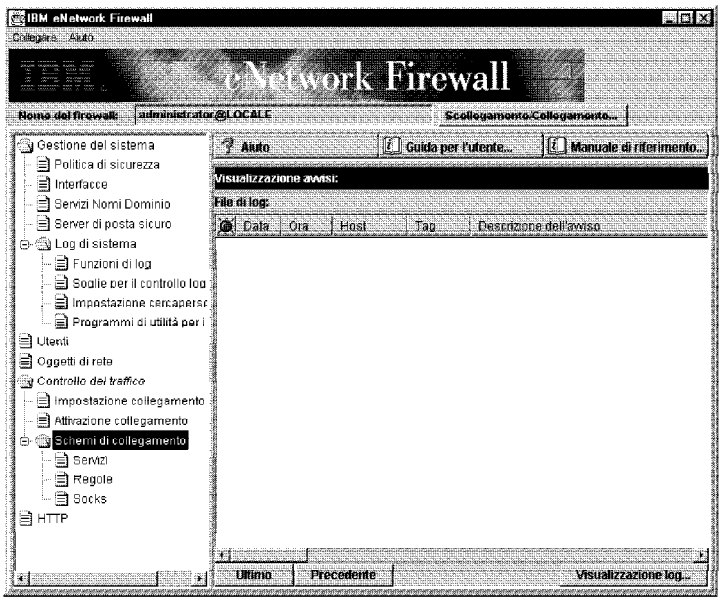

Figura 5. Albero di navigazione del client di configurazione

Funzioni generali del pannello principale

Nella parte superiore del pannello **Visualizzazione avvisi** sono presenti tre pulsanti, come illustrato nella Figura 5.

Aiuto Nella parte superiore del pannello principale del client di configurazione si trova un pulsante **Aiuto**. Fare clic su **Aiuto** per visualizzare le informazioni su come come rendere operativo IBM Firewall.

Guida utente Nella parte superiore del pannello principale del client di configurazione si trova un pulsante **Guida utente**. Fare clic su **Guida utente** per visualizzare la Guida per l'utente in formato elettronico.

Riferimento Nella parte superiore del pannello principale del client di configurazione si trova un pulsante **Riferimento**. Fare clic su **Riferimento** per visualizzare il Manuale di riferimento in formato elettronico.

Gli altri pulsanti presenti sul pannello principale sono:

Ultimo Nella parte inferiore del pannello principale del client di configurazione si trova un pulsante **Ultimo**. Fare clic su **Ultimo** per visualizzare gli avvisi più recenti.

Scollegamento/Collegamento

Nella parte superiore destra del pannello principale del client di configurazione si trova un pulsante **Scollegamento/Collegamento**. È un pulsante di ricollegamento. È possibile riavviare la sequenza di collegamento ad un firewall diverso oppure collegarsi come un responsabile diverso.

Per scollegarsi, fare clic su Scollegamento poi fare clic su Annullo nel pannello di collegamento, quindi fare clic sull'applicazione.

Visualizzazione Log

Nella parte inferiore destra del pannello principale del client di configurazione si trova un pulsante **Visualizzazione log**. Consente di esaminare i log del firewall.

Precedente

Nella parte inferiore del pannello principale del client di configurazione si trova un pulsante **Precedente**. Fare clic su **Precedente** per visualizzare gli avvisi precedenti.

Visualizzazione avvisi

È possibile visualizzare i record di avviso generati dal programma di controllo dei log di sistema nella parte inferiore destra della finestra principale del client di configurazione, come illustrato nella Figura 6 a pagina 19.

I record di avviso visualizzati sono ricavati dal file identificato dalla prima funzione `log avvisi` definita in `ROOTDIR\config\syslog.conf`. Se non è definita alcuna funzione `log avvisi`, sullo schermo non verrà visualizzato alcun dato. Consultare la sezione “Aggiunta delle funzioni di log” a pagina 108 per un aiuto nella definizione della funzione `log avvisi`.

Sul pannello vengono visualizzati il nome del file degli avvisi ed i relativi numeri di riga correntemente visualizzati. È possibile fare clic su **Ultimo** per visualizzare gli avvisi più recenti. Fare clic su **Precedente** per visualizzare gli avvisi precedenti.

Ogni riga visualizzata contiene la data e l'ora di emissione dell'avviso, il nome host del firewall su cui si è verificato, la tag ed il testo del messaggio di avviso. La tag è un'indicazione del tipo di avviso.

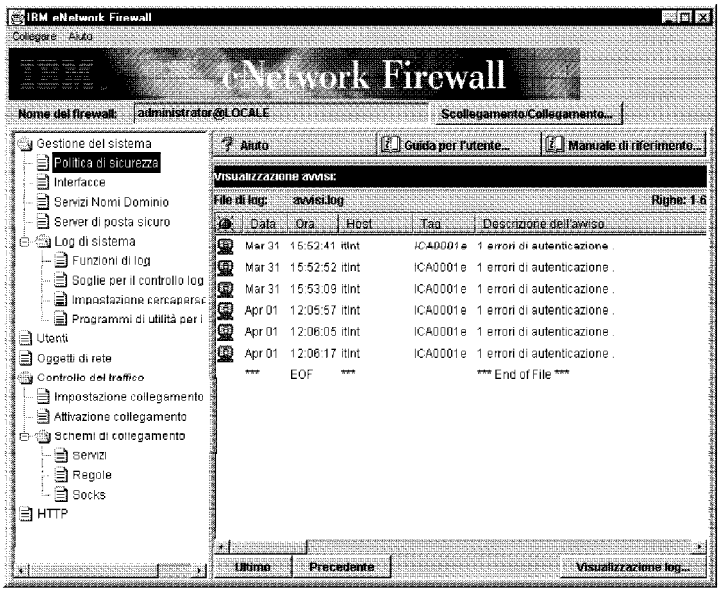

Figura 6. Visualizzazione avvisi

Visualizzazione log

Quando si fa clic su **Visualizzazione log** viene visualizzata un finestra di visualizzazione, come illustrato nella Figura 7 a pagina 20. La finestra Visualizzazione log consente di visualizzare i record dei log del firewall. È possibile specificare un file di log ed un numero di record (il valore assunto è 25).

Il log assunto è il file identificato dalla prima funzione `log firewall` definita in `ROOTDIR\config\syslog.conf`. Dal menu sviluppo azione del campo relativo al nome file è possibile selezionare un file di log di destinazione diverso oppure è possibile immettere il nome di un file da visualizzare.

Per richiedere una riga di inizio specifica, fare clic su **Iniziare a riga:**, dopo aver immesso il numero di riga nel campo vicino. Per richiedere l'ultima riga, fare clic su **Fine**, che consente di andare alla fine del file. Il pulsante **Successivo** consente di andare all'insieme successivo di righe presente nel file. Il pulsante **Precedente** consente di ritornare all'insieme precedente di righe presente nel file. Il pulsante **Inizio** consente di andare all'inizio del file. Facendo clic su **Sì**, è possibile espandere i log del firewall su un testo leggibile.

Consultare la sezione “Creazione dei file di log e di archivio utilizzando il client di configurazione” a pagina 107 ed il Capitolo 14, “Controllo dei log del firewall” a pagina 97 per ulteriori informazioni sui file di log, le funzioni, i controlli e gli avvisi.

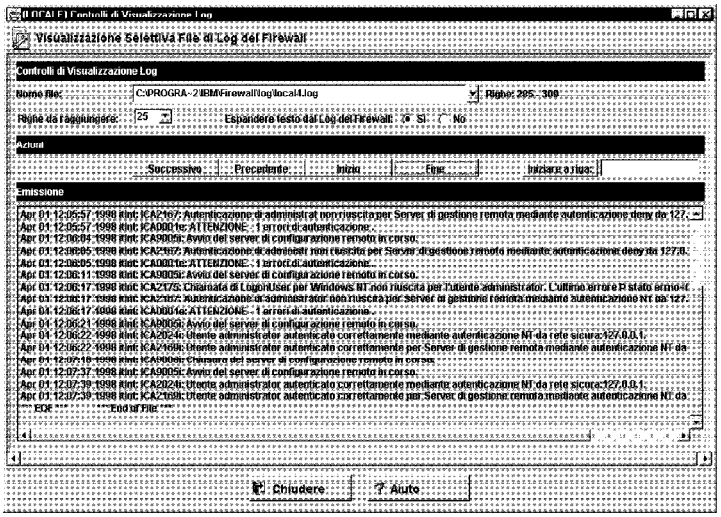

Figura 7. Visualizzazione log

Altre funzioni

Nella parte superiore sinistra di alcuni pannelli si trova un campo **Ricercare**. È possibile immettere una stringa di ricerca e fare clic su **Trovare**.

Gli altri pulsanti nelle caselle di dialogo del client di configurazione sono:

Applicare Fare clic su **Applicare** per immettere nel campo del pannello precedente i dati della selezione corrente e per salvare le modifiche apportate. Quando si fa clic su **Applicare** non di determina la chiusura della finestra.

Fine Fare clic su **Fine** per andare alla fine del pannello.

Annullo Fare clic su **Annullo** per chiudere la finestra senza salvare le modifiche apportate.

Chiudere Fare clic su **Chiudere** per chiudere la finestra correntemente visualizzata.

Copiare Il pulsante **Copiare** permette di risparmiare del tempo quando si aggiungono delle nuove voci all'elenco. Dopo avere selezionato una voce dall'elenco, fare clic su **Copiare** per creare una voce simile a quella selezionata. Quando si fa clic su **Copiare**, viene creata una nuova voce in cui vengono copiati i valori dei campi contenuti nella voce selezionata dall'elenco. È possibile quindi procedere alla modifica di questi valori per adeguarli alle esigenze di questa nuova voce.

Eliminare Fare clic su **Eliminare** per eliminare una voce selezionata dall'elenco.

Spostare giù Selezionare una voce nell'elenco e fare clic su **Spostare giù** per spostare verso il basso la posizione della voce nell'elenco. Ogni volta che si fa clic la voce viene spostata verso il basso di una posizione.

Spostare su Selezionare una voce nell'elenco e fare clic su **Spostare su** per spostare verso l'alto la posizione della voce nell'elenco. Ogni volta che si fa clic la voce viene spostata verso l'alto di una posizione.

OK Fare clic su **OK** per salvare le modifiche apportate e per chiudere la finestra.

Aprire Dopo avere selezionato una voce nell'elenco, fare clic su **Aprire** per visualizzarla o modificarla. Per aggiungere una nuova voce, fare clic su **NUOVO**, quindi fare clic su **Aprire**.

Rigenerare Fare clic su **Rigenerare** per accedere nuovamente ai dati dal firewall e per visualizzarli sul pannello.

Rimuovere Fare clic su **Rimuovere** per eliminare la voce selezionata dall'elenco. Questa azione si limita a rimuovere la voce dall'elenco. Non ha infatti alcun effetto sulle altre definizioni di questa voce.

Selezionare Fare clic su **Selezionare** per accedere ad un elenco di voci selezionabili valide per questa funzione.

Inizio Fare clic su **Inizio** per andare all'inizio del pannello.

Campi comuni

I campi comuni presenti nelle caselle di dialogo del client di configurazione sono:

Emissione Questo campo contiene le informazioni sull'andamento del comando avviato.

Nome Fornire un nome per questa voce. Per questa specifica funzione del firewall, il nome di voce deve essere univoco . Questo nome NON deve contenere un simbolo di pipe(|), un carattere di singolo apice o apostrofo (') oppure un carattere di doppio apice (") in quanto tali caratteri vengono utilizzati come delimitatori di file e SMIT. L'uso di questi caratteri fornisce dati non attendibili.

Descrizione Questo campo è facoltativo ed è fornito nel caso in cui si desideri fornire un commento oppure delle informazioni aggiuntive su questa voce.

Funzioni univoche

Occorre tenere presente alcune caratteristiche peculiari del client di configurazione.

Per un client di configurazione Windows 95 o Windows NT, si consiglia di utilizzare una risoluzione minima di 1024 x 768 pixel.

Se si tiene premuto il tastino sinistro del mouse per eseguire un controllo a scansione ciclica ed accidentalmente si trascina il mouse senza rilasciarlo, il controllo a scansione ciclica continua. Per arrestarlo, fare clic sulle frecce direzionali del controllo a scansione ciclica con il tastino sinistro del mouse.

Capitolo 5. Introduzione a IBM Firewall

Questo capitolo indica i passi per una configurazione di base necessari per impostare IBM Firewall. Contiene una spiegazione delle modalità di definizione di un'interfaccia sicura, di determinazione delle politiche di sicurezza e della definizione degli oggetti di rete.

Passi per una configurazione di base

Per un'impostazione di base di IBM Firewall:

1. Pianificare l'impostazione di IBM Firewall. Stabilire in anticipo quali funzioni del firewall si desidera utilizzare e come. Le seguenti sezioni possono fornire un aiuto:
   - Capitolo 1, “Introduzione a IBM Firewall” a pagina 1
   - Capitolo 2, “Pianificazione” a pagina 7
   - “Considerazioni sulla pianificazione” a pagina 53
2. Indicare al firewall quali delle sue interfacce sono collegate alle reti sicure. Per un corretto funzionamento del firewall occorre avere un'interfaccia sicura ed una non sicura. Dall'albero di navigazione del client di configurazione, aprire la cartella Gestione del sistema e fare clic su **Interfacce** per visualizzare un elenco delle interfacce di rete sul firewall. Per modificare lo stato di sicurezza di un'interfaccia, selezionare l'interfaccia e fare clic su **Modificare**. Per ulteriori informazioni, consultare la sezione “Designazione dell'interfaccia di rete” a pagina 24.
3. Impostare la politica di sicurezza generale accedendo alla casella di dialogo **Politica di sicurezza** dalla cartella Gestione del sistema. Per le configurazioni comuni del firewall:
   - Consentire interrogazioni DNS
   - Negare messaggi di tipo broadcast ad interfacce non sicure
   - Negare Socks ad adattatori non sicuri

   Per ulteriori informazioni, consultare la sezione “Utilizzo del client di configurazione per definire una politica di sicurezza” a pagina 25.
4. Impostare il DNS ed il servizio di posta. Accedere a queste funzioni dalla cartella Gestione del sistema che si trova nell'albero di navigazione del client di configurazione. È consigliata la lettura preliminare del Capitolo 6, “Gestione del DNS (Domain Name Service)” a pagina 31.
5. Definire gli elementi chiave delle reti sul firewall utilizzando la funzione **Oggetti di rete** nell'albero di navigazione del client di configurazione. La funzione Oggetti di rete consente di controllare il traffico sul firewall. Definire gli elementi chiave di seguito riportati come oggetti di rete:
   - Interfaccia sicura del firewall
   - Interfaccia non sicura del firewall
   - Rete sicura
   - Ciascuna sottorete della rete sicura
   - Un oggetto di rete host per i server SDI e per i server di dominio NT, se appropriato

Per ulteriori informazioni, consultare la sezione “Oggetti di rete” a pagina 26.

6. Abilitare i servizi sul firewall. Questi sono i metodi con cui gli utenti di una rete sicura possono accedere ad una rete non sicura (come socks o proxy). I servizi implementati dipendono dalle decisioni prese in fase di pianificazione. L'implementazione di un servizio richiede spesso l'impostazione di alcune configurazioni di collegamento per consentire alcuni tipi di traffico. Ad esempio, se si desidera consentire la navigazione in rete su Internet agli utenti sicuri tramite il proxy HTTP, occorre configurare il daemon Proxy HTTP sul firewall ed impostare i collegamenti per consentire il traffico HTTP. Per ulteriori informazioni su come impostare i collegamenti che supportano determinati servizi, consultare il Capitolo 9, “Esempi di servizi” a pagina 53.
7. Impostare gli utenti del firewall. Se si desidera richiedere l'autenticazione per funzioni quali accesso Web in partenza o per i responsabili del firewall, è necessario definire questi utenti sul firewall. Per ulteriori informazioni, consultare la sezione Capitolo 12, “Gestione degli utenti del firewall” a pagina 75.
8. Se si desidera utilizzare le parole d'ordine per l'autenticazione del dominio Windows NT, è necessario configurare il codice del client Windows, mediante il quale è possibile ricercare i domini Windows NT sicuri per scopi di autenticazione, all'uso di TCP invece di NETBIOS. NETBIOS viene disabilitato. I server Windows NT sicuri devono conoscere i nomi e gli indirizzi degli host TCP/IP e deve esistere un collegamento TCP/IP fra i server Windows NT ed il firewall. Per poter consentire il traffico, è necessario che il responsabile del firewall crei i collegamenti tra il firewall ed i server Windows NT sicuri.

Seguendo questi passi è possibile impostare ed eseguire una configurazione di base del firewall. IBM Firewall fornisce altre funzioni, quali i log di sistema, che aiutano a garantire la sicurezza della rete. Per ulteriori informazioni, consultare il Capitolo 15, “Gestione dei file di log e di archivio” a pagina 107.

Designazione dell'interfaccia di rete

In questo manuale si fa distinzione tra interfacce, reti e host sicuri e non sicuri. Le interfacce sicure collegano l'host IBM Firewall alla rete di host della rete interna, vale a dire la rete che si desidera proteggere. **Il funzionamento del firewall richiede almeno un'interfaccia sicura.** Le interfacce non sicure collegano IBM Firewall ad una o più reti esterne oppure ad Internet. IBM Firewall deve avere almeno un'interfaccia non sicura.

Tutte le reti collegate mediante un'interfaccia sicura vengono considerate reti sicure. Per distinguere tra le varie sottoreti collegate all'interfaccia sicura, utilizzare le regole di filtro avanzato per negare o consentire l'accesso alle varie sottoreti della stessa interfaccia, in base all'indirizzo IP o ad una maschera di indirizzo.

Per designare le interfacce sicure e non sicure, utilizzare la cartella Gestione del sistema dell'albero di navigazione del client di configurazione. Tutte le interfacce note (adattatori) verranno visualizzate e identificate come sicure o non sicure.

È necessario fornire un nome per ogni interfaccia prima di poter eseguire una funzione specifica di filtro delle interfacce.

Per identificare come sicura o non sicura un'interfaccia di rete:

1. Selezionare un'interfaccia e fare clic su **Modificare**.
2. Ripetere l'operazione come necessario.
3. Fare clic su **Chiudere**.

Per identificare come sicura o non sicura l'interfaccia e fornire un nome significativo a tale interfaccia, fare clic su **Aprire**. Questo nome verrà utilizzato dai filtri per una funzione specifica di filtro delle interfacce.

Utilizzo del client di configurazione per definire una politica di sicurezza

Una delle prime cose da valutare quando si configura IBM Firewall è la politica di sicurezza generale per l'installazione.

IBM Firewall fornisce una casella di dialogo di ausilio nell'impostazione della politica di sicurezza, come illustrato nella Figura 8.

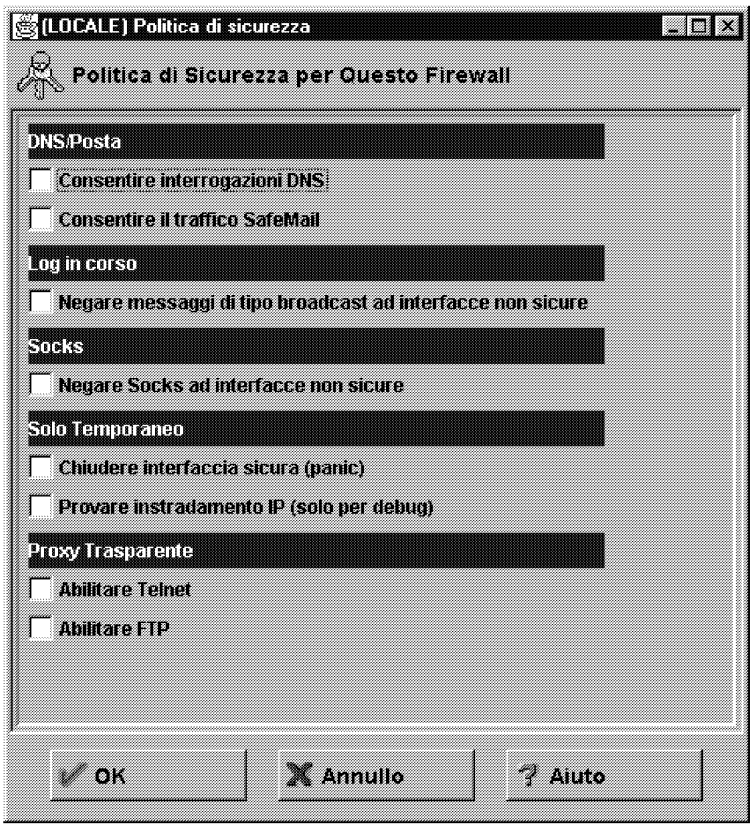

Figura 8. Politica di sicurezza

Per ulteriori informazioni sul pannello della politica di sicurezza, fare clic su Aiuto.

La casella di dialogo Politica di sicurezza fornisce ai responsabili un modo semplice e rapido per impostare le politiche generali per il firewall. La maggior parte delle caselle di spunta visualizzate nella finestra Politica di sicurezza forniscono un accesso rapido alla selezione di alcuni servizi predefiniti validi per tutto il traffico di rete ricevuto dal firewall. Fanno eccezione le scelte possibili per Proxy trasparente, che si limitano ad abilitare o a disabilitare il Telnet trasparente e l'FTP trasparente.

Quando si seleziona una politica di sicurezza, il firewall crea le regole di filtro che è necessario poi attivare. Il firewall abilita i servizi selezionati e li rende tutti disponibili.

Ogni volta che si seleziona una casella di spunta relativa ad un servizio predefinito e si fa clic su **OK**, occorre attivare queste modifiche dalla finestra Attivazione Collegamento. Non occorre attivare le selezioni relative al Proxy trasparente poiché esse non interessano i servizi predefiniti. Per un elenco dei servizi predefiniti, consultare la sezione “Servizi predefiniti” a pagina 63.

Viene visualizzato il seguente elenco di caselle di spunta da cui è possibile selezionare gli attributi che definiscono la politica di sicurezza del proprio sito. Gli attributi selezionati sono validi per tutti gli indirizzi su entrambi i lati del firewall IBM.

- Selezionare **Consentire interrogazioni DNS** per consentire le richieste e le risposte per la risoluzione DNS.
- Selezionare **SafeMail** per consentire al traffico della posta di passare attraverso il firewall.
- Selezionare **Negare messaggi di tipo broadcast ad interfacce non sicure** per fare in modo che i messaggi di tipo broadcast non vengano ricevuti su una porta non sicura. Se l'interfaccia non sicura del firewall è collegata ad Internet, questo servizio consente di ridurre la quantità di collegamenti sul firewall.
- Selezionare **Negare Socks ad adattatori non sicuri** per impedire al traffico socks di accedere al firewall dalla rete non sicura.
- Selezionare **Chiusura interfaccia sicura (panic)** per impedire tutto il traffico attraverso il firewall sulle interfacce sicure. Questo servizio è utilizzato solo in caso di emergenza.
- Selezionare **Provare instradamento IP (solo per debug)** per consentire tutto il traffico attraverso il firewall sulle interfacce. Se si modifica il valore di questa casella di spunta, occorre salvarlo facendo clic su **OK** ed attivarlo dalla finestra Attivazione Collegamento. **L'utilizzo di questo servizio può determinare dei rischi per la sicurezza del firewall. Utilizzarlo con estrema cautela.**
- Selezionare **Abilitare Telnet** per consentire i telnet proxy trasparenti.
- Selezionare **Abilitare FTP** per consentire gli FTP proxy trasparenti.

Oggetti di rete

Gli oggetti di rete sono rappresentazioni di componenti già esistenti sulla rete, quali gli host, le reti, i router, le VPN oppure gli utenti. Gli oggetti di rete designano gli indirizzi di origine e di destinazione dei servizi quando si creano i collegamenti.

È possibile identificare gli oggetti per nome, icona, tipo e descrizione. Esistono vari tipi di oggetti di rete ma Host e Firewall sono i più comuni. L'oggetto di rete assunto inviato con IBM Firewall è "Rete esterna". Si tratta di un oggetto globale che include tutti gli indirizzi IP possibili. Dopo avere completato i fogli di lavoro della configurazione di rete, presenti nella sezione “Foglio di lavoro per la pianificazione della configurazione di rete” a pagina 8, è possibile creare degli oggetti.

È possibile creare degli oggetti singoli o di gruppo. Tutti gli oggetti di rete vengono definiti da un indirizzo IP e da una maschera di indirizzi (maschera di sottorete), in

modo che sia possibile per un oggetto rappresentare un'intera gamma di indirizzi di rete.

Utilizzo del client di configurazione per definire gli oggetti di rete

Per definire un oggetto di rete singolo, selezionare **Oggetti di rete** dall'albero di navigazione del client di configurazione. Viene visualizzata la casella di dialogo Oggetti di rete. Fare doppio clic su **NUOVO**. Viene visualizzata la casella di dialogo **Aggiungere un Oggetto di Rete**, come illustrato nella Figura 9.

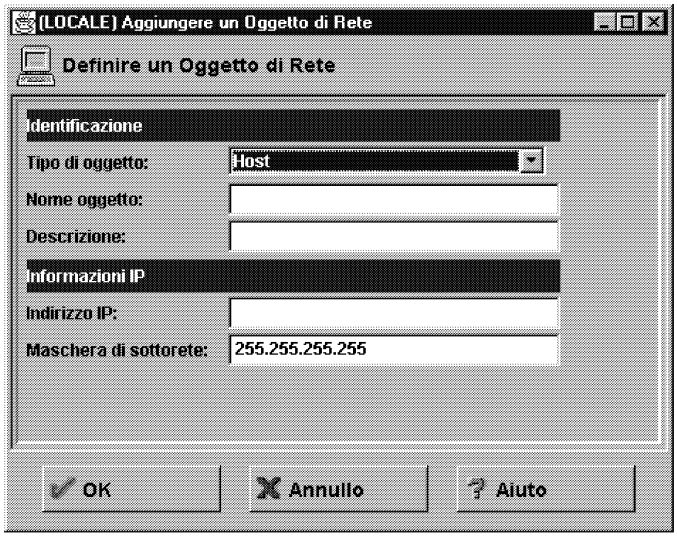

Figura 9. Aggiungere un Oggetto di Rete

1. Immettere il tipo di oggetto. Fare clic su **Tipo di oggetto** per visualizzare i tipi di oggetto che è possibile creare. Per migliorare le prestazioni, si consiglia di creare oggetti di tipo rete e non oggetti di tipo host. I tipi di oggetti che è possibile creare sono:
   - Host - uno specifico nodo sulla rete con una maschera 255.255.255.255.
   - Rete - un intervallo collettivo di indirizzi di rete caratterizzato da un intervallo di indirizzo e da una specifica maschera di sottorete.
   - Firewall - una singola macchina su cui è installato un firewall con una maschera di 255.255.255.255. Solo un oggetto di rete firewall può essere la destinazione di un tunnel IBM o di un tunnel manuale.
   - Router - un host che instrada il traffico tra due o più reti con una maschera 255.255.255.255.
   - Interfaccia - un adattatore di rete su una macchina con una maschera 255.255.255.255. Non deve essere un adattatore sul firewall.
2. Immettere il nome dell'oggetto.
3. Immettere la descrizione. Questo campo è facoltativo.
4. Immettere un indirizzo IP decimale con punti per questo oggetto.
5. Immettere una maschera di sottorete che specifica i bit dell'indirizzo da confrontare con l'indirizzo del pacchetto IP.
6. Fare clic su **OK**.

Gruppi di oggetti di rete

Un gruppo rappresenta un insieme di oggetti di rete. I gruppi vengono utilizzati per comodità in fase di impostazione dei collegamenti e permettono di evitare del lavoro ripetitivo. Un esempio consiste nel raggruppare alcuni indirizzi, singolarmente rappresentati da oggetti di rete, in un gruppo di oggetti di rete per rappresentare un dipartimento. Questo dipartimento può quindi essere utilizzato come l'indirizzo di origine o di destinazione di un collegamento.

Per definire un gruppo di oggetti di rete, dall'albero di navigazione del client di configurazione, selezionare Oggetti di rete. Viene visualizzata la casella di dialogo **Oggetti di rete**. Fare doppio clic su **NUOVO**. Viene visualizzata la casella di dialogo **Aggiungere un Oggetto di Rete**.

1. Immettere il nome del gruppo.
2. Immettere una descrizione. Questo campo è facoltativo.
3. Fare clic su **Selezionare** per selezionare degli oggetti per il gruppo.
4. Fare clic su **OK**.

Suggerimento: È buona norma includere degli intervalli di indirizzo contigui in un singolo oggetto di rete, quando possibile. Si migliorerà così l'esecuzione dell'elaborazione delle regole di collegamento. Viene di seguito riportato un esempio.

```
UFFICIO CONTABILITÀ
   Macchina di Kevin 191.1.10.1
   Macchina di Susan 191.1.10.3
   Macchina di Helen 191.1.10.5
   Macchina di Peter 191.1.10.7
   Macchina di Bob   191.1.10.9
```

Per creare un oggetto di rete per questo ufficio contabilità, immettere le informazioni sugli indirizzi IP relativi a questo gruppo come: 191.1.10.0 con una maschera di sottorete 255.255.255.0. Questo oggetto di rete, ufficio contabilità, può essere utilizzato come origine o come destinazione per un collegamento.

Copia di riserva della configurazione del firewall

Il firewall memorizza tutti i file di configurazione in `ROOTDIR\config`. Se si desidera eseguire la copia di riserva solo della configurazione del firewall e non di tutti i file del firewall, eseguire la copia di riserva dell'intero contenuto dell'indirizzario `ROOTDIR\config`.

Se si desidera ripristinare una configurazione del firewall di cui è stata eseguita la copia di riserva, eliminare tutti i file esistenti dall'indirizzario `ROOTDIR\config` e ripristinare le versioni di riserva dei file. È necessario rigenerare ed attivare le regole di filtro prima che la configurazione ripristinata sia considerata valida.

I file di configurazione chiave del firewall sono elencati di seguito. È possibile che l'indirizzario `\config` sul firewall non li contenga tutti. Tuttavia, mentre la maggior parte dei file di configurazione del firewall sono semplici file di testo visualizzabili con un editor di testo, **l'editazione manuale di questi file non è supportata**.

- carriers.cfg - Definizioni della portante del cercapersone
- cfgfilt.output

- explode.cfg
- filters.active - Indica se il filtro è attivo
- fwadpt.cfg - Definizioni per le interfacce di rete
- fwconfig.map - Contiene i nomi dei file di configurazione
- fwconns.cfg - Definizioni per i collegamenti di filtro
- fwfilters.cfg - Filtri attivi correnti
- fwhttp.cfg - Configurazione del proxy HTTP
- fwmail.conf - Configurazione SafeMail
- fwobjects.cfg - Definizioni per gli oggetti di rete
- fwpolicy.cfg - Opzioni della politica di sicurezza
- fwrules.cfg - Definizioni per gli schemi di regole di filtro
- fwservices.cfg - Definizioni per i servizi
- fwsocks.cfg - Regole Socks 5 dal client di configurazione
- fwtdefn.conf - Definizioni per gli avvisi
- fwtpproxy.cfg - Definizioni per proxy trasparente
- fwusrdb.cfg - Database dell'utente del firewall
- logmgmt.cfg - Definizioni per l'archiviazione
- modems.cfg - Definizioni per i modem
- pager.cfg - Definizioni per i cercapersone
- rcsfile.cfg - Parametri del servizio di configurazione
- Socks5.conf - File di configurazione Socks 5 generato
- Socks5.header.cfg - Parti fornite dall'utente del Socks5.conf generato
- syslog.conf - Definizioni per le funzioni di log

Capitolo 6. Gestione del DNS (Domain Name Service)

Questo capitolo spiega come configurare il DNS (Domain Name Service) (DNS) in relazione a IBM Firewall. Scopo del DNS è fornire un servizio di nomi dominio completo agli host interni alla rete sicura senza fornire alcuna informazione agli host esterni alla rete sicura. Ciò consente agli utenti interni alla rete sicura di poter accedere a tutti i servizi Internet. Tuttavia, non essendo divulgate le informazioni sulla rete sicura, diventa più difficile per un pirata dell'informatica individuare un elaboratore da attaccare.

Per ottenere tale scopo sono necessari tre server nomi dominio:

1. Uno su IBM Firewall
2. Uno all'interno della rete sicura
3. Uno all'esterno della rete sicura

Fare riferimento alla Figura 10 per informazioni su come utilizzare il DNS con IBM Firewall.

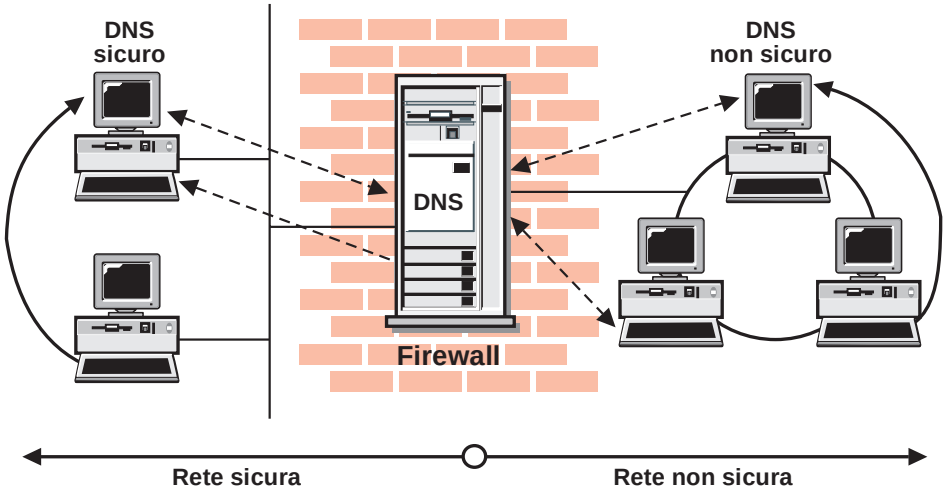

Figura 10. DNS

Il firewall viene configurato in modo da poter essere utilizzato come un gateway tra i server nomi della rete sicura ed i server che gestiscono la rete non sicura. La definizione ufficiale per il funzionamento del firewall è *server nomi di sola memoria cache*, in quanto il DNS del firewall non contiene alcun file di database.

La Figura 10 illustra il funzionamento del firewall. Ogni volta che il firewall deve risolvere un nome per poterlo utilizzare, si rivolge ai server nomi sicuri. Ogni volta che un'interrogazione viene inoltrata al firewall, il firewall a sua volta la inoltra ai server nomi non sicuri.

Quando un client della rete sicura richiede un'informazione sulla parte sicura, la richiesta viene inviata al DNS sicuro. Quando lo stesso client richiede un'informazione sulla parte non sicura, la richiesta viene inviata ugualmente al DNS sicuro. Poiché l'interrogazione riguarda informazioni sulla parte non sicura, il DNS sicuro non può rispondere ed inoltra quindi l'interrogazione al firewall. Nel caso in cui un DNS non sicuro inviasse una richiesta al firewall, questa richiesta sarebbe

inoltrata al dominio DNS non sicuro, per cui le informazioni riservate non sarebbero in alcun caso divulgate.

Configurazione del DNS utilizzando il client di configurazione

Per configurare il DNS, selezionare Gestione del Sistema dall'albero di navigazione del client di configurazione. Fare doppio clic sull'icona della cartella di file per espandere la vista. Selezionare **Servizi Nomi Dominio**. IBM Firewall visualizza la configurazione corrente del DNS, che è possibile modificare.

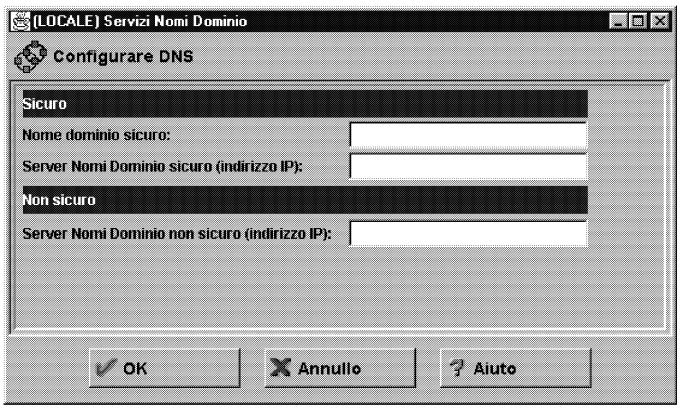

Figura 11. Servizi Nomi Dominio

Nota: Quando si aggiunge il DNS, il firewall salva e ridenomina i file di configurazione del DNS esistenti.

1. Il campo **Nome Dominio Sicuro** identifica il nome dominio che il firewall accoda a qualsiasi nome host non completo.
2. Il campo **Server Nomi Dominio sicuro** fa riferimento al server che risolve i nomi e gli indirizzi IP per gli host protetti da Internet mediante IBM Firewall. È possibile immettere indirizzi IP decimali con punti, separati da spazi.
3. Il campo **Server Nomi Dominio non sicuro** fa riferimento ai server forniti dal fornitore di servizi per risolvere le informazioni sulla rete non sicura. È possibile immettere indirizzi IP decimali con punti, separati da spazi.

Nota: Quando un server nomi viene inizializzato, invia una richiesta per ottenere l'elenco dei server nomi di root. La maggior parte delle realizzazioni conserva questo elenco in memoria. La realizzazione Microsoft, tuttavia, riscrive questo elenco nel file di configurazione. Ciò non modifica il funzionamento del server nomi, ma modifica i valori visualizzati nel campo **Server Nomi Dominio non sicuro**. Ciò non rappresenta un problema.

Configurazione del server nomi sicuro

Il server nomi sicuro deve essere configurato per inoltrare al firewall le interrogazioni non risolte. Se si dispone di una realizzazione BIND standard, aggiungere un'istruzione *forwarders* ed un'istruzione *cache* al file *boot* sul server nomi sicuro:

```
forwarders      aaa.bbb.ccc.ddd
cache           .               named.cache
```

Creare un file di cache, *named.cache*, per indicare al firewall:

```
. 99999999 IN NS firewall.private.com
firewall.private.com   99999999 IN A aaa.bbb.ccc.ddd
```

dove *private.com* è il nome dominio utilizzato dal dominio sicuro e *aaa.bbb.ccc.ddd* è l'indirizzo IP del firewall.

È possibile, inoltre, aggiungere i nomi host del firewall ai database del DNS. In questo modo gli utenti possono accedere al server Socks, al proxy HTTP, al proxy Telnet ed al proxy FTP del firewall mediante il nome host del firewall invece dell'indirizzo IP. Questa operazione richiede due fasi supplementari, come descritto nel *Capitolo 4* di *DNS and BIND*. Per ulteriori dettagli su questo manuale, consultare la *Bibliografia*.

Aggiungere prima un record A al file di database del dominio:

```
firewall.private.com     IN A aaa.bbb.ccc.ddd
```

Aggiungere quindi un record PTR al file di ricerca inversa:

```
ddd.ccc.bbb.aaa.in-addr.arpa.     IN PTR   firewall.private.com.
```

Se per la rete sicura non viene utilizzato il DNS, il firewall deve risolvere le informazioni. Configurare il firewall come descritto per il caso normale me inserire l'interfaccia sicura del firewall nel campo **Server Nomi Dominio sicuro**. Aggiungere quindi la seguente stringa a `c:\winnt\system32\dns\boot`.

```
primary ccc.bbb.aaa.in-addr.arpa c:\winnt\system32\dns\fwnamed.rev
```

Creare quindi *fwnamed.rev* per raggruppare le seguenti informazioni:

```
ccc.bbb.aaa.in-addr.arpa  IN SOA firewall.private.com. root.public.com. (
                          9        ; Serial
                          86400    ; Refresh after 1 day
                          300      ; Retry after 5 minutes
                          654000   ; Expire after 1 week
                          3600  )  ; Minimum TTL of 1 day
ccc.bbb.aaa.in-addr.arpa.          IN NS    firewall.private.com.
ddd.ccc.bbb.aaa.in-addr.arpa.      IN PTR   firewall.private.com.
```

Configurazione dei client sicuri

I client della rete sicura devono essere configurati in modo che le loro interrogazioni vengano inviate al server nomi sicuro e non al firewall. Ciò garantisce che le informazioni sulla parte sicura non vengano conservate nella memoria cache del firewall. In questo modo il firewall non viene sovraccaricato, a meno che un'interrogazione non venga inviata dal dominio sicuro al dominio non sicuro.

Se per la rete sicura non viene utilizzato il DNS, i client devono indicare il firewall come proprio server nomi.

Diffusione dei servizi fra gli utenti

Molte organizzazioni desiderano diffondere determinati servizi fra gli utenti di Internet. Spesso questi servizi includono la posta elettronica ed i server Web, anche se è possibile utilizzare qualsiasi server TCP/IP. Per rendere disponibili questi servizi, è necessario non solo inserire il server nella rete, in modo che sia possibile accedervi, ma anche elencare quel server con il DNS pubblico, in modo che gli utenti possano ottenere le informazioni corrette.

Per ottenere ciò, possono essere utilizzati due metodi. Il fornitore di servizi deve elencare i server come parte del rispettivo dominio, (e quindi come server nomi) oppure l'utente deve fornire il proprio server nomi e registrarlo con Internet. È più semplice se questo servizio viene fornito dall'ISP (Internet Service Provider). Se si sceglie questa soluzione, è necessario fornire all'ISP i nomi host e gli indirizzi IP che si desidera elencare. Ad esempio, se si utilizza il proprio server web come *www.public.com*, l'indirizzo IP del quale è *50.100.150.200*, è necessario richiedere all'ISP di elencare *www.public.com at 50.100.150.200*.

Inoltre, se si desidera ricevere la posta elettronica, è necessario richiedere all'ISP di elencare il firewall come *dispositivo per lo scambio della posta* per il dominio di posta elettronica sicuro. L'ISP deve conoscere il nome host *(gateway.public.com)*, il relativo indirizzo IP *(50.100.150.201)* ed il nome dominio con cui si desidera che riceva la posta *(public.com)*.

Se l'ISP non è in grado di fornire questi servizi, l'utente deve provvedere a ciò personalmente. Esistono due possibilità. È possibile inserire un server DNS nel DMZ oppure è possibile utilizzare il firewall come server nomi. Se viene utilizzato il firewall, non vengono procurati altri rischi per la sicurezza, in quanto i file del database che vengono inseriti nel firewall non contengono informazioni sulla rete sicura. Le uniche informazioni memorizzate riguardano i servizi pubblici che l'utente ha deciso di offrire.

I dettagli relativi all'impostazione di un server DNS sono contenuti nel capitolo 4 del manuale *DNS and BIND*, presente nella *Bibliografia*. Se necessario, si consiglia di leggere questo capitolo ed i capitoli precedenti. L'impostazione di un server DNS non rappresenta un'attività semplice ed è pertanto consigliabile che venga eseguita da esperti. Se non è possibile delegare un esperto, seguire le sue indicazioni per impostare il server DNS.

Per ulteriori informazioni, consultare “Configurazioni di esempio” a pagina 35.

Installazione del server DNS Microsoft

Per installare il server DNS Microsoft, andare al pannello di controllo, fare clic su **Rete**, fare clic sulla scheda **Servizi**, quindi fare clic su **Aggiungere** e selezionare **Server DNS Microsoft**. È necessario il CDROM di installazione.

Risoluzione dei problemi relativi al DNS

IBM eNetwork Firewall - Manuale di riferimento contiene un capitolo sulla risoluzione dei problemi relativi al firewall. In questo capitolo è presente una sezione specifica relativa ai problemi del DNS. In questa sezione vengono forniti dei suggerimenti su come utilizzare il comando *nslookup* per identificare il segmento errato del sistema DNS.

Configurazioni di esempio

Questa sessione illustra alcune configurazioni di esempio mediante le quali è possibile installare un firewall. La maggior parte di questi esempi mette in evidenza la configurazione necessaria per l'operazione del DNS. È improbabile che uno di questi esempi illustri la propria rete, pertanto prestare attenzione a ciascun esempio ed ai concetti fondamentali per l'installazione.

Esempio 1: Server DNS in un DMZ sull'interfaccia non sicura

Il primo esempio illustra i file necessari per utilizzare il server nomi in un DMZ ubicato all'interno della rete non sicura, come indicato nella Figura 12.

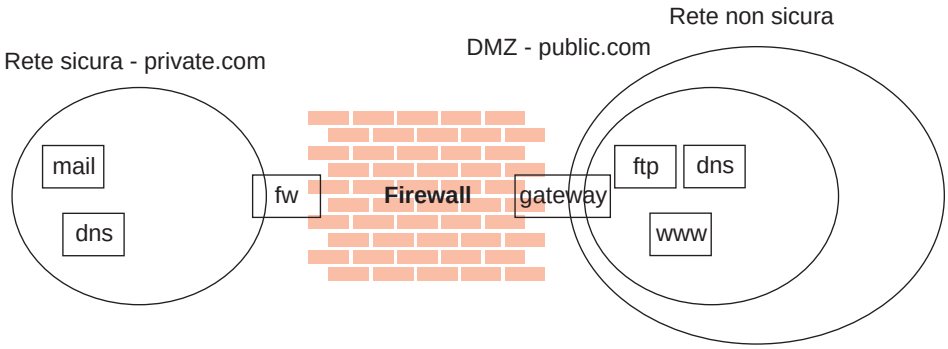

Figura 12. Server nomi in DMZ all'interno della rete non sicura

Questa figura illustra una rete privata, *private.com*, ed un firewall la cui interfaccia sicura è denominata *fw.private.com* e l'interfaccia non sicura *gateway.public.com*. Il DMZ della società è collegato all'interfaccia non sicura e contiene un server nomi *dns.public.com*, un server FTP *ftp.public.com* ed un server web *www.public.com*. I file in *dns.public.com* per implementare questo scenario sono i seguenti:

db.public

```
public.com.   IN SOA dns.public.com. admin.public.com.  (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                  3600        ; retry after 1 hour
                  604800      ; expire after 1 week
                  86400 )     ; minimum TTL 1 day
;
; Nameservers
;
public.com           IN NS  dns.public.com.
;
; Hosts in the DMZ
;
dns.public.com.      IN A 50.100.150.202
gateway.public.com.  IN A 50.100.150.201
www.public.com.      IN A 50.100.150.200
ftp.public.com.      IN A 50.100.150.203
;
; Mail-related entries
;
public.com.          IN MX  0  gateway.public.com.
public.com.          IN CNAME gateway.public.com.
```

db.50.100.150

```
150.100.50.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
202.150.100.50.in-addr.arpa.      IN NS dns.public.com.
203.150.100.50.in-addr.arpa.      IN PTR  ftp.public.com.
202.150.100.50.in-addr.arpa.      IN PTR  dns.public.com.
201.150.100.50.in-addr.arpa.      IN PTR  gateway.public.com.
200.150.100.50.in-addr.arpa.      IN PTR  www.public.com.
```

db.127.0.0

```
0.0.127.in-addr.arpa.   IN SOA dns.public.com. admin.public.com.  (
                 1           ; serial number
                 10800       ; refresh after 3 hours
                 3600        ; retry after 1 week
                 604800      ; expire after 1 week
                 86400  )    ; minimum TTL 1 day
0.0.127.in-addr.arpa.   IN NS  dns.public.com.
1.0.0.127.in-addr.arpa.   IN PTR localhost.
```

db.cache

La scelta migliore per questo file è di eseguire l'FTP dell'elenco di server nomi root corrente da *ftp://ftp.rs.internic.net/domain/named.root*.

boot

```
primary public.com                  db.public
primary 150.100.50.in-addr.arpa     db.50.100.150
primary 0.0.127.in-addr.arpa        db.127.0.0
cache   .                           db.cache
```

Per impostare il filtro del traffico in modo da consentire il traffico DNS appropriato, abilitare *Consentire interrogazioni DNS* sul pannello **Politica di sicurezza**.

Esempio 2: DNS in un DMZ su un'interfaccia dedicata

Nel secondo esempio, il DNS per il DMZ è ancora su un server nomi dedicato, ma questa volta il DMZ è collegato ad un'interfaccia particolare, diversa da quella della rete non sicura.

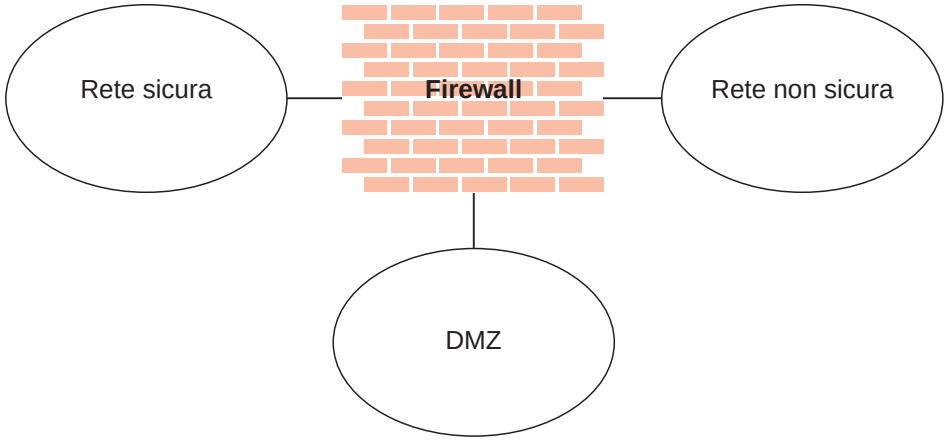

Figura 13. DNS in un DMZ su un'interfaccia dedicata

I file di dati del DNS su *dns.public.com* sono gli stessi dell'esempio precedente. Affinché il server nomi possa possa accedere alla rete pubblica, è necessario aprire il filtro del traffico o eseguire un tersferimento di zona per copiare i file di dati nel firewall.

Per aprire il filtro del traffico, copiare i tre schemi di regole denominati *DNS Server queries*, *DNS Replies* e *DNS Client queries*. Modificare l'impostazione di instradamento di ogni regola da *locale* a *instradato*. Quindi includere i tre nuovi schemi di regole in un servizio ed impostare gli indicatori di flusso nel seguente modo:

- DNS Client queries: --->
- DNS Replies: <---
- DNS Server queries: --->
- DNS Server queries: <---

Includere questo servizio in un collegamento che utilizza la *Rete esterna* come oggetto di origine e *dns.public.com* come oggetto di destinazione.

Per eseguire un trasferimento di zona, è necessario impostare il filtro del traffico ed indicare ai server nomi di copiare i file appropriati. Per impostare il filtro del traffico:

1. Nel pannello **Politica di sicurezza**, abilitare *Consentire interrogazioni DNS*.
2. Aggiungere un collegamento da *dns.public.com* (oggetto di origine) all'interfaccia DMZ (oggetto di destinazione) del firewall, che contiene il servizio denominato *DNS Transfers*.

Per attivare il trasferimento di zona, aggiungere le seguenti righe al file *boot* del firewall in `c:\winnt\system32\dns`:

```
secondary public.com     50.100.150.202 db.public
secondary 150.100.50.in-addr.arpa  50.100.150.202 db.50.100.150
```

Andare quindi al programma di gestione dei servizi ed arrestare e riavviare il servizio DNS Server.

Esempio 3: Utilizzo del firewall come server nomi di origine

Per utilizzare il firewall come server nomi sicuro, collocare nel firewall i file del database, ubicati normalmente sul server sicuro, sul firewall. A questo punto è possibile puntare al firewall come al server DNS. I rischi sono che il server DNS non è in grado di distinguere le richieste provenienti dal lato sicuro da quelle provenienti dal lato non sicuro. Quindi, fornisce le informazioni provenienti dal lato sicuro a qualsiasi utente le richieda; pertanto le informazioni DNS sicure non possono essere nascoste a lungo.

Per eseguire questa operazione, configurare la funzione DNS del firewall utilizzando il client di configurazione. Per il campo *Nome Dominio Sicuro*, elencare il nome dominio che verrà utilizzato sulla rete sicura. Per *Server Nomi sicuro*, elencare l'interfaccia sicura del firewall. Per *Server Nomi non sicuro*, elencare il server nomi fornito dall'ISP. Quindi è necessario creare un file di ricerca inversa sul firewall per integrare questa configurazione.

Creare il file `c:\winnt\system32\dns\fwnamed.rev` nel seguente modo:

Per questo esempio, l'interfaccia sicura del firewall è denominata *fw.private.com* e l'indirizzo IP è *10.100.100.1*.

```
100.100.10.in-addr.arpa.   IN SOA fw.private.com. admin.fw.private.com. (
                  1           ; serial number
                  10800       ; refresh after 3 hours
                  3600        ; retry after 1 week
                  604800      ; expire after 1 week
                  86400  )    ; minimum TTL 1 day
1.100.100.10.in-addr.arpa.         IN NS fw.private.com.
1.100.100.10.in-addr.arpa.         IN A  fw.private.com.
```

Aggiungere quindi la seguente riga a `c:\winnt\system32\dns\boot`:

```
primary 100.100.10.in-addr.arpa     fwnamed.rev
```

In questo scenario, i client devono essere configurati per indicare il firewall (10.100.100.1) come server DNS. Il firewall si avvale dell'apporto delle informazioni che provengono dall'esterno, ma non può garantire la riservatezza di quelle provenienti dal lato sicuro. Ciò significa che un client del lato sicuro che desidera collegarsi al server di configurazione o ad un qualsiasi server proxy sul firewall, deve far riferimento al firewall per indirizzo IP e non per nome host.

Capitolo 7. SafeMail

Il gateway SafeMail di IBM Firewall è un gateway per il traffico SMTP. Questo gateway trasmette i messaggi dai server di posta sicuri alla parte non sicura, nascondendo i nomi di dominio riservati. Tale gateway, inoltre, trasmette i messaggi dalla parte non sicura al dominio di posta sicuro ed isola la rete sicura da eventuali intrusioni.

Sebbene SafeMail non esegua una verifica del contenuto dei messaggi, fornisce una funzione di uscita mediante la quale è possibile eseguire tale verifica. Per ulteriori informazioni, consultare “Funzione di uscita da SafeMail” a pagina 41.

SafeMail trasmette in tempo reale i messaggi dal mittente al destinatario. In questo modo si evitano i rischi e le difficoltà che si riscontrano conservando una coda di messaggi sul firewall. Sui domini di posta adiacenti sono tuttavia necessari determinati requisiti di configurazione. In alcuni casi, questi requisiti non verranno utilizzati praticamente per eseguire un'installazione. In questi casi, è possibile acquistare separatamente uno dei server SMTP ed installarlo al posto di SafeMail. Se si decide di installare un server SMTP completo, configurare tale server con i requisiti di sicurezza. Per ulteriori informazioni, consultare “Utilizzo di un server SMTP al posto di SafeMail” a pagina 41.

Configurazione di SafeMail utilizzando il client di configurazione

Per configurare SafeMail, selezionare Gestione del Sistema dall'albero di navigazione del client di configurazione. Fare doppio clic sull'icona della cartella di file per espandere la vista. Selezionare **SafeMail**. IBM Firewall visualizza l'elenco dei server e dei domini di posta configurati. Per ciascun dominio di posta privato, è necessario configurare un'entrata.

1. Per aggiungere un dominio, selezionare **NUOVO** e fare clic su **Aprire**. Viene visualizzata la casella di dialogo **Aggiungere Server di Posta**.
2. Il campo **Nome dominio sicuro** contiene il nome con cui il dominio di posta che viene descritto è noto agli utenti della parte sicura del firewall.
3. Il campo **Nome server di posta sicuro** contiene il nome host o l'indirizzo IP decimale con punti del server di posta a cui viene applicata questa entrata. Questo server deve trovarsi su una delle reti sicure. È possibile indicare un unico server di posta per un determinato dominio.
4. Il campo **Nome dominio pubblico** contiene il nome con cui il dominio di posta che viene descritto è noto agli utenti della parte non sicura del firewall. Questo nome verrà utilizzato al posto del nome dominio sicuro, in modo da nascondere la topografia della rete sicura.
5. Fare clic su **OK**.

Modifica di un'entrata di configurazione della posta

Per modificare un'entrata di configurazione della posta, selezionare un'entrata dall'elenco e fare clic su **Aprire**. Viene visualizzata la casella di dialogo **Modificare la Configurazione del Server di Posta**.

Il campo **Nome Dominio Sicuro** viene disabilitato, ma è possibile modificare gli altri campi, come descritto nella sezione “Configurazione di SafeMail utilizzando il client di configurazione”.

Note:

1. Se SafeMail è stato precedentemente configurato e adesso si specifica un server di posta sicuro, questo server di posta sostituisce quello configurato in precedenza.
2. Se SafeMail *non* è stato precedentemente configurato e adesso si specifica un server di posta sicuro, questo server di posta viene aggiunto alla configurazione.

Eliminazione di un'entrata di configurazione della posta

Per eliminare un'entrata di configurazione di SafeMail, selezionare un'entrata nell'elenco e fare clic su **Eliminare**. Viene visualizzata un'avvertenza relativa a questa eliminazione. Fare clic su **OK** per confermare l'eliminazione o su **Annullo** per non confermarla.

Configurazione dei server sicuri

È necessario configurare i server di posta sicuri per indicare il firewall come gateway per i domini sconosciuti. In questo modo la posta diretta alla rete non sicura viene inoltrata al firewall. Inoltre, ogni server deve essere configurato in modo da accettare i messaggi indirizzati al nome del dominio pubblico oltre che al nome dominio privato. Quando il firewall inoltra una nota dalla rete non sicura, tutti i destinatari sono in ascolto con i loro nomi di dominio pubblico.

Se nella rete sicura è presente più di un singolo dominio di posta, è necessario inoltre configurare ciascun server affinché la posta diretta ad un altro dominio sicuro venga inoltrata direttamente a quel server, senza passare per il firewall. In questo modo il firewall non viene sovraccaricato inutilmente ed il meccanismo di consegna in tempo reale funziona correttamente.

Configurazione del dominio pubblico

L'unica configurazione necessaria nella rete non sicura consiste nell'indicare il firewall come dispositivo di scambio della posta per la rete. Per le informazioni necessarie sui server DNS, rivolgersi al fornitore di servizi. Per ulteriori dettagli sui meccanismi utilizzati, consultare il Capitolo 6, “Gestione del DNS (Domain Name Service)” a pagina 31.

L'obiettivo è quello di indicare il firewall come *dispositivo di scambio della posta* per ciascun nome dominio pubblico per il quale si desidera accettare la posta. Ad esempio, se si utilizza il nome dominio *private.com* all'interno della rete sicura ed il nome dominio *public.com* all'esterno della rete sicura, è possibile denominare il firewall *gateway.public.com*. In tal caso, richiedere al fornitore di servizi di indicare il nome host e l'indirizzo IP del firewall come un host (indicato generalmente con i record "A" ed i record "PTR"). Quindi, dal momento che si desidera accettare la posta indirizzata a *user@public.com*, richiedere al fornitore di servizi di aggiungere un record MX per il dominio *public.com* che indichi *gateway.public.com* come il dispositivo di scambio della posta per quel dominio. Inoltre, se si desidera ricevere

la posta indirizzata a *user@somethingelse.com*, è possibile indicare un record MX supplementare anch'esso rivolto al firewall.

Funzione di uscita da SafeMail

SafeMail fornisce una funzione di uscita mediante la quale un'installazione può predisporre SafeMail in modo da rifiutare il traffico potenzialmente pericoloso. Consultare *IBM eNetwork Firewall - Manuale di riferimento* per una descrizione dettagliata del Kit di sviluppo del software fornito a tale scopo.

La funzione di uscita consente di creare una funzione *UsrCheck()*, che viene richiamata ogni volta che SafeMail riceve un pacchetto dal mittente. Tale funzione presenta una struttura che contiene vari campi relativi allo stato del sistema. Questa struttura include una sessione ID univoca, gli indirizzi IP dei server di invio e di ricezione, gli indicatori relativi ai comandi precedentemente ricevuti ed un buffer di testo contenente il pacchetto analizzato.

Alcuni tipi di verifica che è possibile eseguire mediante questa funzione sono:

- elenco degli host *vietati*
- scansione delle sequenze di caratteri non consentiti, ad esempio lingua o nomi del codice di progetto non appropriati
- verifica delle stringhe con virgolette
- limitazioni relative alla lunghezza dei messaggi

La funzione di uscita può anche essere utilizzata, eventualmente, per realizzare un'interfaccia per un prodotto di verifica del contenuto di un altro fornitore.

Se mediante la funzione di uscita viene stabilito che un messaggio non deve essere elaborato, la funzione restituisce a Safemail un codice motivo. SafeMail rifiuta immediatamente il collegamento al server di invio SMTP. Allo stesso tempo, viene scritto un messaggio nel log del firewall, che comprende il codice motivo restituito dalla funzione di uscita.

Quando si scrive la funzione di uscita, questa funzione viene richiamata per tutti i pacchetti ricevuti. Scrivere quindi tale funzione in modo che risulti più efficace possibile, per evitare un impatto negativo sulle prestazioni del sistema. Inoltre, dal momento che questa funzione viene eseguita in un ambiente con più thread, accertarsi che venga scritta in modo da proteggere i thread. È possibile scrivere la funzione di uscita con qualsiasi programma di compilazione che supporti il funzionamento di più thread ed è possibile utilizzare la convenzione *_cdecl* per il collegamento. Vengono forniti alcuni file di compilazione di esempio per IBM Visual Age C++ e per Microsoft Visual C++.

Utilizzo di un server SMTP al posto di SafeMail

Disabilitazione di SafeMail

Per disabilitare SafeMail in modo da evitare conflitti con un altro server SMTP, disabilitare il servizio SafeMail dal programma di gestione dei servizi. Dal menu **Avvio** di Windows, selezionare **Impostazioni, Pannello di controllo, Servizi**. Scorrere l'elenco fino a selezionare *Server SafeMail di IBM Firewall*. Fare clic su **Avvio**. Nel campo **Tipo di avvio**, selezionare **Disattivato**. Fare clic su **OK**.

Configurazione di un server SMTP

Quando viene installato un server SMPT completo al posto di SafeMail, è necessario considerare vari fattori. Questa sezione descrive le funzioni di sicurezza di SafeMail, affinché il server SMTP venga configurato in modo da eseguire funzioni simili. Alcuni server SMTP non sono in grado di eseguite determinate attività, per cui, prima di acquistare un prodotto, è necessario esaminare attentamente le scelte disponibili e le proprie necessità.

Alcuni attacchi hanno il fine di creare un overflow o di danneggiare in qualche modo la coda di posta. Sebbene nessun server possa funzionare senza una coda di posta, i rischi associati alla coda di posta vengono ridotti se è possibile dedicare un volume di disco esclusivamente a questa attività. In questo modo le possibilità che una coda di overflow comprometta le operazioni del firewall vengono ridotte.

Inoltre, è importante che il server di posta nasconda le informazioni sulla rete sicura. In base alle regole dei server SMTP, ogni server che inoltra la posta deve inserire una riga di intestazione *Ricevuto:*. Queste righe di intestazione possono essere utilizzate da un pirata per mappare alla rete sicura. SafeMail elimina queste intestazioni quando elabora una nota; configurare il server SMTP perché faccia lo stesso. Inoltre, SafeMail riscrive tutti i nomi host privati sul nome dominio pubblico. In questo modo vengono eliminate anche le informazioni che potrebbero essere utilizzate per mappare alla rete.

Emissione di log di esempio relativa a SafeMail

Di seguito viene riportato un esempio dell'emissione di log relativa a SafeMail.

```
Feb 03 13:46:11 1998 mr16n18: ICA2163i: safemaild started.

Feb 03 13:41:14 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e7a19
received from RACK3BD.
Feb 03 13:41:21 1998 mr16n18: ICA2179i: SafeMail has forwarded 215575
bytes for connection 0xd71e6118 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:21 1998 mr16n18: ICA2178i: SafeMail session 0xd71e7a19
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:23 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e831a
received from RACK3BD.
Feb 03 13:41:36 1998 mr16n18: ICA2177i: SafeMail connection 0xd71e901b
received from RACK3BD.
Feb 03 13:41:56 1998 mr16n18: ICA2179i: SafeMail has forwarded 215567
bytes for connection 0xd71e7a19 from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e831a
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:56 1998 mr16n18: ICA2178i: SafeMail session 0xd71e901b
has been established from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 346
bytes for connection 0xd71e901b from 9.67.144.52 to 9.67.131.250.
Feb 03 13:41:57 1998 mr16n18: ICA2179i: SafeMail has forwarded 358
bytes for connection 0xd71e831a from 9.67.144.52 to 9.67.131.250.
```

Di seguito sono riportati alcuni messaggi di log:

- ICA2177 - indica l'avvio di un nuovo collegamento.
- ICA2179 - indica un'operazione completata correttamente.
- ICA2178 - indica che è stato stabilito un contatto con il server SMTP di ricezione.
- ICA2181 - indica che SafeMail ha rifiutato la sessione. Per i codici di errore, consultare *IBM eNetwork Firewall - Manuale di riferimento*.
- ICA2180 - indica la fine della sessione.
- ICA2182 - indica che la funzione di uscita ha determinato il rifiuto della sessione.

Capitolo 8. Controllo del traffico in transito sul firewall

Questo capitolo descrive come utilizzare il client di configurazione per controllare il traffico di rete in transito sul firewall. Utilizzando filtri avanzati, il firewall filtra i pacchetti a livello di sessione in base a più criteri, come l'ora del giorno, l'indirizzo IP e la sottorete. I filtri agiscono tra le interfacce di reti sicure e non sicure. Non influiscono quindi sulle tabelle di instradamento del firewall.

Per valore assunto, sul firewall non è consentito il traffico tra reti sicure e non sicure. Per consentire tipi specifici di traffico tra reti sicure e non sicure, è necessario creare dei collegamenti.

Utilizzo del client di configurazione per creare dei collegamenti

I componenti del client di configurazione illustrati nella Figura 14 a pagina 46 vengono utilizzati per creare oggetti di rete, schemi di regola, servizi e collegamenti.

Collegamenti Associano gli oggetti di rete ai servizi e/o agli schemi socks per definire i tipi di comunicazione consentiti tra punti terminali. Ciascun collegamento definisce un tipo specifico di traffico IP da consentire o negare tra un oggetto di rete di origine ed uno di destinazione.

Servizi Sono costituiti da uno o più schemi di regole. Ciascun servizio definisce il tipo di traffico IP consentito o negato tra un oggetto di origine ed uno di destinazione. Ad esempio, è possibile costituire un servizio per consentire Telnet o negare Ping (uno dei servizi FTP è composto da otto schemi di regole). IBM Firewall viene fornito con una serie di servizi assunti. Non è possibile eliminare questi servizi assunti precaricati ma è possibile modificare alcuni campi. Se questi servizi predefiniti non rispondono però alle esigenze dell'utente, è possibile aggiungere altri servizi utilizzando gli schemi di regole per creare delle nuove regole. Per ulteriori informazioni, consultare la sezione “Definizione dei servizi” a pagina 65.

Schemi di regole Forniscono al firewall le istruzioni per consentire o negare i pacchetti IP in base ai loro diversi attributi.

Schemi socks Forniscono al daemon socks del firewall le istruzioni per consentire o negare i pacchetti IP in base ai loro diversi attributi.

Oggetti di rete Rappresentano i vari componenti di rete, quali host, utenti e sottoreti che interagiscono con il firewall. Tali componenti vengono definiti da un indirizzo IP e da una maschera di indirizzi, in modo che sia possibile per un oggetto rappresentare un'intera gamma di indirizzi di rete. Gli oggetti di rete possono essere raggruppati.

Gruppi di oggetti di rete
Rappresentano uno o più oggetti di rete. È possibile utilizzarli per comodità in fase di impostazione dei collegamenti e

permettono di evitare del lavoro ripetitivo. Un esempio consiste nel raggruppare più indirizzi in un gruppo di oggetti di rete per rappresentare un dipartimento. Questo gruppo di oggetti di rete può quindi essere utilizzato come l'origine o la destinazione di un collegamento.

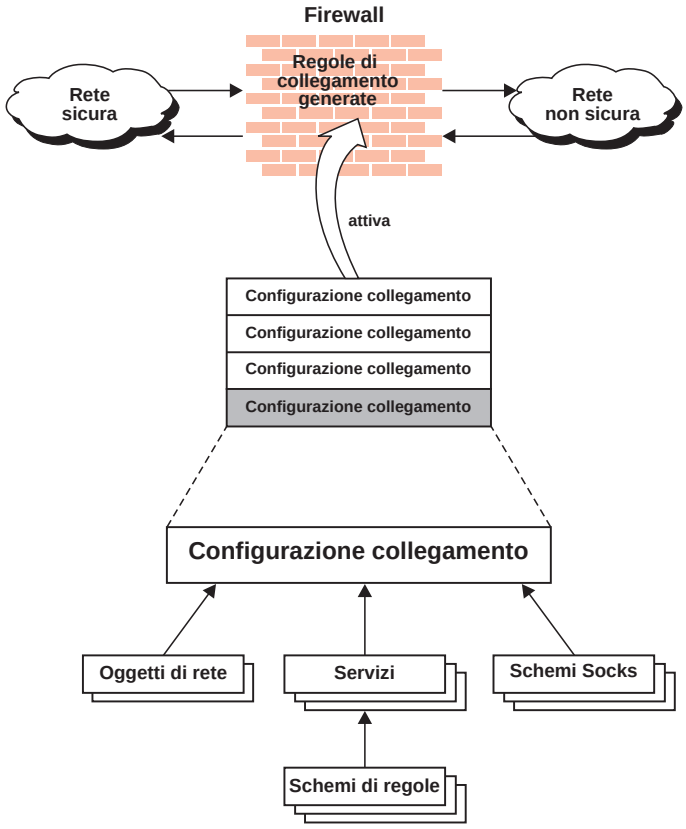

Figura 14. Creazione di collegamenti

Creazione dei collegamenti utilizzando i servizi predefiniti

Per consentire o negare specifici tipi di comunicazione tra due oggetti di rete denominati o tra gruppi di oggetti di rete che fungono da punti terminali, è necessario creare un collegamento.

Dopo avere definito i propri oggetti di rete è possibile creare i collegamenti. Selezionare un oggetto o un gruppo di oggetti di rete che deve fungere da origine ed un altro oggetto o gruppo di oggetti di rete che deve fungere da destinazione per il flusso del traffico sul firewall.

Per creare un collegamento, dall'albero di navigazione del client di configurazione, selezionare Controllo del Traffico e fare doppio clic sull'icona della cartella di file per espandere la vista. Selezionare **Impostazione collegamento**. Viene visualizzata la casella di dialogo **Elenco di collegamenti**. Selezionare **NUOVO** e fare clic su **Aprire**. Viene visualizzata la casella di dialogo **Aggiungere un Collegamento**, come illustrato nella Figura 15 a pagina 47.

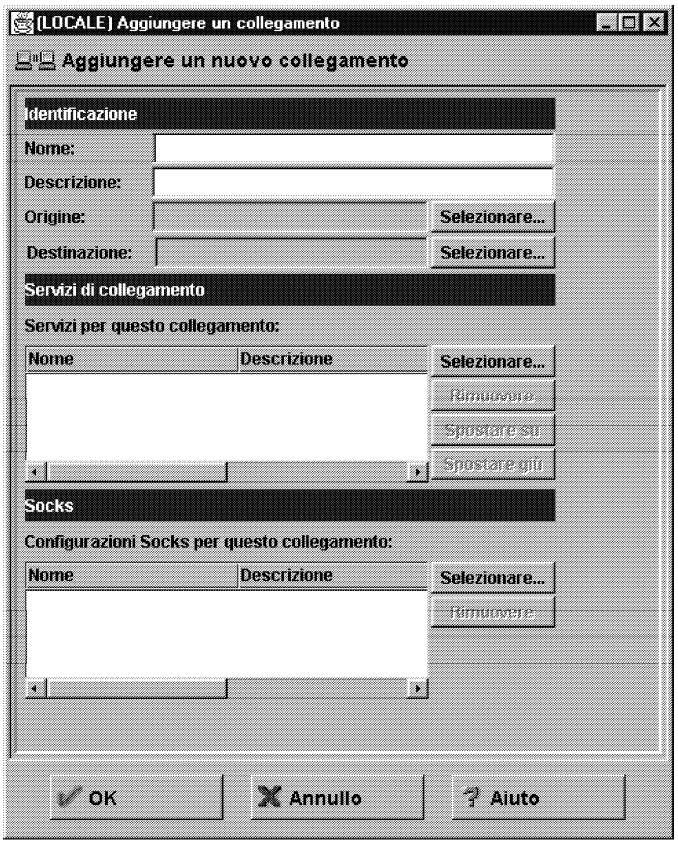

Figura 15. Aggiungere un Collegamento

1. Inserire un nome per il collegamento.
2. Immettere una descrizione del collegamento.
3. Per il campo di origine, fare clic su **Selezionare** e scegliere un oggetto di rete dall'elenco **Oggetti di rete**.
4. Per il campo di destinazione, fare clic su **Selezionare** e scegliere un oggetto di rete dall'elenco **Oggetti di rete**.
5. Per scegliere i servizi per questo collegamento, fare clic su **Selezionare** e scegliere il tipo di traffico che si desidera tra i punti finali.
6. Scegliere uno o più servizi dall'elenco per aggiungerli al collegamento.
7. È possibile riordinare l'elenco selezionando un servizio e facendo clic su **Spostare su** o **Spostare già**. Consultare la sezione “Ordinamento dei collegamenti” a pagina 48.
8. È possibile rimuovere un servizio selezionandolo e facendo clic su **Rimuovere**.
9. Utilizzare **Configurazioni Socks per questo collegamento**. Per eseguire collegamenti per Socks, seguire i passi 5–7.
10. Dopo aver definito ogni elemento, fare clic su **OK**.
11. Attivare tutti i collegamenti. Fare riferimento a “Attivazione dei collegamenti” a pagina 48.

Ordinamento dei collegamenti

Molti utenti di IBM Firewall dispongono di un numero inferiore a 1000 regole. Più regole ci sono, più forte sarà l'impatto sulle prestazioni.

Quando un'interfaccia di rete riceve un pacchetto in entrata o in uscita dall'host del firewall, le regole vengono applicate partendo dall'inizio delle regole di collegamento create. Quando le informazioni del pacchetto corrispondono esattamente alle informazioni contenute in una regola, viene eseguita l'azione (consentire o negare). Se l'intero file non contiene nessuna corrispondenza, la richiesta viene negata.

Suggerimento: Inserire i collegamenti più specifici nella parte alta dell'elenco ed i collegamenti meno specifici nella parte bassa dell'elenco. Ad esempio, è possibile avere un Dipartimento ABC, con un indirizzo 1.1.10.X ed una macchina utilizzata come server nel Dipartimento ABC, con un indirizzo 1.1.10.7. Se si desidera escludere la macchina 1.1.10.7 in quanto si tratta di un server da non utilizzare per il traffico telnet, occorre collocare il collegamento `Deny telnet for Dept ABC server` prima del collegamento `Permit telnet for Dept ABC`. Se si inverte l'ordine dei collegamenti, il collegamento di negazione non viene rilevato.

Attivazione dei collegamenti

Nota: Prima di attivare i collegamenti, accertarsi che la propria interfaccia sicura sia definita

Selezionare **Attivazione Collegamento** dall'albero di navigazione del client di configurazione per:

Rigenerare le regole di collegamento ed attivare Il firewall costituisce dalla configurazione di collegamento un insieme di regole di collegamento generate ed attiva questo insieme.

Disattivare regole di collegamento Il firewall viene protetto dalle regole assunte.

Elenco delle regole di collegamento correnti Viene visualizzato l'insieme delle regole di collegamento generate di recente. Se queste regole vengono precedentemente disattivate, non verranno utilizzate.

Convalidare la creazione di regole Le regole create sono valide o non valide.

Abilitare il log delle regole di collegamento Il firewall esegue il log del traffico selezionato con la funzione `log firewall`.

Disabilitare il log delle regole di collegamento Il log del firewall viene arrestato.

Viene visualizzata **Attivazione Collegamento**, come illustrato nella Figura 16 a pagina 49.

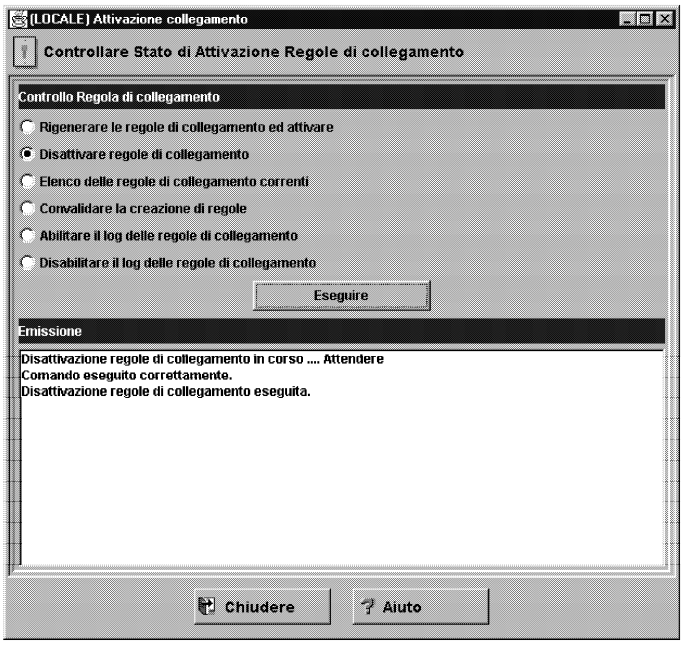

Figura 16. Attivazione Collegamento

Dopo aver eseguito una selezione, fare clic su **Eseguire**.

Emissione di log di esempio quando vengono rigenerate ed attivate le regole di collegamento

Di seguito viene riportato un esempio dell'emissione di log quando vengono rigenerate ed attivate le regole di collegamento.

```
Feb 03 13:46:53 1998 mr16n18: ICA9037i: Aggiornamento
automatico delle interfacce del firewall in corso
Giovedì 3 Febbraio 1998 alle ore 13:46:53.

Feb 03 13:46:55 1998 mr16n18: ICA1032i: Fregole di filtro aggiornate alle
13:46:55 del 3 Febbraio 1998

Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp gt  1023 eq 53 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
udp eq  53 gt  1023 both local both l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:4 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp     gt  1023 eq 25 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:5 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
tcp/ack eq  25 gt 1023 both local both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:6 permit 9.67.144.49 255.255.255.240
9.67.130.154 255.255.248.0 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:7 permit 9.67.130.154 255.255.248.
0 9.67.144.49 255.255.255.240 all any 0 any 0 both both both l=y f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:8 permit 9.67.144.49 255.255.255.240
9.67.131.250 255.255.255.255 tcp     gt  1023 eq  21 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:9 permit 9.67.131.250 255.255.255.255
9.67.144.49 255.255.255.240 tcp/ack eq  21 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:10 permit 9.67.131.250 255.255.255.
255 9.67.144.49 255.255.255.240 tcp     eq  20 gt  1023 secure local outbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:11 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp/ack gt  1023 eq  20 secure local inbound
l=n f=y t=0 e=none a=none
Feb 03 13:46:55 1998 mr16n18: ICA1037i: #:12 permit 9.67.144.49 255.255.255.
240 9.67.131.250 255.255.255.255 tcp     gt  1023 gt  1023 secure local inbound
l=n f=y t=0 e=none a=none
.
.
.
Feb 03 13:46:58 1998 mr16n18: ICA1037i: #:100 deny 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
all any 0 any 0 both both both l=y f=y t=0 e=none a=none
```

Determinazione degli stati delle regole

Le regole IBM Firewall possono trovarsi in uno dei seguenti stati:

1. La configurazione non è attiva.

   Non è stato ancora utilizzato il client di configurazione per attivare la configurazione oppure la configurazione è stata disattivata. Questo è lo stato della configurazione quando si installa per la prima volta IBM Firewall e si esegue il boot del sistema o si disattivano le regole di filtro. I filtri assunti proteggono la rete da intrusioni quando si esegue la prima installazione del firewall.

   Accesso al firewall:

- La configurazione dei filtri assunta consente tutto il traffico locale in arrivo e tutto il traffico in partenza.

2. La configurazione è attiva ma contiene degli errori.

   La configurazione è stata attivata. Esistono degli errori (regole non valide) nella configurazione oppure non è stato configurata nessuna regola. Gli errori e le avvertenze vengono visualizzati nella finestra di emissione Attivazione.

   Accesso al firewall:

   - Consentire tutto il traffico locale in arrivo.
   - Consentire tutto il traffico in partenza.

3. La configurazione è attiva e valida. È possibile che ci siano state avvertenze, relative soprattutto a regole di filtro duplicate.

   La configurazione definita dall'utente è stata attivata utilizzando la sezione relativa al controllo del traffico del client di configurazione.

   Nota: Il file di configurazione può essere valido e non contenere alcuna regola. In tal caso, risulta attiva la regola “deny all access”.

   Accesso al firewall:

   - L'accesso è determinato dal file di configurazione.

     Ogni pacchetto ricevuto o in procinto di essere inviato da una qualsiasi interfaccia di rete viene esaminato ed il suo contenuto posto a confronto con ciascuna delle regole di collegamento create. Quando viene trovata una corrispondenza, viene eseguita l'azione (consentire o negare l'accesso) su quella regola.
   - Se non vengono trovate corrispondenze tra le regole e il pacchetto, viene attivata la regola “deny all” che nega l'accesso.

Capitolo 9. Esempi di servizi

Questo capitolo descrive come configurare il firewall in modo da eseguire alcune attività comuni. Le attività qui elencate sono semplicemente degli esempi ma, una volta compreso i criteri su cui essi sono basati, l'utente sarà in grado di configurare il proprio firewall in modo da utilizzare tutti i servizi forniti.

Considerazioni sulla pianificazione

Il controllo del traffico del firewall è organizzato in termini di collegamenti che definiscono i tipi di comunicazione consentiti o proibiti tra coppie di punti terminali. È pertanto fondamentale pianificare i propri collegamenti tenendo conto dei punti terminali.

Come descritto nel Capitolo 8, “Controllo del traffico in transito sul firewall” a pagina 45, i punti terminali sono rappresentati sul firewall dagli oggetti di rete. Se non lo si è già fatto, occorre completare il modulo di pianificazione di rete nel Capitolo 2, “Pianificazione” a pagina 7 e creare gli oggetti di rete necessari per rappresentare la propria rete.

Gli esempi contenuti in questo capitolo utilizzano i seguenti oggetti di rete:

Interfaccia sicura L'interfaccia sicura del firewall.

Interfaccia non sicura
L'interfaccia non sicura del firewall.

Rete sicura
L'insieme di indirizzi accessibili mediante l'interfaccia sicura del firewall. Può trattarsi di un gruppo di oggetti di rete contenente più domini distinti, ognuno dei quali rappresentato da un proprio oggetto di rete.

Rete esterna La rete non sicura.

Ogni tipo di comunicazione desiderato deve essere visualizzato in base alla comunicazione punto terminale-punto terminale esistente. In questa fase, valutare se il firewall agirà come un proxy per le comunicazioni o se instraderà le comunicazioni.

Se il firewall agisce come un proxy, esso eseguirà le operazioni necessarie per conto dell'utente sicuro e gli host non sicuri non rileveranno mai la presenza dell'host sicuro. Se il firewall deve instradare il traffico, l'host sicuro e quello non sicuro comunicheranno direttamente tra loro.

Se si utilizza il firewall come un proxy, i punti terminali della comunicazione includeranno il firewall, come illustrato nella Figura 17 a pagina 54.

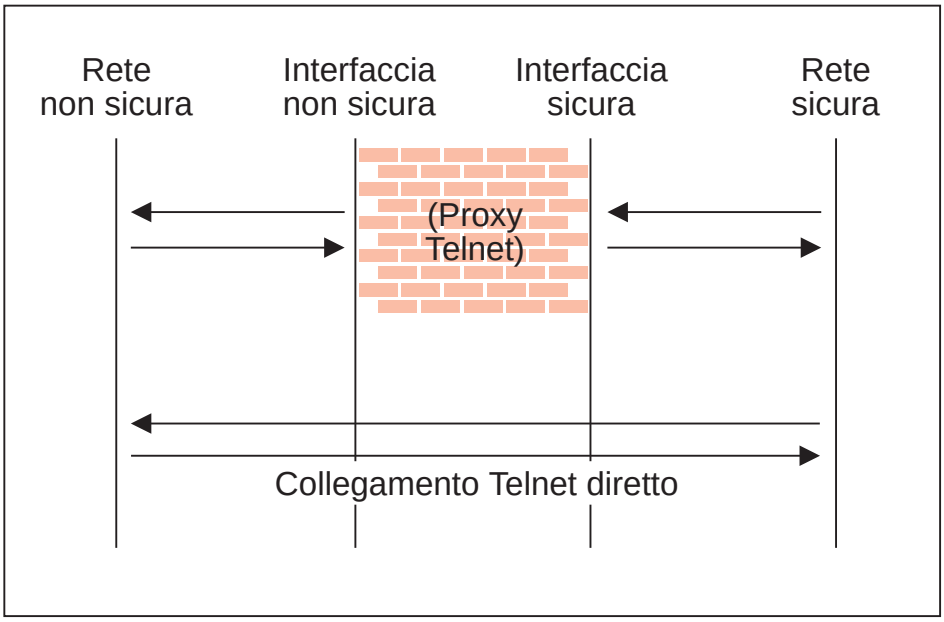

Figura 17. Proxy Telnet e collegamento Telnet diretto

Esempio di un proxy telnet

Questo primo esempio rappresenta un collegamento proxy telnet in partenza diretto. In questo esempio, gli utenti nella rete sicura potranno utilizzare il proxy telnet del firewall per accedere ai servizi telnet sugli host della rete non sicura.

Come descritto nella Figura 17, si verificano due collegamenti:

1. Il client all'interno della rete sicura è collegato al proxy telnet del firewall.
2. Il proxy telnet del firewall, è collegato, per conto dell'utente sicuro, all'host della rete non sicura.

Per configurare il controllo del traffico del firewall per questa comunicazione, occorre impostare due collegamenti:

Tabella 1. Proxy Telnet

Oggetto origine	**Oggetto di destinazione**	**Servizi richiesti**
Rete sicura	Interfaccia Sicura	Telnet Proxy out 1/2
Interfaccia non sicura	Rete esterna	Telnet Proxy out 2/2

Esempio di un telnet filtrato

Mettere a confronto l'esempio precedente con quello di un semplice collegamento telnet filtrato. In questo caso, il client della rete sicura stabilirà un collegamento diretto con l'host della rete non sicura.

Tabella 2. Telnet filtrato		
Oggetto origine	**Oggetto di destinazione**	**Servizi richiesti**
Rete sicura	Rete esterna	Telnet direct out

Come già indicato, questa configurazione esporrà gli indirizzi dei client sicuri quando questi si collegheranno agli host non sicuri.

Esempio di un proxy HTTP

La maggior parte delle installazioni verrà impostata in modo tale da permettere la navigazione in Web ad almeno alcuni dei client sicuri. IBM Firewall fornisce un servizio diretto in partenza HTTP predefinito per consentire un HTTP instradato, che funziona in modo identico al telnet filtrato di esempio. Il firewall fornisce, inoltre, un proxy HTTP.

Il protocollo HTTP, a differenza di quello Telnet, può incapsulare altri protocolli. Anche per la semplice navigazione, la maggior parte degli utenti avrà bisogno non solo di un proxy HTTP ma anche dei servizi FTP. Per fornire la piena funzionalità di HTTP sarà consentito anche l'utilizzo di Gopher e WAIS, sebbene essi siano utilizzati con una frequenza nettamente inferiore.

Quando vengono utilizzati, questi protocolli aggiuntivi vengono trasmessi in formato HTTP tra il client ed il proxy. La comunicazione si presenterà pertanto in modo simile al diagramma illustrato nella Figura 18.

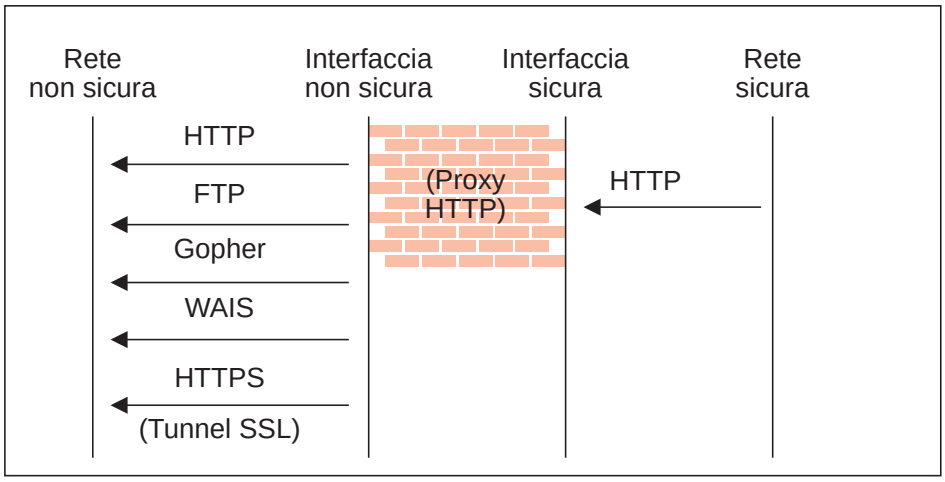

Figura 18. Proxy HTTP

Poiché sono coinvolte due coppie di punti terminali, occorre codificare due collegamenti.

Tabella 3. Proxy HTTP		
Oggetto origine	**Oggetto di destinazione**	**Servizi richiesti**
Rete sicura	Interfaccia Sicura	HTTP proxy outbound 1/2
Interfaccia non sicura	Rete esterna	Selezionare da... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Gopher proxy out 2/2 • WAIS proxy out 2/2 • HTTPS proxy out 2/2

Per ulteriori informazioni sul proxy HTTP, consultare il Capitolo 13, “Configurazione dei server proxy” a pagina 89.

Esempio di socks

Il socks svolge una funzione analoga a quella del proxy HTTP in quanto il daemon socks gestisce molti protocolli differenti e li incapsula in un singolo flusso di dati tra il firewall ed il client. Il socks è più flessibile del proxy HTTP in quanto può adattare qualsiasi protocollo orientato su TCP o UDP ed il firewall può essere configurato indipendentemente dai filtri per un ulteriore controllo delle comunicazioni.

A causa di questa maggiore flessibilità, la configurazione del socks richiede un terzo collegamento in aggiunta ai due illustrati per il proxy HTTP. I due collegamenti di base consentono il flusso dei pacchetti attraverso il firewall; il terzo collegamento serve ad indicare al daemon socks di agire come proxy per le richieste dopo avere ricevuto i pacchetti.

Tabella 4. Socks		
Oggetto origine	**Oggetto di destinazione**	**Servizi richiesti**
Rete sicura	Interfaccia Sicura	Socks 1/2
Interfaccia non sicura	Rete esterna	Selezionare da... • HTTP proxy out 2/2 • FTP proxy out 2/2 • Telnet proxy out 2/2 Qualsiasi servizio proxy relativo alla seconda metà (2/2) per cui si desidera fornire un supporto)
Rete sicura	Rete esterna	Nella finestra Configurazione socks, selezionare da... • permit socksified HTTP • permit socksified FTP • permit sockisfied Telnet

I client all'interno della rete sicura devono, ovviamente, essere con socks e configurati in modo da utilizzare il firewall come server socks.

Per ulteriori informazioni sul socks, consultare il Capitolo 11, “Configurazione del server Socks” a pagina 69.

Suggerimenti per il DNS

L'efficienza delle comunicazioni sarà limitata se non si fornisce una risoluzione DNS. Per ulteriori dettagli sulla configurazione del DNS, consultare il Capitolo 6, “Gestione del DNS (Domain Name Service)” a pagina 31. Abilitare "Consentire interrogazioni DNS" nella politica di sicurezza.

Suggerimenti per i client socks non sicuri

Il pannello Politica di sicurezza contiene una casella di spunta per **Negare Socks ad interfacce non sicure**. Questo servizio respingerà tutti i pacchetti indirizzati al daemon socks da interfacce non sicure e renderà il firewall molto più sicuro.

Se si desidera consentire ai client l'accesso alla propria rete da una rete non sicura, *non* attivare questa casella di spunta.

Capitolo 10. Personalizzazione del controllo del traffico

Questo capitolo aiuta l'utente a definire le regole di filtro ed i servizi. I servizi sono una raccolta di regole oppure una serie di istruzioni che consentono oppure negano uno specifico tipo di traffico attraverso il firewall, ad esempio una sessione telnet. È possibile aggiungere dei servizi utilizzando gli schemi di regole per creare delle nuove regole. È anche possibile eliminare dei servizi. I servizi socks sono validi per i collegamenti con socks.

IBM Firewall viene fornito con una serie assunta di servizi precaricati. È possibile personalizzare i servizi predefiniti in base alle proprie esigenze oppure crearne di nuovi.

Utilizzo del client di configurazione per creare degli schemi di regole

Utilizzare questa procedura per aggiungere una nuova regola all'elenco di schemi di regole disponibili.

1. Dall'albero di navigazione del client di configurazione, selezionare Controllo del Traffico e fare doppio clic sull'icona della cartella di file. Selezionare **Schemi di collegamento**, quindi selezionare **Regole**.
2. Nella casella di dialogo **Elenco di regole**, fare doppio clic su **NUOVO**.

   IBM Firewall visualizza una casella di dialogo **Aggiungere Regola IP**, come illustrato nella Figura 19, che consente di definire una regola.

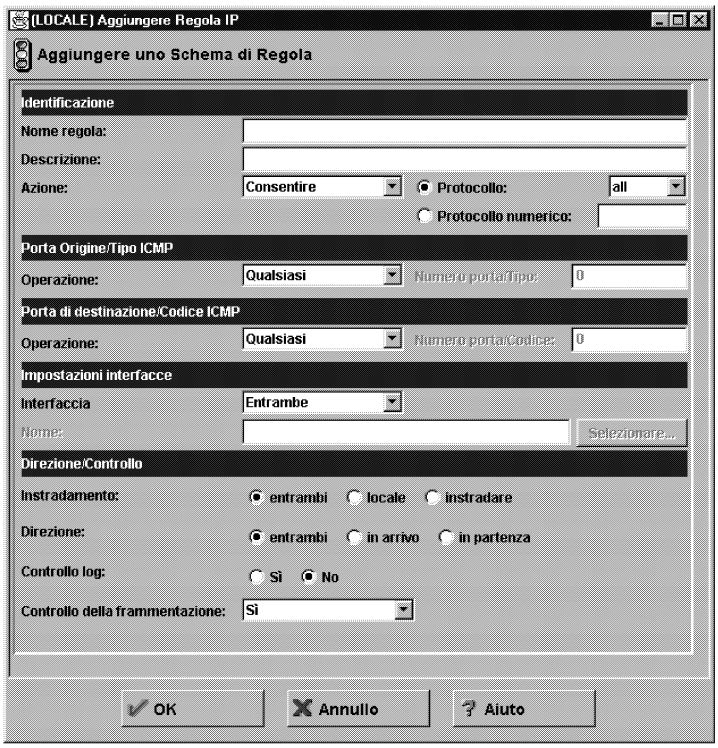

Figura 19. Aggiungere Regola IP

3. Immettere il Nome Regola.

4. Immettere la Descrizione. Questo campo è facoltativo.
5. Fare clic sulla freccia relativa all'azione e stabilire se consentire o negare l'accesso al firewall.
6. Fare clic sulla freccia relativa al protocollo ed eseguire una selezione dall'elenco:

   all Tutti i protocolli soddisferanno questa regola.

   tcp Il protocollo di pacchetto deve essere TCP (Transmission Control Protocol) per soddisfare tale regola.

   tcp/ack Il protocollo di pacchetto deve essere tcp/ack per soddisfare tale regola.

   udp Il protocollo di pacchetto deve essere UDP (User Packet Protocol) per soddisfare tale regola.

   icmp Il protocollo di pacchetto deve essere ICMP (Internet Control Message Protocol) per soddisfare tale regola.

   ospf Il protocollo di pacchetto deve essere ospf (open shortest path first) per soddisfare tale regola. Quando ospf è specificato come protocollo, l'operazione della porta di origine ed il valore della porta di origine vengono utilizzati per il valore di tipo record ospf. Sul tipo ospf è possibile eseguire anche la funzione di filtro. È possibile specificare un valore di tipo **any** ed i campi delle porte di destinazione devono essere specificati come **any 0**. Tutto il resto viene ignorato.

   ipip Il protocollo di pacchetto deve essere IPIP (IP-in-IP) per soddisfare tale regola. Quando IPIP è specificato, i campi delle porte devono essere specificati come **any 0**.

   esp Il protocollo di pacchetto deve essere esp (encapsulating security protocol), un protocollo utilizzato dalla VPN per inviare pacchetti IP incapsulati.

   ah Il protocollo ah (authentication header) è il protocollo di pacchetto utilizzato dalla VPN per inviare i pacchetti IP ai quali è associato un token di autenticazione.
7. Il protocollo numerico consente di specificare un protocollo utilizzando il relativo valore decimale (in base a RFC-1700). I valori validi sono quelli compresi tra 1 e 252. Quando si utilizza questa opzione, i campi relativi alle porte per questa regola devono essere impostati su 0 (corrispondente a qualsiasi porta). Consultare RFC-1700 per un elenco di tutti i protocolli. È possibile accedere a IANA (Internet Assigned Numbers Authority) direttamente con un browser.
8. Gli operandi dell'operazione e del numero porta sono utilizzati in combinazione. Le operazioni relative all'origine e alla destinazione stabiliscono una relazione tra il numero di porta (di origine o di destinazione) del pacchetto e gli operandi del numero di porta di origine e del numero di porta di destinazione. Ad esempio, se la porta di destinazione del pacchetto è la porta 20 e l'operazione di destinazione e la porta di destinazione sono “ge 15”, il pacchetto corrisponde (20 è maggiore o uguale a 15).

   Se si utilizza un'operazione di origine o di destinazione **any**, il filtro non prende in considerazione il numero di porta, in quanto qualsiasi porta corrisponde. In questo caso non è possibile cambiare il numero di porta.

Per il protocollo ICMP, specificare un tipo ICMP anziché una porta di origine, e specificare un codice ICMP anziché una porta di destinazione. L'operatore logico specificato viene applicato al tipo o codice e, per ciò che riguarda le porte, l'operatore "any" indica che per tale regola è adatto qualsiasi valore relativo al tipo e/o codice. In questo caso non è possibile cambiare il numero di porta.

I valori relativi all'operazione sono:

- Qualsiasi
- Uguale a
- Non uguale a
- Minore di
- Maggiore di
- Minore di o Uguale a
- Maggiore di o Uguale a

Di seguito sono riportate alcune delle più importanti porte da proteggere. I valori relativi ai numeri di porta devono essere compresi tra 1 e 65535:

Porta	**Utilizzo**
20	dati FTP
21	controllo FTP
23	Telnet
25	Posta
53	Domain Name Server
70	Gopher
80	HTTP
111	RPC
161	SNMP
1080	socks

Di seguito sono riportati alcuni tipi e codici ICMP:

Tipo	**Codice e Descrizione**
0	0 - Risposta ping
8	0 - Richiesta ping
3	1 - Host non raggiungibile
3	3 - Porta non raggiungibile
5	1 - Reindirizzare per l'host

9. Fare clic sulla freccia **Interfaccia** per selezionare il tipo di interfaccia (adattatore).

   entrambe Per pacchetti in arrivo o in partenza dall'interfaccia sicura o da quella non sicura.

   sicura Per pacchetti in arrivo o in partenza dall'interfaccia sicura.

   non sicura Per pacchetti in arrivo o in partenza dall'interfaccia non sicura.

specifica Se è stato assegnato un nome all'interfaccia, utilizzare con il campo relativo al nome dell'interfaccia quando se ne seleziona una.

10. Se si seleziona "specifica" per il tipo di interfaccia, il nome dell'interfaccia specifica verrà visualizzato nel campo Nome.
11. Fare clic sull'instradamento desiderato:

    entrambi Valido per tutto il traffico.

    locale Il pacchetto è locale rispetto all'host del firewall. Ciò significa che:

    - I pacchetti locali in arrivo sono pacchetti ricevuti dall'interfaccia e destinati a questo host del firewall; essi non verranno instradati ad un altro host. La loro destinazione è locale.
    - I pacchetti in partenza sono trasmessi dall'interfaccia, ma vengono creati sull'host del firewall. La loro origine è locale.

    instradare Il pacchetto viene instradato dall'host del firewall. Ciò significa che:

    - I pacchetti locali in arrivo sono pacchetti ricevuti dall'interfaccia e destinati ad un altro host; essi non resteranno sul firewall. La loro destinazione è remota.
    - I pacchetti in partenza sono trasmessi dall'interfaccia e vengono creati su un altro host. La loro origine è remota.
12. Fare clic sulla direzione desiderata:

    entrambe Per pacchetti in arrivo o in partenza dall'interfaccia selezionata

    in arrivo Per pacchetti in arrivo nell'interfaccia selezionata e provenienti dalla rete

    in partenza Per pacchetti in partenza dall'interfaccia selezionata e diretti alla rete
13. Se si seleziona Sì per il campo Controllo log, tutti i pacchetti corrispondenti alla regola specificata verranno registrati nel `log firewall` con un livello di priorità `Errore`. Se questo parametro non è specificato, il valore assunto è no.
14. Fare clic sulla freccia **Controllo della frammentazione** per scegliere il controllo della frammentazione desiderato. Perché le informazioni di pacchetto IP corrispondano ad una specifica regola di controllo della frammentazione, il controllo viene interpretato nel seguente modo:

    Sì La regola corrisponderà alle intestazioni di frammenti, ai frammenti ed ai non frammenti. Per i frammenti, le informazioni sulla porta saranno ignorate e ritenute corrispondenti.

    Solo La corrispondenza può avvenire solo con i frammenti e le intestazioni di frammenti. Per le intestazioni di frammenti, le informazioni sulla porta devono corrispondere. Per i frammenti, le informazioni sulla porta saranno ignorate.

    No Possono corrispondere solo i non frammenti. Frammenti e intestazioni di frammenti sono esclusi da questo parametro.

    Intestazioni Possono corrispondere solo i non frammenti e le intestazioni di frammenti. I frammenti sono esclusi da questo parametro.

    Se questo parametro non è specificato, il valore assunto sia per la regola "permit" che per la regola "deny" è "Sì".

Nota: **Indipendentemente dall'impostazione di questo controllo, i frammenti IP con offset uno (1), vengono ignorati**. Questa azione impedisce che l'utilizzo dei frammenti di pacchetto comporti la sovrapposizione degli indicatori di intestazione TCP.

Perché un'intestazione di pacchetto soddisfi una regola IP definita, le informazioni sul pacchetto devono corrispondere a tutti i parametri specificati nella regola codificata. Per i frammenti di pacchetto, tutti i parametri ad eccezione delle informazioni sulla porta vengono utilizzati per definire una corrispondenza.

Se i frammenti non sono stati consentiti da una regola precedente che presenta la codifica Sì o Solo, i frammenti di pacchetto verranno negati dalla regola finale che è sempre accodata al termine del file delle regole.

Modifica dell'entrata di configurazione della regola IP

Per modificare una regola IP creata:

1. Fare doppio clic su una regola esistente nella casella di dialogo **Elenco di regole**. Viene visualizzata la casella di dialogo **Modificare Regola IP**.
2. Modificare i campi appropriati come descritto nel Capitolo 10, “Personalizzazione del controllo del traffico” a pagina 59 e fare clic su **OK** per applicare le modifiche.

Eliminazione di una entrata di configurazione di regola

Per eliminare una regola, selezionare una regola da **Elenco di regole** e fare clic su **Eliminare**.

Servizi predefiniti

IBM Firewall viene fornito con una serie assunta di servizi precaricati. I servizi sono una raccolta di regole oppure una serie di istruzioni che consentono oppure negano uno specifico tipo di traffico attraverso il firewall, ad esempio una sessione telnet. È possibile aggiungere dei servizi utilizzando gli schemi di regole per creare nuove regole.

I servizi assunti precaricati sono:

All non-secure Negare tutto il traffico sull'interfaccia non sicura

All permit Consentire tutto il traffico (solo per scopi di debug)

All permit, in one direction Consentire tutto il traffico (solo per scopi di debug)

All secure Negare tutto il traffico sull'interfaccia sicura (in caso di violazione della sicurezza)

All shutdown Negare tutti i pacchetti (chiusura o debug)

Anti Spoofing Negare i pacchetti in arrivo non sicuri con indirizzo di origine sicuro

Broadcasts Negare messaggi di tipo broadcast ad interfacce non sicure

Config Client non-secure Consentire l'uso del client di configurazione dalla rete non sicura

Config Client secure Consentire l'uso del client di configurazione dalla rete sicura

CU-SeeMe Video CU-SeeMe sulle porte assunte 7649 e 7648

DNS queries (POLITICA DI SICUREZZA) Consentire le interrogazioni DNS

DNS transfers Consentire i trasferimenti di zona DNS (per server nomi secondari)

Domain Controller Authentication Consentire l'uso di Domain Controller per l'autenticazione dell'utente

FTP proxy in 1/2 Consentire FTP in arrivo da rete non sicura a firewall

FTP proxy in 2/2 Consentire FTP in arrivo da firewall a rete sicura

FTP proxy out 1/2 Consentire FTP in partenza da rete sicura a firewall

FTP proxy out 2/2 Consentire FTP in partenza da firewall a rete non sicura

Gopher proxy in 2/2 Consentire gopher da firewall a rete sicura

Gopher proxy out 2/2 Consentire gopher da firewall a rete non sicura

HTTP deny non-secure Negare HTTP ad interfacce non sicure

HTTP direct out Consentire HTTP da rete sicura direttamente a rete non sicura

HTTP proxy in 2/2 Consentire HTTP da firewall a rete non sicura

HTTP proxy out 1/2 Consentire HTTP (porta 8080) da rete sicura a firewall

HTTP proxy out 2/2 Consentire HTTP da firewall a rete non sicura

HTTPS direct out Consentire HTTPS (SSL) da rete sicura a rete non sicura

HTTPS proxy out 2/2 Consentire HTTPS (tunnel SSL) da firewall a rete non sicura

IDENTD Consentire l'identificazione degli utenti con protocollo Socks

Mail (POLITICA DI SICUREZZA) Consentire il traffico della posta sul firewall

NetBT Name Services broadcasts Consentire trasmissioni di tipo broadcast NetBIOS su TCP/IP Name Services

Ping Consentire ping in partenza da rete sicura a qualsiasi destinazione

SDI authentication Consentire il collegamento al server SecurID ACE nella rete sicura

Socks 1/2 Consentire l'uso del Socks da rete sicura a firewall

Socks deny non-secure Negare l'uso del Socks da adattatori non sicuri

Socks in 1/2 Consentire l'uso del Socks da rete non sicura a firewall

Telnet direct out Consentire Telnet in partenza da rete sicura a rete non sicura

Telnet proxy in 1/2 Consentire Telnet in arrivo da rete non sicura a firewall

Telnet proxy in 2/2 Consentire Telnet in arrivo da firewall a rete sicura

Telnet proxy out 1/2 Consentire Telnet in partenza da rete sicura a firewall

Telnet proxy out 2/2 Consentire Telnet in partenza da firewall a rete non sicura

VDOLIVE Direct In Consentire client non sicuri su server sicuri

Gli utenti devono configurare proprietà specifiche per utilizzare la porta UDP 7001.

VDOLIVE Direct Out Consentire client sicuri su server non sicuri

WAIS proxy in 2/2 Consentire WAIS (z39.50) da firewall a rete sicura

WAIS proxy out 2/2 Consentire WAIS (z39.50) da firewall a rete non sicura

Definizione dei servizi

Dopo avere definito delle regole, occorre aggiungerle ad un servizio. Selezionare Controllo del Traffico dall'albero di navigazione del client di configurazione e fare doppio clic su Schemi di collegamento e selezionare quindi Servizi. Viene visualizzata la casella di dialogo Elenco di servizi. Fare doppio clic su NUOVO per visualizzare la casella di dialogo Aggiungere un servizio, come illustrato nella Figura 20.

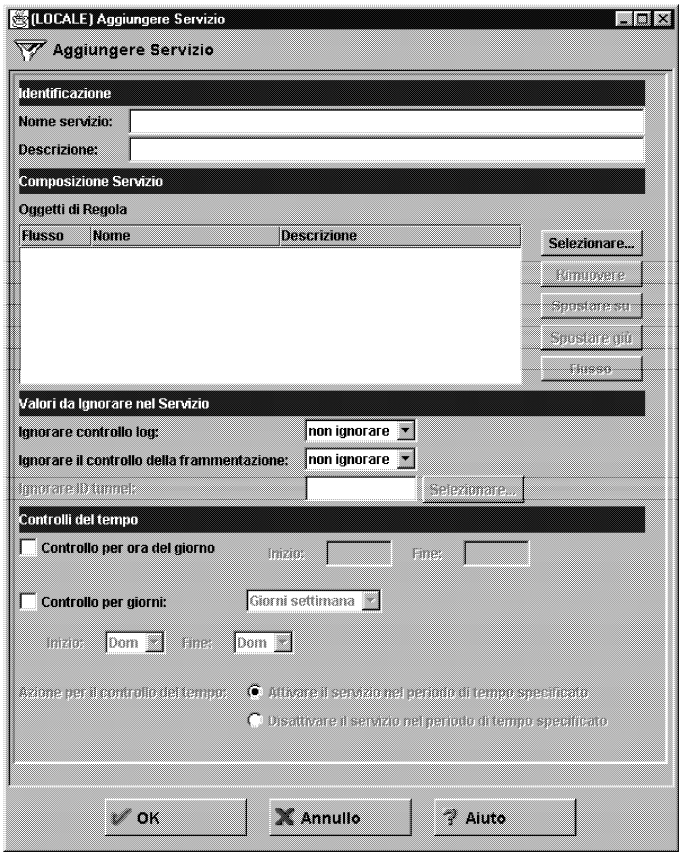

Figura 20. Aggiungere un Servizio

Utilizzo del client di configurazione per creare dei servizi

1. Immettere il nome servizio.
2. Immettere una descrizione.
3. Il campo **Ignorare controllo log** consente di sostituire l'impostazione relativa al controllo log negli schemi di regole selezionati per questo servizio. Ad esempio, se si include una serie di schemi di regole il cui controllo dei log è di norma impostato su No, è possibile sostituire questa impostazione con Sì per le funzioni di questo servizio. L'impostazione sostituita avrà effetto su tutte le regole contenute in questo servizio. Nel campo **Ignorare controllo log**, immettere una delle seguenti opzioni:

- nessuna sostituzione - la sostituzione è disattivata; le impostazioni specificate nelle regole sono ancora valide
- sì - scrivere un record di log quando vi è una corrispondenza ad una delle regole contenute in questo servizio
- no - non scrivere un record di log quando vi è una corrispondenza con una delle regole contenute in questo servizio

Quando per una regola di filtro viene scritto un record di log, i valori presenti in tale record sono quelli effettivi del pacchetto IP. Il log delle regole di filtro per le quali esiste una corrispondenza può fornire informazioni utili sul contenuto dei pacchetti IP controllati dal firewall, quali i protocolli effettivi ed i numeri di porta.

4. Il campo **Ignorare il controllo della frammentazione** consente di sostituire l'impostazione del controllo della frammentazione negli schemi di regole selezionati per questo servizio. Ad esempio, se si include una serie di schemi di regole il cui controllo della frammentazione è di norma impostato su No, è possibile sostituire questa impostazione con Sì per le funzioni di questo servizio. L'impostazione sostituita avrà effetto su tutte le regole contenute in questo servizio. Nel campo Ignorare il controllo frammentazione, immettere una delle seguenti scelte:
   - nessuna sostituzione - la sostituzione è disattivata; le impostazioni specificate nelle regole sono ancora valide
   - sì - corrispondenza con i pacchetti IP, ad esempio quelli non frammenti, le intestazioni di frammenti ed i frammenti senza intestazioni
   - no - corrispondenza solo con i pacchetti non frammenti, nessuna corrispondenza con le intestazioni di frammenti o con i frammenti senza intestazioni
   - solo - corrispondenza solo con le intestazioni di frammenti ed i frammenti senza intestazioni, non corrispondenza con i pacchetti non frammenti
   - intestazioni - corrispondenza solo con i non frammenti e le intestazioni di frammenti, nessuna corrispondenza con i frammenti senza intestazioni
5. I controlli del tempo consentono di associare un intervallo temporale ad ogni servizio. Pertanto, questo servizio sarà valido solo per questo periodo di tempo specificato. Se non si specifica un tempo, un servizio è sempre valido.

   Controllo per ora del giorno Selezionare per attivare o disattivare questo servizio in base ad un orario iniziale e finale nel corso della giornata. Utilizzare un formato di 24 ore. Se questo campo non è abilitato, i campi relativi all'ora del giorno saranno effettivi 24 ore su 24.

   Controllo per Giorni Selezionare per attivare o disattivare questo servizio in base ad una pianificazione basata sui giorni della settimana o sulle date. Un servizio è attivato o disattivato a seconda del valore specificato nel campo Azione per il controllo del tempo.

   Azione per il controllo del tempo Scegliere **Attivare il servizio nel periodo di tempo specificato** se si desidera che questo servizio sia attivato durante il periodo di tempo specificato. Questo servizio sarà disattivato nei periodi che non rientrano in quello specificato.

   Scegliere **Disattivare il servizio nel periodo di tempo specificato** se si desidera che questo servizio sia disattivato nel periodo di

tempo specificato. Questo servizio sarà attivato nei periodi di tempo che non rientrano in quello specificato.

6. Fare clic su **Selezionare** per scegliere le regole che formano questo servizio.
7. Utilizzare il commutatore Flusso per determinare il modo in cui i valori Origine e Destinazione del collegamento devono essere assegnati ai filtri quando vengono scritti nel file di database delle regole.

   ```
   --> La freccia rivolta verso destra indica che l'origine e la
   destinazione del collegamento vengono scritte direttamente nella
   regola quando questa viene scritta nel file di database delle regole.

   <--- La freccia rivolta verso sinistra indica che l'origine e
   la destinazione del collegamento sono invertite quando vengono scritte
   nel file di database delle regole.
   ```

8. Quando viene ricevuto un pacchetto, IBM Firewall confronta le informazioni in esso contenute con le regole presenti nel file di configurazione delle regole, partendo dall'inizio del file. Quando viene trovata la prima corrispondenza esatta, il confronto viene interrotto e viene eseguita l'azione contenuta nella regola.

   Una volta aggiunto un insieme di regole al servizio, è possibile modificarne l'ordine. Selezionare una regola dall'elenco **Oggetti di servizio** e fare clic sui pulsanti **Spostare su** o **Spostare giù** per modificare la posizione della regola. È inoltre possibile rimuovere una regole facendo clic su **Rimuovere**. Il client di configurazione visualizza un elenco di regole aggiornato. Fare clic su **OK** per salvare le modifiche.

Capitolo 11. Configurazione del server Socks

Socks è uno standard Internet per i gateway a livello di circuito. Utilizzare il server Socks per la conversione degli indirizzi se la propria applicazione utilizza TCP, ad esempio il browser Web, l'FTP o le applicazioni Telnet. Socks facilita l'accesso ad Internet, nascondendo gli indirizzi IP interni.

Per le richieste in partenza da un client sicuro ad un server non sicuro il server Socks svolge le stesse funzioni di un server proxy: interrompere la sessione sul firewall e fornire una porta sicura che consente agli utenti di accedere alla rete esterna, non sicura, proteggendo allo stesso tempo l'indirizzamento e la struttura della rete interna. Il server Socks ha il vantaggio della semplicità per l'utente, con un minimo lavoro di gestione supplementare.

Il server Socks può intercettare tutte le richieste TCP in partenza che intercorrono tra la propria rete ed Internet. Il server Socks fornisce un'API remota (application program interface), cosicché le funzioni eseguite dai programmi client nei domini sicuri vengono incanalate attraverso server sicuri sulle stazioni di lavoro del firewall, nascondendo l'indirizzo IP del client. L'accesso è controllato dai filtri associati alle regole Socks.

Il server Socks è simile al server proxy. La differenza risiede nel fatto che mentre il server proxy esegue effettivamente la funzione TCP/IP sul firewall, il server Socks si limita ad identificare l'utente ed a reindirizzare la funzione sul firewall. La funzione TCP/IP effettiva viene eseguita sulla stazione di lavoro del client, e non sul firewall. In questo modo viene evitata l'elaborazione sul firewall. Gli utenti della rete sicura possono utilizzare i vari prodotti TCP/IP che supportano gli standard Socks. La Figura 21 illustra il server Socks che intercetta una richiesta HTTP da un client all'interno della rete sicura.

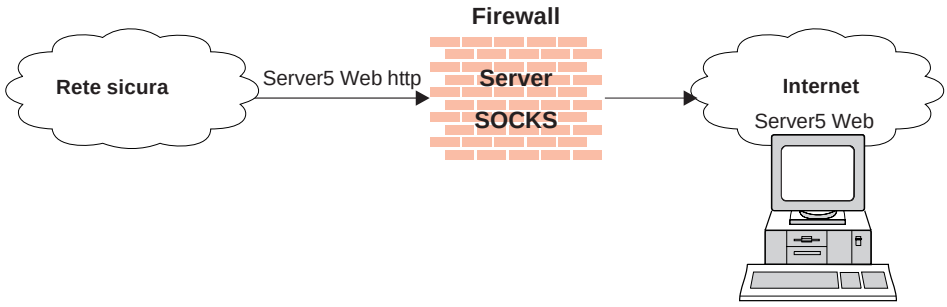

Figura 21. Il server Socks

Il server Socks nasconde in modo efficiente gli indirizzi IP agli utenti esterni.

IBM Firewall fornisce il Socks Protocol Versione 5 che consente ai client all'interno della rete sicura di passare per una fase di autenticazione prima di accedere alle applicazioni della rete non sicura. Fornisce inoltre il proxy generico autenticato ed il proxy di alcuni protocolli di diffusione audio e video.

Il daemon Socks viene eseguito come un servizio Windows NT, avviato automaticamente all'avvio del sistema. Inoltre, per consentire il controllo del server, viene fornito un agente analizzatore. È possibile avviare Watch Agent manualmente.

IBM Firewall fornisce un semplice percorso di migrazione sotto forma di tre profili di autenticazione, in modo che gli utenti possano continuare ad utilizzare i client del Socks Protocol Versione 4 installati quando introducono i client del Socks Protocol Versione 5.

1. Il profilo più permissivo non abilita l'autenticazione in partenza e consente il collegamento a tutti gli utenti che utilizzano un client del Socks Protocol Versione 4 o Versione 5. In questo scenario, i collegamenti in arrivo vengono negati.
2. Il profilo di migrazione consente il collegamento senza autenticazione agli utenti del Socks Protocol Versione 4, ma richiede che gli utenti del Socks Protocol Versione 5 vengano autenticati. I collegamenti del Socks Protocol Versione 4 in arrivo vengono negati, mentre per i collegamenti del Socks Protocol Versione 5 viene richiesta l'autenticazione. Questo rappresenta il profilo assunto.
3. Il profilo più sicuro richiede che tutti gli utenti utilizzino i client del Socks Protocol Versione 5 e forniscano autenticazioni valide.

Quando viene installato il firewall, viene abilitato il server socks ma nel file di configurazione di socks non esistono regole. Perché i client Socks possano utilizzare il server Socks, è necessario configurare il socks utilizzando il client di configurazione. Consultare la sezione “Esempio di socks” a pagina 56, per un esempio di modalità di impostazione di un servizio socks.

Protocolli supportati dal server Socks Protocol Versione 5

Il server Socks Protocol Versione 5 supporta i protocolli TCP di seguito riportati ed altri ancora:

- Archie
- Finger
- FTP
- Gopher
- HTTP
- Proxy HTTP
- News
- SNMP
- Telnet
- TFTP
- RealAudio
- RealPlayer
- Whois
- X-Windows

Vengono inoltre supportati molti client di posta elettronica. Il supporto per questi protocolli dipende dall'effettiva realizzazione.

Configurazione del server Socks utilizzando il client di configurazione

Gli schemi Socks sono regole che controllano la sicurezza sul server Socks. Consentono di personalizzare, aggiungere, copiare o eliminare gli schemi socks esistenti. Questi schemi socks, a loro volta, possono essere utilizzati per definire i collegamenti sul firewall nello stesso modo degli schemi di regole.

Aggiunta di una nuova regola socks

Per aggiungere una regola al file di configurazione di socks utilizzando uno schema socks fornito dal client di configurazione, selezionare Controllo del Traffico dall'albero di navigazione del client di configurazione. Fare doppio clic sull'icona della cartella di file per espandere la vista. Selezionare Schemi di collegamento. Fare doppio clic sull'icona della cartella di file per espandere la vista. Selezionare **Socks**. Viene visualizzata la casella di dialogo **Socks**.

1. Fare clic su **NUOVO** per aggiungere un nuovo schema socks.

   Viene visualizzata la casella di dialogo **Aggiungere una Regola Socks**, come illustrato nella Figura 22.

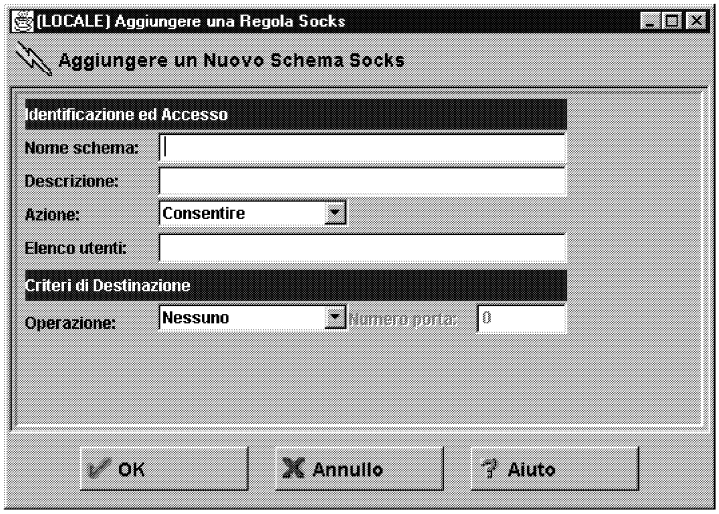

Figura 22. Aggiungere una Regola Socks

2. Nel campo **Nome schema**, immettere il nome dell'entrata socks. Questo nome deve essere univoco e non deve contenere un simbolo di pipe (|), un carattere di singolo apice o apostrofo (') oppure un carattere di doppi apici (") poiché tali simboli sono utilizzati come delimitatori di file. L'uso di questi caratteri può fornire dati non attendibili.
3. Immettere una descrizione.
4. Fare clic su Azione e scegliere se consentire o negare l'accesso da un'origine ad una destinazione.

   Quando riceve un datagram, un server Socks ne confronta le specifiche con ciascuna regola presente nel file di configurazione, a cominciare dalla prima regola e fino a trovarne una che corrisponda esattamente. Quindi la ricerca viene interrotta e sulla regola viene eseguita la relativa azione per consentire o negare l'accesso. Se non viene trovata nessuna corrispondenza, l'accesso è negato automaticamente.

5. Nel campo **Elenco utenti**, è possibile immettere un ID utente o un elenco di ID utente. Se si immette un elenco, separare le entrate utilizzando le virgole. Non utilizzare spazi, tabulazione, il simbolo di pipe (|) o i doppi apici (") nell'elenco utenti.
   - L'elenco utenti ha un limite massimo di 396 caratteri.
   - Gli ID utente devono essere ID di utenti presenti sull'host che effettua la richiesta e non ID di utenti presenti sull'host di destinazione o sull'host del server Socks.
   - Un ID utente può essere composto da 1 a 8 dei seguenti caratteri:
     – dalla a alla z
     – dalla A alla Z
     – da 0 a 9
     – _ (carattere di sottolineatura)
6. Un ID utente non deve contenere il simbolo di pipe (|) ed i doppi apici (").
7. Se vengono utilizzati, i nomi file devono essere completi, inclusa la barra "/" iniziale per evitare che vengano interpretati come ID utente. Ciascun file può contenere un elenco di ID utente, con uno o più ID per riga separati da virgole ed eventualmente presentare un commento delimitato dal carattere #. Sono supportate anche righe intere di commento, che iniziano con il carattere #. Ciascuna riga del file può contenere fino a 1023 caratteri e deve terminare con un carattere di "avanzamento riga".
8. Nel campo **Operazione**, immettere l'operazione logica da eseguire sul numero di porta:

eq	Uguale a
neq	Non uguale a
lt	Minore di
gt	Maggiore di
le	Minore di o Uguale a
ge	Maggiore di o Uguale a

   Quando viene utilizzato con il numero di porta, l'operazione logica stabilisce una relazione da rispettare. Ad esempio, se si immette l'operatore gt(>) ed il numero di porta 23, il numero di porta deve essere maggiore di 23 perché la regola possa essere richiamata.
9. Nel campo **Numero di porta**, immettere il numero di una porta. Il numero di porta viene utilizzato con l'operazione per stabilire una relazione da rispettare. Ad esempio, se si immette l'operatore gt(>) ed il numero di porta 23, il numero di porta deve essere maggiore di 23 perché la regola possa essere richiamata. Se l'operazione ed il numero di porta vengono omessi, la regola viene applicata a tutti i numeri delle porte di destinazione.

Utilizzare la casella di dialogo **Aggiungere una Regola Socks** per consentire o negare l'accesso al firewall agli host della rete in base all'indirizzo IP.

Modifica di una regola socks

1. Fare doppio clic su un'entrata della casella di dialogo **Socks**.

   Viene visualizzata la casella di dialogo **Modificare una Regola Socks**.

2. Modificare i campi appropriati come descritto nella sezione “Aggiunta di una nuova regola socks” a pagina 71, e fare clic su **OK**.

Eliminazione di una regola socks

Selezionare un'entrata dalla casella di dialogo **Socks** e fare clic su **Eliminare**. Viene richiesta la conferma dell'eliminazione della regola socks. Fare clic su **OK** per eliminare la regola.

Attivazione delle regole di collegamento

Come per le regole di filtro, occorre attivare le regole socks. Fare clic su **Attivazione Collegamento** nell'albero di navigazione del client di configurazione, selezionare **Rigenerare le regole di collegamento ed attivare**, quindi fare clic su **Eseguire**.

Il firewall copia le regole dal file di configurazione socks nelle regole del firewall e le attiva. Quando le regole vengono attivate, le nuove regole vengono registrate nel file di log del firewall.

Emissione di log di esempio relativa a Socks

Di seguito viene riportato un esempio dell'emissione di log relativa a Socks.

```
Feb 03 13:46:20 1998 mr16n18: ICA3123i: Avvio del server sockd in corso
Feb 03 13:47:31 1998 mr16n18: ICA3010i: Avvio della sessione
Feb 03 13:47:31 1998 mr16n18: ICA3011i: Avvio della sessione
Feb 03 13:49:15 1998 mr16n18: ICA3007i: Troppi thread
Feb 03 13:58:31 1998 mr16n18: ICA3015i: Fine sessione
```

Valutazioni dei client per l'utilizzo del server Socks

La maggior parte dei browser Web sono con socks ed è possibile ottenere degli stack con socks per la maggior parte delle piattaforme. Client con socks per altre applicazioni TCP/IP sono disponibili da molte fonti. Per uno specifico client che implementa i socks, consultare la documentazione del client. Per ulteriori informazioni, consultare:

http://www.raleigh.ibm.com/sng/sng-socks.html
http://www.socks.nec.com

Concatenamento di server Socks

Il Concatenamento di server Socks è una funzione mediante la quale un server Socks può risiedere dietro un altro server Socks e continuare a consentire l'accesso alla rete oltre il server Socks più esterno (è come assegnare una funzione socks ad un server socks). Questo è uno scenario intranet molto utile.

Per impostare il concatenamento dei server Socks con il server Socks, editare il file `socks5.header.cfg`. Questo file risiede nel sottoindirizzario `config` del firewall. Aggiungere quanto segue:

- Una direttiva *no proxy*, per indicare le sottoreti a cui il firewall ha accesso diretto
- Una direttiva *socks4*, per indicare le sottoreti accessibili mediante un server SOCKS Protocol Versione 4
- Una direttiva *socks5*, per indicare le sottoreti accessibili mediante un server Socks Protocol Versione 5

Ad esempio, consideriamo la seguente rete. Il dipartimento delle ricerche ha una piccola rete privata, *q.private.com*, dietro il proprio firewall. La sottorete di questo dipartimento è 10.007.007.0/255.255.255.0. La rete privata della società, *private.com*, contiene l'intera rete 10.0.0.0/255.0.0.0. Il server SOCKS Protocol Versione 4, *socks.private.com*, fornisce l'accesso ad Internet.

Sul server Socks del dipartimento, *socks.q.private.com*, aggiungere le seguenti righe a `socks5.header.cfg`.

```
no proxy 10.0.0.0/255.0.0.0 - - -
socks4      0/0   - socks.private.com 1080
```

Infine, aggiungere un collegamento di controllo del traffico per consentire a *socks.q.private.com* di comunicare con *socks.private.com*. Ciò potrebbe essere già stato fatto da un servizio più generale. Aggiungere un collegamento la cui origine è l'interfaccia non sicura del firewall *q.private.com*, la cui destinazione è *socks.private.com* ed includere il servizio *Concatenamento Proxy Socks*. Riattivare quindi le regole di controllo del traffico.

Capitolo 12. Gestione degli utenti del firewall

Questo capitolo descrive come eseguire le seguenti attività di gestione quotidiane con IBM Firewall:

- Aggiunta di utenti a IBM Firewall per permettere loro di accedere ad host che non fanno parte della rete protetta
- Modifica degli attributi degli utenti che accedono al firewall
- Eliminazione degli utenti cui non occorre più accedere all'esterno della rete

Non editare i file di configurazione direttamente; in questo caso gli attributi utente IBM Firewall non saranno impostati correttamente. Eseguire tutte le attività di gestione IBM Firewall utilizzando le caselle di dialogo del client di configurazione oppure la riga comandi.

Aggiunta di un utente a IBM Firewall

IBM Firewall definisce tre tipi di utenti e ne memorizza le informazioni in due diversi database.

Tipi di utenti

IBM Firewall divide gli utenti in tre categorie:

Utenti proxy Utilizzano i servizi del firewall, ad esempio il servizio proxy HTTP, per accedere ai siti Web su Internet da una rete aziendale. Gli utenti proxy possono utilizzare i servizi del firewall ma non hanno accesso alla macchina firewall e non possono eseguire i login locali alla macchina firewall.

Responsabili del firewall Possono utilizzare i servizi proxy del firewall ma possono anche configurare il firewall, utilizzando il client di configurazione e collegandosi al firewall da un host remoto. Come gli utenti proxy, i responsabili del firewall non possono eseguire i login locali alla macchina firewall.

I responsabili del firewall possono creare e modificare le definizioni relative agli utenti proxy ma non possono creare o modificare le definizioni di altri responsabili del firewall.

Responsabili principali del firewall Ricoprono le stesse funzioni dei responsabili del firewall, ma possono anche eseguire i login locali alla macchina firewall. I responsabili principali del firewall possono creare e modificare le definizioni relative ad altri responsabili del firewall.

Tipi di database

Esistono due tipi di database degli utenti.

Database degli utenti del firewall Contiene gli attributi correlati al firewall relativi a tutti gli utenti e responsabili proxy. Sono compresi attributi quali la parola d'ordine per il firewall dell'utente, le regole relative alla parola d'ordine ed i metodi di autenticazione da utilizzare per autenticare l'utente per ciascun servizio.

Se l'utente proxy non è definito nel database degli utenti del firewall ma cerca di utilizzare i servizi proxy del firewall, verrà utilizzato il record dell'utente assunto, `fwdfusr`, per definire gli attributi e gli schemi di autenticazione utilizzati per convalidare l'utente.

I responsabili principali del firewall non possono essere definiti nel database degli utenti del firewall. Per assegnare attributi ai responsabili, utilizzare il record del responsabile del firewall assunto, `fwdfadm`.

Come gli utenti proxy, se i responsabili del firewall sono definiti anche nel database degli utenti di Windows NT, le loro parole d'ordine per il collegamento ad NT verranno utilizzate quando l'utente richiede i servizi che devono essere autenticati mediante le parole d'ordine per l'accesso a NT.

Database degli utenti di Windows NT Contiene le parole d'ordine degli utenti per il collegamento a NT. In generale, gli utenti proxy non devono essere definiti nel database degli utenti NT, a meno che non si desideri autenticarli utilizzando la parola d'ordine per il collegamento a NT.

Se per autenticare gli utenti proxy si desidera utilizzare altri metodi di autenticazione, non è necessario definire gli utenti proxy nel database degli utenti di Windows NT.

I responsabili principali del firewall sono gli utenti di Windows NT che fanno parte del gruppo di responsabili NT e pertanto devono essere definiti nel database degli utenti di Windows NT.

Utilizzo del client di configurazione per aggiungere un utente

Un utente aggiunto a IBM Firewall ha la possibilità di accedere alla rete esterna.

1. Dall'albero di navigazione del client di configurazione, selezionare Utenti. Viene visualizzata la casella di dialogo **Gestione Utente**.
2. Selezionare **Nuovo** dalla casella di dialogo **Gestione Utente** e fare clic su **Aprire**. Viene visualizzata la casella di dialogo **Aggiungere Utente**, come illustrato nella Figura 23 a pagina 77.

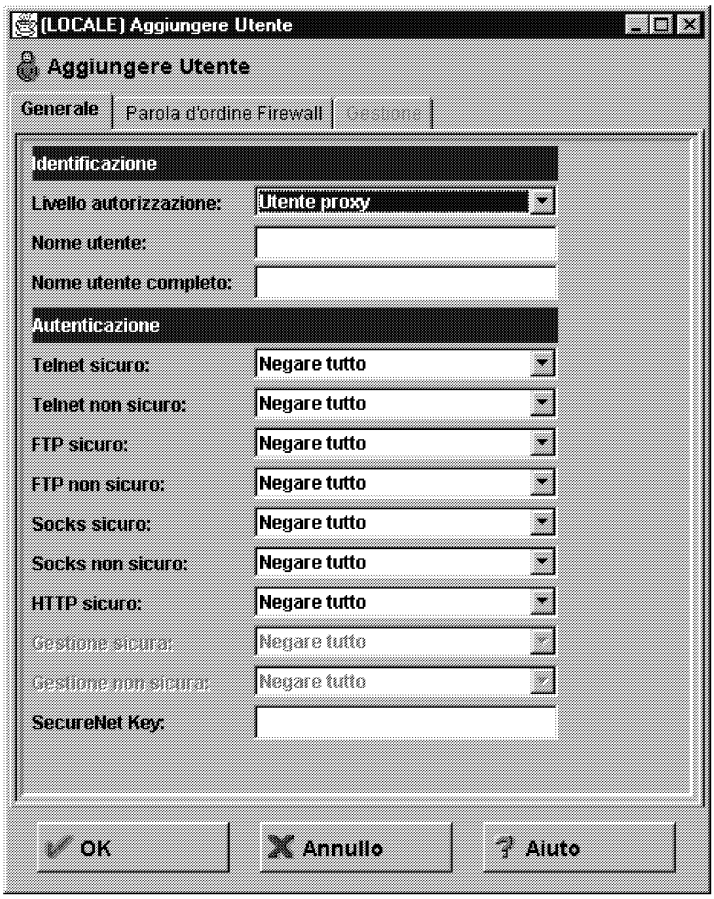

Figura 23. Aggiungere Utente

3. Fornire le seguenti informazioni:

   Livello di autorizzazione

   Specifica il livello di autorizzazione per questo utente. Fare clic sulla freccia **Livello autorizzazione** per selezionare il tipo di utente.

   Socks/Utente proxy L'utente che viene definito ha accesso al server Socks e al proxy. Questo utente non possiede l'autorizzazione alla gestione. Questo è il valore assunto.

   Responsabile firewall

   Dispone di tutti gli attributi di un utente ma può anche eseguire il login al firewall ed eseguire attività di gestione. Un responsabile dispone degli attributi supplementari che definiscono le funzioni di gestione che il responsabile è autorizzato ad eseguire. Un responsabile del firewall può creare utenti del firewall, ma non può creare altri

responsabili del firewall. I responsabili del firewall non possono eseguire il login localmente alla macchina firewall. Devono accedere al server di configurazione da una macchina remota.

Responsabile principale del firewall

Al responsabile principale del firewall è consentito eseguire il login locale alla macchina firewall. Questo responsabile dispone dell'accesso completo a tutte le funzioni di gestione. Può inoltre creare altri responsabili del firewall, ad eccezione dei responsabili principali.

Il responsabile principale del firewall viene definito creando un utente nel database degli utenti NT e rendendo tale utente un membro del gruppo dei responsabili NT. Per definire gli attributi relativi al responsabile principale del firewall, modificare il record `fwdfadm`.

Nome utente

Specifica il nome di questo utente. Questo è il nome utente con cui questo utente eseguirà il login al server telnet o FTP su IBM Firewall. Non deve essere necessariamente il nome host o utente TCP/IP dell'utente anche se possono essere uguali.

Un nome utente può essere composto da 1 a 20 caratteri:

dalla a alla z
dalla A alla Z
da 0 a 9
_ (carattere di sottolineatura)

I nomi utente sono sensibili al maiuscolo/minuscolo.

Il firewall è dotato di due utenti preinstallati:

a. Utente assunto o `fwdfuser`. Se un utente non è definito nel database del firewall, `fwdfuser` viene utilizzato per determinare gli attributi firewall dell'utente, ad esempio i metodi di autenticazione da utilizzare quando viene autenticato un utente.

   In fase di installazione, quando viene creato `fwdfuser`, tutti i metodi di installazione vengono impostati su "deny all". L'autorizzazione per `fwdfuser` controlla il modo in cui il firewall elabora i nomi utente non definiti.

Il responsabile può visualizzare `fwdfuser` oppure modificare il metodo di autenticazione assegnato utilizzando il client di configurazione oppure la riga comandi. In ogni caso, `fwdfuser` non può essere eliminato e deve necessariamente essere presente nel firewall. Parola d'ordine firewall e SNK, inoltre, non rappresentano tipi di autenticazione validi per `fwdfuser`. Per ulteriori informazioni, consultare *IBM eNetwork Firewall - Manuale di riferimento.*

b. Il responsabile principale del firewall assunto, `fwdfadm`, definisce gli attributi del firewall relativi a tutti i responsabili principali del firewall. Dal momento che i responsabili principali del firewall non dispongono di propri record di utenti nel database del firewall, questo record viene utilizzato per definire i metodi di autenticazione per autenticare i responsabili principali del firewall.

   In fase di installazione, tutti i metodi di autenticazione per `fwdfadm` sono impostati su *deny all*, ad eccezione dei metodi di autenticazione per la gestione sicura e non sicura, che sono impostati sulla parola d'ordine per l'accesso a NT. I responsabili principali del firewall possono visualizzare e modificare questo record, ma non possono eliminarlo. Inoltre, la parola d'ordine del firewall e SNK non rappresentano tipi di autenticazione validi per `fwdfadm`.

Nome utente completo
Specifica una descrizione dell'utente.

I seguenti campi fanno riferimento ai metodi di autenticazione: Fare clic sulle frecce per eseguire una selezione dall'elenco dei metodi di autenticazione. Queste scelte sono spiegate nella sezione “Metodi di autenticazione utente” a pagina 81.

Telnet sicuro Indica se, quando si esegue il login dalla rete sicura, l'identità di questo utente deve essere in qualche modo autenticata.

Telnet non sicuro Indica se, quando si esegue il login dalla rete non sicura, l'identità di questo utente deve essere in qualche modo autenticata.

FTP sicuro Specifica il livello di autenticazione che occorre all'utente per utilizzare FTP per accedere al firewall dalla rete sicura.

FTP non sicuro Specifica il livello di autenticazione che occorre all'utente per utilizzare FTP per accedere al firewall dalla rete non sicura.

Socks sicuro Specifica il metodo di autenticazione Socks V5 per i collegamenti ai client Socks in arrivo dalla parte sicura del firewall. Fare clic sulla freccia per eseguire una selezione da un elenco di scelte disponibili. Tali scelte sono illustrate nella sezione “Metodi di autenticazione utente” a pagina 81.

Socks non sicuro Specifica il metodo di autenticazione Socks V5 per i collegamenti ai client Socks in arrivo dalla parte non sicura del firewall. Fare clic sulla freccia per eseguire una selezione da un elenco di scelte disponibili. Tali scelte sono illustrate nella sezione “Metodi di autenticazione utente” a pagina 81.

HTTP sicuro Specifica un tipo di autenticazione della parola d'ordine/ID utente sulle richieste proxy HTTP in partenza. Fare clic sulla freccia per eseguire una selezione da un elenco di scelte disponibili. Tali scelte sono illustrate nella sezione “Metodi di autenticazione utente” a pagina 81.

Il browser richiede l'ID utente e la parola d'ordine, per cui, se si utilizza SDI, inserire il codice di accesso alla richiesta della parola d'ordine.

Per il metodo di autenticazione fornito dall'utente, si consideri che Socks/parola d'ordine non supporta la modalità interattiva mediante caselle di dialogo.

Gestione sicura Specifica il metodo di autenticazione utilizzato per collegarsi dal client di configurazione tramite un'interfaccia sicura. Quando ci si collega in modo locale (scegliendo "locale" nel pannello di collegamento) ci si trova sempre in un ambiente sicuro ed è pertanto il metodo di autenticazione raccomandato.

Gestione non sicura

Specifica il metodo di autenticazione utilizzato per collegarsi dal client di configurazione tramite un'interfaccia non sicura.

SecureNet Key Specifica la sequenza di caratteri che deve essere immessa dall'utente remoto che dispone di una scheda SecureNet Key della AssureNet Pathways. Immettere il codice chiave con cui verrà altresì attivata la scheda. Consultare le informazioni relative alla SecureNet Key per istruzioni sulla selezione e l'installazione di un codice chiave.

Note:

a. Questo campo non è utilizzato per la scheda SecurID.

b. Occorre creare una chiave casuale univoca per ogni utente.

c. Quando si installa la chiave nella scheda SecureNet Key, utilizzare la procedura di installazione AssureNet Pathways e selezionare **Modo 5**.

Per ulteriori informazioni, consultare la sezione “Metodi di autenticazione” a pagina 85 .

Metodi di autenticazione utente

Le scelte per l'autenticazione utente sono:

Negare tutto Viene negato l'accesso all'utente.

Consentire tutto Non è necessaria alcuna autenticazione.

Parola d'ordine per l'accesso a NT

Parola d'ordine per l'accesso a NT è un metodo di autenticazione meno sicuro di Parola d'ordine firewall. Tuttavia, se gli utenti sono già definiti in un dominio Windows NT, è possibile utilizzare la parola d'ordine per l'accesso a Windows NT in modo da non dover utilizzare più parole d'ordine.

Se viene scelto questo metodo di autenticazione, l'ID utente e la parola d'ordine vengono convalidate in base al database degli utenti Windows NT locali. Se il firewall è configurato in modo da stabilire relazioni sicure con altri server Windows NT, questi server sicuri vengono ricercati per le definizioni utente.

Prima di poter impostare relazioni sicure tra il firewall di Windows NT ed i server sicuri di Windows NT, è necessario impostare un collegamento, in modo da consentire il traffico delle comunicazioni TCP/IP tra due macchine.

Impostare il collegamento mediante i servizi predefiniti di seguito riportati:

1. Domain Controller Authentication - che consente l'uso di Domain Controller per l'autenticazione dell'utente
2. NetBT Name Services broadcasts - che consente trasmissioni broadcast NetBIOS su servizi per nomi TCP/IP

Programmi di utilità per la configurazione di Windows NT per definire relazioni sicure.

SecureNet Key L'autenticazione viene eseguita utilizzando SecureNet Key della AssureNet Pathways.

Nel campo SecureNet Key, immettere il codice chiave con il quale viene altresì attivata la scheda SecureNet Key.

Note:

1. Occorre creare una chiave casuale univoca per ogni utente.
2. La chiave casuale deve avere un valore compreso tra 1 e 377 per ogni 8 valori ottali
3. Quando si installa la chiave nella scheda SecureNet Key, utilizzare la procedura di installazione AssureNet Pathways e selezionare **Modo 5**.

Per ulteriori informazioni, consultare la sezione “Metodi di autenticazione” a pagina 85.

Scheda SecurID L'autenticazione viene eseguita utilizzando una scheda di sicurezza SecurID della Security Dynamics oppure una scheda pinpad. *Non* utilizzare il campo SecureNet Key. Prima di utilizzare questo metodo di autenticazione con IBM Firewall occorre impostare il PIN.

Per FTP, non sono supportati i modi SDI Nuovo PIN e Token successivo.

Per ulteriori informazioni, consultare la sezione “Metodi di autenticazione” a pagina 85 .

Autenticazione 1,2 e 3 fornita dall'utente
L'autenticazione è fornita dall'utente. È possibile installare sul firewall un massimo di tre metodi di autenticazione forniti dall'utente. Per informazioni su come creare e compilare una subroutine per l'autenticazione fornita dall'utente, consultare *IBM eNetwork Firewall - Manuale di riferimento*.

Parola d'ordine firewall
All'utente viene richiesta l'immissione di una parola d'ordine valida. Quando questo pannello è completo, IBM Firewall richiede di specificare una parola d'ordine per questo nuovo utente.

La parola d'ordine del firewall consente di utilizzare più parole d'ordine sicure e regole di parole d'ordine rispetto alla parola d'ordine per l'accesso a Windows NT, per cui rappresenta la scelta consigliata per le parole d'ordine.

Richiedere modifica Fare clic su Sì o su No per indicare se all'utente viene richiesto di modificare le parole d'ordine dopo che sono state autenticate.

Bloccare parola d'ordine Fare clic su Sì o su No per indicare se la parola d'ordine è bloccata. Sì indica che il numero massimo di tentativi di login è stato superato e che la parola d'ordine non è stata utilizzata per il numero di settimane specificato da Numero massimo di settimane prima del blocco.

Il responsabile può impostare questo campo su Sì per impedire che un utente utilizzi l'autenticazione relativa alla parola d'ordine.

Note:

1. Le parole d'ordine sono sensibili al maiuscolo/minuscolo. Se viene immessa una parola d'ordine in lettere maiuscole e minuscole, l'utente deve immettere la parola d'ordine in maniera identica. Se esistono stazioni di lavoro che funzionano solo con lettere maiuscole, immettere le parole d'ordine per i relativi utenti in lettere maiuscole.
2. Il sistema operativo consente di definire le regole relative alle parole d'ordine. Tali regole vengono applicate quando un utente modifica la propria parola d'ordine ma non quando le modifiche vengono apportate da un responsabile. Le regole relative alle parole d'ordine sono:

Numero di giorni prima della scadenza (giorni)
Numero di giorni prima della scadenza di una parola d'ordine in cui il firewall consente all'utente di modificare la parola d'ordine.

Numero massimo di settimane prima della scadenza
Numero di settimane prima che all'utente venga richiesto di modificare la parola d'ordine.

Numero massimo di settimane prima del blocco
Numero di settimane in cui la parola d'ordine non viene utilizzata prima di essere bloccata.

Numero massimo consentito di tentativi di login
Numero massimo di tentativi di login prima del blocco della parola d'ordine.

Parole d'ordine prima del riutilizzo Numero di parole d'ordine memorizzate nell'elenco cronologico delle parole d'ordine. La parola d'ordine non può essere sostituita da nessuna parola d'ordine attualmente presente nell'elenco cronologico. Questo parametro è valido solo se il valore di Numero di settimane prima del riutilizzo della parola d'ordine è uguale a zero.

Numero di settimane prima del riutilizzo della parola d'ordine Numero di settimane in cui le parole d'ordine vengono conservate nell'elenco cronologico delle parole d'ordine. La parola d'ordine non può essere sostituita da nessuna parola d'ordine attualmente presente nell'elenco cronologico.

Lunghezza minima Numero minimo di caratteri in una parola d'ordine.

Numero minimo di caratteri alfabetici Numero minimo di caratteri alfabetici in una parola d'ordine.

Numero minimo di altri caratteri Numero minimo di caratteri non alfabetici in una parola d'ordine.

Numero massimo di caratteri ripetuti Numero massimo di volte in cui un singolo carattere può essere ripetuto in una parola d'ordine.

Numero minimo di caratteri diversi Numero minimo di caratteri diversi nella parola d'ordine.

Fare clic sulla scheda **Parola d'ordine firewall** per personalizzare questi valori in base a ciascun utente, come illustrato nella Figura 24 a pagina 84.

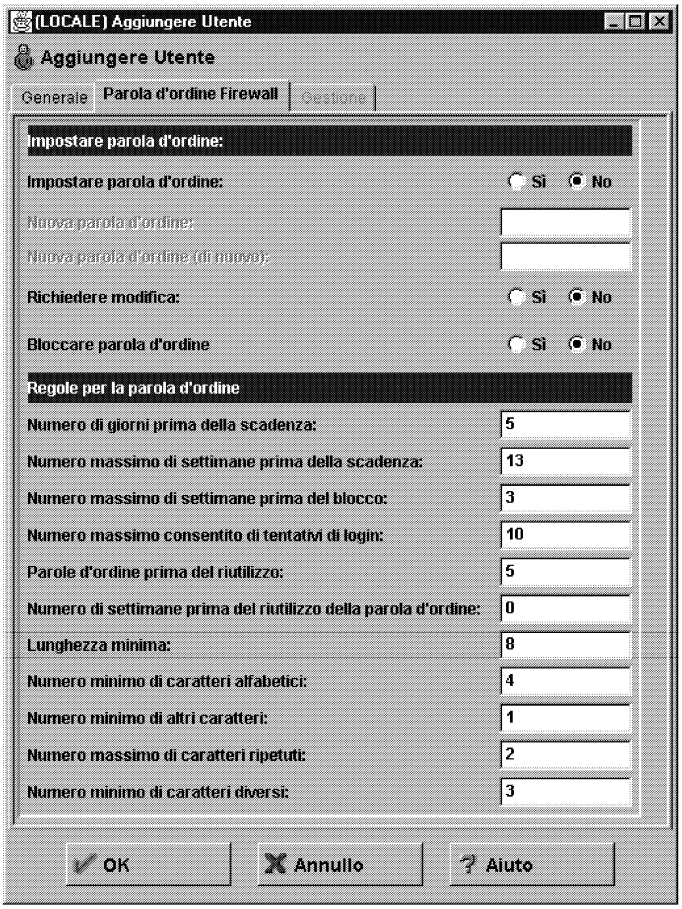

Figura 24. Scheda Parola d'ordine firewall

Modifica dell'accesso di un utente

Dopo aver aggiunto un utente al firewall, è possibile modificare gli attributi di sicurezza relativi all'utente dalla casella di dialogo **Modificare Utente**.

1. Selezionare l'utente di cui si desidera modificare gli attributi dalla casella di dialogo **Utenti** e fare clic su **Aprire**.
2. Quando viene visualizzata la casella di dialogo **Modificare Utente**, modificare i campi appropriati. Consultare la sezione “Aggiunta di un utente a IBM Firewall” a pagina 75 per un elenco degli attributi utente che è possibile modificare.
3. Una volta eseguite le modifiche, fare clic su **OK**.

Eliminazione di un utente da IBM Firewall

Nota: Non eliminare gli utenti `fwdfuser` o `fwdfadm`.

Per eliminare un utente, fare clic su **Eliminare** dal pannello **Elenco Utenti**.

Livello di autorizzazione del responsabile per funzione

Solo il *responsabile principale del firewall* può creare e modificare i responsabili e determinare su quali funzioni firewall avranno le autorizzazioni. Ad esempio, è possibile limitare l'autorizzazione per uno specifico responsabile alle sole funzioni Utenti e Controllo log.

Nelle casella di dialogo **Aggiungere Utente**, selezionare Responsabile firewall per il campo **Livello autorizzazione**. Per ulteriori dettagli sulle opzioni della casella di dialogo **Aggiungere Utente**, consultare la sezione “Aggiunta di un utente a IBM Firewall” a pagina 75.

Quindi, selezionare la scheda **Gestione** nella parte superiore della casella di dialogo **Aggiungere Utente**. Selezionare le funzioni che il responsabile è autorizzato ad utilizzare.

Metodi di autenticazione

Di seguito vengono riportati i vari metodi di autenticazione utente.

Negare tutto

IBM Firewall impedisce l'accesso al server.

Consentire tutto

Non è richiesta alcuna autenticazione. Il server non tenta di autenticare l'utente ma visualizza il prompt dei comandi in modo da consentire l'accesso all'host esterno.

Parola d'ordine firewall

Prima di concedere all'utente di procedere, il server richiede l'immissione della parola d'ordine del firewall (che non verrà visualizzata).

```
Parola d'ordine:
```

Immettere la parola d'ordine del firewall. È la stessa parola d'ordine con cui il nome utente è stato aggiunto al firewall.

Scheda SecurID

Utilizzare questo metodo se si possiede una scheda SecurID e la rete utilizza Security Dynamics ACE/Server.

Prima di concedere all'utente di procedere, il server richiede l'immissione di un CODICE DI ACCESSO (che non verrà visualizzato).

```
Immettere il CODICE DI ACCESSO:
```

A questo punto, immettere il codice PIN SecurID a quattro cifre seguito da una virgola e quindi il codice della scheda SecurID. Ad esempio, per collegarsi come utente NUOVOUTENTE con un PIN assegnato di 1234 e con un codice di SecurID di 179091, immettere:

```
login: NUOVOUTENTE
Immettere il CODICE DI ACCESSO: 1234,179091
```

Se gli utenti utilizzano FTP, l'autenticazione Scheda SecurID non viene eseguita correttamente, in quanto FTP non dispone dell'opzione per modificare la parola d'ordine. La prima che tentano di eseguire l'autenticazione Scheda SecurID, gli utenti devono utilizzare telnet, mediante cui viene creato un PIN. Gli utenti possono utilizzare quel PIN per le successive autenticazioni, ad esempio FTP, HTTP e così via.

Se la scheda SecurID è nel modo nuovo PIN, occorre impostare il PIN prima si utilizzare questo metodo di autenticazione con IBM Firewall.

SecureNet Key

Utilizzare questo metodo se si possiede una scheda SecureNet Key della Assurenet Pathways. Quando viene inizializzata la scheda SNK, utilizzare quanto segue:

- Formato di visualizzazione (esadecimale)
- Funzione di cancellazione (attiva o disattiva)
- Funzione di riconoscimento a singola cifra (disattiva)

Prima di concedere all'utente di procedere, Il server proxy richiede una risposta fornita dalla scheda SecureNet Key.

```
Utilizzare SNK per il riconoscimento
######## per l'utente id_utente
Ed:
```

Il riconoscimento `########` è un numero a 8 cifre immesso dall'utente nella scheda SecureNet Key.

1. Quando si riceve questo prompt, attivare la scheda SecureNet Key ed immettere il proprio codice PIN. Il codice PIN viene fornito insieme alla scheda.
2. Immettere il riconoscimento nel modo in cui è fornito dal server.

   Ad esempio: si esegue il login al server; il server visualizza il prompt:

   ```
   Utilizzare SNK per il riconoscimento
      78987648 per l'utente NUOVOUTENTE
   Ed:
   ```

   Immettere il valore 78987648 nella scheda SecureNet Key. La scheda visualizza la risposta che l'utente fornisce al server proxy.
3. Immettere questa risposta sul server.

   Se la scheda SecureNet Key ha visualizzato `8AE222A9` in risposta al riconoscimento dell'utente, immettere `8AE222A9` sul server:

   ```
   collegamento: NUOVOUTENTE
      Utilizzare SNK per il riconoscimento 78987648 per l'utente NUOVOUTENTE
   Ed:8AE222A9
   ```

SecurNetKey (SNK) è stato ridenominato Defender Handheld Token** (DHT) dalla AXENT** Technologies.

Accesso NT

Se viene scelto questo metodo di autenticazione, l'ID utente e la parola d'ordine vengono convalidate in base al database degli utenti Windows NT locali. Se il firewall è configurato in modo da stabilire relazioni sicure con altri server Windows NT, questi server sicuri vengono ricercati per le definizioni utente.

Metodo di autenticazione 1, 2 e 3 fornito dall'utente

È possibile utilizzare il metodo di autenticazione fornito dall'utente per FTP e telnet. Per ulteriori informazioni, consultare *IBM eNetwork Firewall - Manuale di riferimento*.

Capitolo 13. Configurazione dei server proxy

Questo capitolo contiene informazioni generiche sulle modalità di utilizzo e di configurazione dei server proxy da stazioni di lavoro interne o esterne alla rete sicura.

Proxy HTTP

proxy HTTP gestisce in modo efficiente le richieste del browser tramite IBM Firewall permettendo così di fare a meno di un server socks per l'esecuzione del browsing di rete. Gli utenti possono accedere ad informazioni utili su Internet senza compromettere la sicurezza delle loro reti interne e senza modificare il loro ambiente client per implementare il proxy HTTP.

Il proxy HTTP non è un server. L'utente finale non può scaricare file dal proxy oppure inserire file nel proxy. Inoltre, il proxy HTTP non è un proxy di cache. Nulla viene memorizzato sul firewall ad una richiesta HTTP.

Sessioni permanenti

I collegamenti permanenti consentono ad un client e ad un server di segnalare la chiusura di un collegamento TCP. Questa segnalazione utilizza un campo con l'intestazione del collegamento.

Il proxy di IBM Firewall supporta i collegamenti permanenti tra un client ed il proxy. I campi *Numero massimo di richieste permanenti* e *Timeout di collegamento permanente* controllano la durata del collegamento. Se viene raggiunto il valore indicato in uno di questi campi, il collegamento socket tra il proxy ed il client viene chiuso. Se i valori indicati nei campi *Numero massimo di richieste permanenti* e *Timeout di collegamento permanente* non vengono raggiunti, il collegamento resta aperto e sarà compito del client determinare quando una richiesta è completa.

Se il client determina in maniera errata quando una richiesta è completa, viene visualizzato un pannello in cui viene indicata la presenza di traffico sul collegamento anche se tale traffico è inesistente. Un esempio è rappresentato da un'icona animata di un browser in continua esecuzione anche se tutta la pagina è stata caricata. Fare clic su **Arrestare** per arrestare il movimento dell'icona. Per ulteriori informazioni su questi parametri, fare riferimento a “Numero massimo di richieste permanenti” a pagina 91 ed a “Timeout di collegamento permanente” a pagina 92.

Configurazione del proxy HTTP utilizzando il client di configurazione

Per configurare il proxy HTTP, attenersi alla seguente procedura:

1. Per un corretto funzionamento del proxy HTTP, occorre consentire le interrogazioni DNS. È possibile farlo in modo semplice accedendo alla casella di dialogo Politica di Sicurezza dalla cartella Gestione del Sistema nell'albero di navigazione del client di configurazione e facendo clic su Consentire interrogazioni DNS.
2. Attivare i filtri

3. Aggiungere un collegamento. Per un esempio di come impostare un collegamento sul lato non sicuro della rete, consultare la sezione “Esempio di un proxy HTTP” a pagina 55.
4. Per configurare il proxy HTTP, selezionare HTTP dall'albero di navigazione del client di configurazione. IBM Firewall visualizza la casella di dialogo **Configurazione proxy HTTP**, come illustrato nella Figura 25.

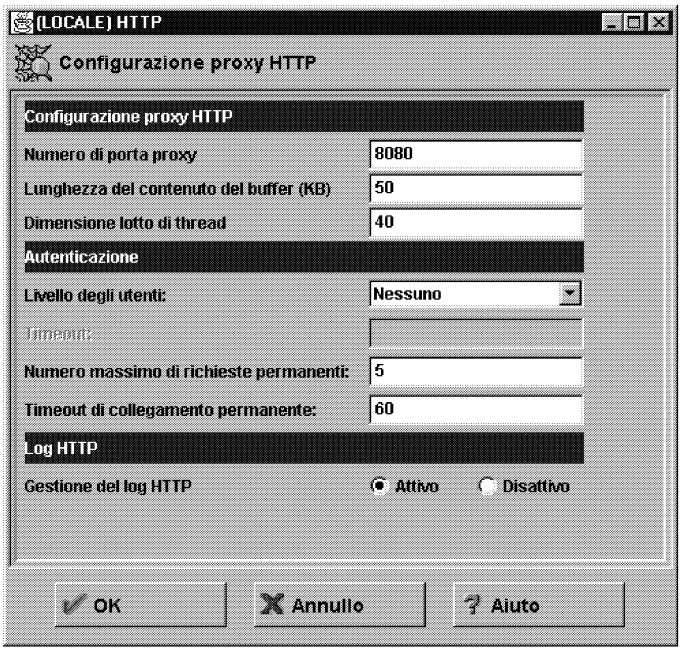

Figura 25. HTTP

5. Per arrestare il proxy, selezionare `Risorse del computer/Pannello di controllo/Servizi`. Scegliere il Proxy HTTP di IBM Firewall e fare clic su *Ferma*.

   L'eseguibile phttpd è un servizio di sistema che viene avviato automaticamente all'avvio del sistema.

Configurare i parametri nella casella di dialogo **Configurazione Proxy HTTP**. Se questi parametri vengono modificati, il servizio proxy HTTP IBM Firewall viene arrestato e riavviato. Le richieste degli utenti del proxy attivo vengono interrotte fino a quando il proxy non viene riavviato (dopo pochi secondi).

Numero di porta proxy

Utilizzare questo parametro per specificare il numero di porta su cui il proxy ascolterà le richieste. Se si modifica il numero di porta, occorre configurare i filtri in modo da consentire o meno il flusso attraverso le porte. I numeri di porta inferiori a 1024 sono riservati alle applicazioni TCP/IP. Le porte comuni utilizzate per i server di rete proxy sono 8080 e 8088.

Le regole di filtro assunte sono impostate per disabilitare il traffico in arrivo e non sicuro sulla porta 8080, permettendo però il traffico sicuro sulla stessa porta. Il proxy rifiuta solo le richieste del proxy non sicuro. Il valore assunto è `8080`. Se si modifica questo valore, il numero di porta deve essere modificato anche nei servizi impostati per questa configurazione. Se si modificano queste impostazioni, occorre riavviare il processo phttpd.

Lunghezza del contenuto del buffer
Utilizzare questo parametro per impostare la dimensione del buffer per i dati dinamici generati da un server. I dati dinamici sono l'emissione dei programmi CGI, del server e dei programmi API. Sono dati che non provengono da un proxy.

Specificare il valore in kilobyte (K). Il valore assunto è `50K`.

Dimensione lotto di thread
Utilizzare questo parametro per impostare il numero fisso di thread che si desidera siano attivi simultaneamente. Il proxy congela le nuove richieste fino a quando non viene terminata la richiesta in corso e non vengono resi disponibili nuovi thread. Di norma, quanto più è potente una macchina, tanto più alto è il valore da utilizzare per questo parametro. Se una macchina comincia ad impiegare troppo tempo in attività di sistema, quali lo swap della memoria, provare a ridurre questo valore. Specificare un numero intero, ad esempio 60. Il valore assunto è `200`.

Livello degli utenti
Questo parametro indica al proxy il livello degli utenti da autenticare. Specificare il valore all, new o none. Il valore assunto è none. I valori sono:

all A tutti i browser viene inviata la risposta di autenticazione del proxy per indicare che il browser deve richiedere all'utente un ID utente ed una parola d'ordine. Se il browser non supporta la risposta di autenticazione del proxy, viene visualizzata una pagina di errore. Se il browser supporta tale risposta, vengono visualizzati i prompt dell'ID utente e della parola d'ordine.

new Viene utilizzato come un aiuto per la migrazione. Viene inviata solo la risposta di autenticazione del proxy 407, che indica al browser di eseguire un prompt idutente/parola d'ordine, ad un browser del client che viene identificato come un browser HTTP/1.1. È possibile impostare Internet Explorer 4.0 in modo che venga eseguita una trasmissione di tipo broadcast delle richieste con l'identificativo HTTP/1.1. Netscape ed altri programmi vengono identificati come richieste HTTP/1.0.

none Le richieste del browser non vengono controllate. Non viene richiesto alcun idutente/parola d'ordine.

Timeout
Questo parametro indica al proxy il periodo di tempo che è necessario attendere per una richiesta del client prima di richiedere all'utente una nuova autenticazione. Un utente viene autenticato da un indirizzo IP e da un ID utente specifici forniti al momento della prima autenticazione per il periodo di tempo in cui resta inattivo. Specificare il tempo in minuti. Il valore assunto è 60 minuti.

Finché il browser viene utilizzato attivamente, la finestra non è sottoposta a scadenza.

Numero massimo di richieste permanenti
Questo parametro indica il numero massimo di richieste che un proxy può ricevere su un collegamento HTTP/1.1 permanente. Si tratta di un tool che influisce direttamente sul timeout dell'autenticazione. Durante una sessione permanente, non viene eseguita alcuna verifica dell'autenticazione di un utente fino al termine della sessione permanente. Specificare il valore con un numero intero, ad esempio 25. Il valore assunto è 5.

Timeout di collegamento permanente

Questo parametro indica il tempo in secondi in cui viene mantenuto un collegamento HTTP/1.1 permanente con il browser di un client, una volta che un browser HTTP/1.1 avvia una sessione con il proxy. Si tratta di un tool che influisce direttamente sul timeout dell'autenticazione. Durante una sessione permanente, non viene eseguita alcuna verifica dell'autenticazione di un utente fino al termine della sessione permanente. Specificare il tempo in secondi. Il valore assunto è 60 minuti.

Gestione dei log HTTP

Questo parametro indica al proxy di registrare l'avvio/chiusura e tutte le richieste proxy nel log del firewall. Viene utilizzato il livello di log LOG_NOTICE. Impostare questo parametro come attivo se si desidera controllare l'attività di richiesta di HTTP. Il log degli eventi viene eseguito con la funzione `log firewall`.

Configurazione del browser

Il browser del client deve essere configurato in modo che venga collegato alla porta su cui il proxy HTTP è in ascolto.

Se si utilizza HTTPS, indicare il proxy HTTP in IBM Firewall anche per il proxy di sicurezza.

Se si desidera indicare il browser Internet Explorer come browser HTTP/1.1 al proxy, attenersi alla seguente procedura:

- Aprire il menu sviluppo azione *Visualizza*.
- Selezionare *Opzioni...*.
- Selezionare la scheda *Avanzate*.
- Scorrere fino alle impostazioni HTTP 1.1 ed attivarle.

Collegamenti SSL

È supportata la funzione di tunnel SSL per il collegamento sicuro HTTP ad altri server. IBM Firewall in questo caso funziona come un gateway. Il tunnel va dal client al server passando per il firewall. Utilizzare la porta standard 443 per il collegamento sicuro HTTP come indicato nel seguente esempio:

```
https://www.ibm.com:443
```

Utilizzare, inoltre, il servizio predefinito `HTTPS proxy out 2/2`.

Se si utilizza HTTPS, indicare il proxy HTTP in IBM Firewall anche per il proxy di sicurezza.

Per ulteriori informazioni, consultare la sezione “Esempio di un proxy HTTP” a pagina 55.

Metodi supportati

Il proxy HTTP supporta i seguenti metodi, che rappresentano modi diversi di consultare Internet:

- FTP
- Gopher
- HTTP

- HTTPS
- WAIS

Emissione di log di esempio relativa al proxy HTTP

Di seguito viene riportato un esempio dell'emissione di log relativa alle richieste get autenticate del proxy HTTP.

```
Mar 06 14:04:50 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication UNSUCCESSFUL
for user <Unknown>, on 9.67.140.162, thru secure network ... RC:30.
Mar 06 14:04:50 1998 fire3: ICA2099i: httpd --> Status: 407 from client
9.67.140.162, who requested "GET http://9.67.128.69/ HTTP/1.1" for 0 bytes.
Mar 06 14:05:05 1998 fire3: ICA2024i: User fred successfully authenticated
using NT authentication from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2169i: User fred successfully authenticated
for HTTP Server using NT from secure network:9.67.140.162.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:05 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/HTTP/1.1" for 2693 bytes.
Mar 06 14:05:05 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user (fred), on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:06 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgsplash.gif HTTP/1.1"
for 211 bytes.
Mar 06 14:05:10 1998 fire3: ICA2140i: httpd --> HTTP Proxy authentication
SUCCESSFUL for user fred, on 9.67.140.162, thru secure network ...RC:1.
Mar 06 14:05:10 1998 fire3: ICA2099i: httpd --> Status: 200 from client
9.67.140.162, who requested "GET http://9.67.128.69/Admin/lgmast.gif HTTP/1.1"
for 211 bytes.
```

L'attività di log può essere spiegata nel seguente modo:

- ICA2099i - visualizza il codice di errore 407 ed indica che l'autenticazione non è riuscita per la richiesta get indicata.

  Il browser quindi richiede all'utente delle autenticazioni. Il browser richiede un ID utente ed una parola d'ordine.

- ICA2140i - l'autenticazione è stata eseguita correttamente per l'utente (fred).

L'autenticazione è stata eseguita su ogni richiesta get per ciascun elemento della pagina Web.

FTP

1. Utilizzare il proxy FTP per accedere all'host del firewall. Come nome host per il firewall viene qui utilizzato `ftp_gw.domain.net.com`.

   ```
   ftp ftp_gw.domain.net.com
   ```

   Il server proxy richiederà il nome utente:

   ```
   login:
   ```

2. Immettere il nome utente autorizzato ad utilizzare il firewall:

   ```
   login: jane_doe
   ```

Il server convalida l'identità dell'utente in base allo schema di autenticazione selezionato quando il nome utente è stato aggiunto al firewall (consultare la sezione “Aggiunta di un utente a IBM Firewall” a pagina 75). Per informazioni sul

modo in cui gli utenti sono autenticati dai server proxy, consultare la sezione “Metodi di autenticazione” a pagina 85.

Dopo avere autenticato l'utente, il server proxy visualizza un prompt di comandi FTP.

```
ftp>
```

Utilizzare i comandi FTP `quote` e `site` per stabilire il collegamento con l'host esterno:

```
ftp> quote site forhost.network.outside.com
```

L'host esterno, prima di stabilire il collegamento, richiede l'immissione di un nome utente e di una parola d'ordine. Si tratta quasi certamente di un nome utente e di una parola d'ordine diversi da quelli utilizzati per eseguire FTP sul firewall.

Il valore di timeout assunto per il login è 60 secondi e per il proxy inattivo 7200 secondi. Per modificare i valori di timeout assunti, consultare “Sostituzione dei valori di timeout nei proxy FTP e Telnet” a pagina 96.

FTP trasparente

È possibile eseguire l'ftp in modo trasparente attraverso il firewall. I proxy trasparenti non richiedono alcuna autenticazione firewall e pertanto i relativi utenti non devono essere definiti come utenti proxy del firewall. I proxy trasparenti sono consentiti solo andando dal lato sicuro del firewall a quello non sicuro. Per rendere funzionante il proxy trasparente, occorre selezionarlo nel pannello del client di configurazione Politica di sicurezza.

1. Utilizzare ftp per accedere all'host del firewall. Come nome host per il firewall viene qui utilizzato `ftp_gw.domain.net.com`.

   ```
   ftp ftp_gw.domain.net.com
   ```

2. Il server proxy richiederà il nome utente:

   ```
   USER:
   ```

3. Immettere il nome utente sulla rete non sicura:

   ```
   USER: nomeutente@nome_host_sito_remoto
   ```

4. L'host di destinazione richiede quindi la parola d'ordine del `nomeutente` immesso al passo precedente.

   ```
   parola d'ordine:
   ```

5. Immettere la parola d'ordine.

Il valore di timeout assunto per il login è 60 secondi e per il proxy inattivo 7200 secondi (due ore). Per modificare i valori di timeout assunti, consultare “Sostituzione dei valori di timeout nei proxy FTP e Telnet” a pagina 96.

Telnet

Utilizzare il proxy telnet per eseguire il login al server proxy del firewall. È possibile utilizzare il nome host oppure l'indirizzo Internet. Dopo l'autenticazione delle credenziali, è possibile utilizzare il comando telnet sul firewall per eseguire il login all'host desiderato. Ad esempio, utilizzare il telnet dalla rete sicura, attraverso il firewall con il nome host `telnet_gw`, per accedere alla propria destinazione finale, `forhost.network.outside.com`.

1. Per avviare il processo, utilizzare il telnet per accedere all'host del firewall. Come nome host per il firewall viene qui utilizzato telnet_gw.domain.net.com.

   ```
   telnet telnet_gw.domain.net.com
   ```

2. Il server proxy richiederà il nome utente:

   ```
   login:
   ```

3. Immettere il nome utente autorizzato ad utilizzare il firewall:

   ```
   login: jane_doe
   ```

Il server convalida l'identità dell'utente in base allo schema di autenticazione selezionato quando il nome utente è stato aggiunto al firewall (consultare la sezione “Aggiunta di un utente a IBM Firewall” a pagina 75). Per informazioni sul modo in cui gli utenti sono autenticati dai server proxy, consultare la sezione “Metodi di autenticazione” a pagina 85.

Viene utilizzata una shell che esegue una singola azione. Con il daemon telnet proxy di IBM Firewall, tutte le comunicazioni passano attraverso il firewall.

Se si utilizza la shell che esegue una singola azione, dopo l'autenticazione, il server proxy visualizza:

```
IMMETTERE L'HOST DESIDERATO:
```

Tipo

```
telnet forhost.network.outside.com
```

l'host esterno richiede l'immissione del nome utente e della parola d'ordine con cui si è noti a tale host. È possibile che il nome utente e la parola d'ordine siano diversi dal nome utente e dalla parola d'ordine utilizzati sul server proxy del firewall.

Il valore di timeout assunto per il login è 60 secondi e per il proxy inattivo 7200 secondi. Per modificare i valori di timeout assunti, consultare “Sostituzione dei valori di timeout nei proxy FTP e Telnet” a pagina 96.

Telnet trasparente

È possibile eseguire il telnet in modo trasparente attraverso il firewall. I proxy trasparenti non richiedono alcuna autenticazione firewall e pertanto i relativi utenti non devono essere definiti come utenti proxy del firewall. I proxy trasparenti sono consentiti solo andando dal lato sicuro del firewall a quello non sicuro. Per rendere funzionante il proxy trasparente, occorre selezionarlo nel pannello del client di configurazione Politica di sicurezza.

1. Utilizzare telnet per accedere all'host del firewall. Come nome host viene qui utilizzato `ftp_gw.domain.net.com`.

```
telnet telnet_gw.domain.net.com
```

2. Il server proxy richiederà il nome utente:

   ```
   Login:
   ```

3. Immettere il nome utente sulla rete non sicura:

   ```
   Login@host_remoto
   ```

L'host esterno richiede l'immissione del nome utente e della parola d'ordine con cui si è noti a tale host. È possibile che il nome utente e la parola d'ordine siano diversi dal nome utente e dalla parola d'ordine utilizzati sul server proxy del firewall.

Il valore di timeout assunto per il login è 60 secondi e per il proxy inattivo 7200 secondi. Per modificare i valori di timeout assunti, consultare “Sostituzione dei valori di timeout nei proxy FTP e Telnet”.

Sostituzione dei valori di timeout nei proxy FTP e Telnet

FTP e Telnet presentano dei valori di timeout per il login ed i tempi di attesa in cui sono inattivi. Per valore assunto, durante il login e l'autenticazione dell'utente deve verificarsi un'attività di sessione almeno una volta ogni 60 secondi. Questo parametro è noto come loginTimeout.

Una volta che il login è stato completato, deve verificarsi un'attività di sessione almeno una volta ogni 7200 secondi o la sessione viene scollegata.

È possibile sostituire questi valori assunti creando un file `fwTimeout.cfg` nell'indirizzario `ROOTDIR\config` e specificando nuovi valori di timeout in secondi. Il file `fwTimeout.cfg` deve avere il seguente formato:

```
telnet
proxyTimeout=7200
loginTimeout=60

   ftp
proxyTimeout=7200
loginTimeout=60
```

Capitolo 14. Controllo dei log del firewall

Questo capitolo descrive come controllare la funzione dei log di avviso in tempo reale. Quando viene violata una delle soglie configurate, viene generato un avviso.

IBM Firewall controlla i messaggi inviati al log del firewall per rilevare potenziali situazioni critiche basandosi sulle soglie definite dall'utente. Se una di queste soglie viene violata, il firewall invia un avviso attenendosi alle modalità specificate dal responsabile del firewall.

Definizioni delle soglie

Una soglia è composta da un parametro di conteggio e uno di tempo: se il conteggio (numero di eventi specifici) supera il valore specificato entro il tempo stabilito (minuti), la soglia viene considerata violata e viene generato un messaggio di avviso. Il controllo dei log riconosce quattro tipi di soglie:

1. Numero totale di errori di autenticazione
2. Errori di autenticazione per uno specifico ID utente
3. Errori di autenticazione da uno specifico host
4. Ricorrenze di una tag di messaggio nel log

È possibile configurare tutte le soglie utilizzando il client di configurazione oppure l'interfaccia della riga comandi. Le modifiche apportate alle definizioni di soglia sono automaticamente rilevate da IBM Firewall.

Messaggi di avviso

Quando viene raggiunta una soglia, IBM Firewall genera un messaggio di avviso. L'emissione di un messaggio di avviso può assumere una delle quattro forme seguenti:

1. Entrata in un file di log:
   - Tramite la funzione `log avvisi`, configurabile servendosi del client di configurazione o della riga comandi.
   - In `log firewall`
2. Messaggio postale per un elenco di utenti tramite safemail
3. Cercapersone, come da configurazione. Consultare la sezione “Supporto di notifica tramite cercapersone” a pagina 99.
4. Esecuzione di un comando definito dall'utente, con il messaggio di avviso come primo parametro

Il messaggio di avviso contiene informazioni relative ad una specifica violazione di soglia. Ad esempio:

```
ICA0001e: AVVISO – 20 errori di autenticazione.
ICA0002e: AVVISO – 10 errori di autenticazione per l'utente root.
ICA0003e: AVVISO – 15 errori di autenticazione dall'host 56.67.78.89
ICA0004e: AVVISO – Tag ICA1234e con tre entrate di log.
```

I messaggi di avviso e gli altri messaggi originati dal controllo dei log non vengono controllati.

Configurazione del controllo dei log utilizzando il client di configurazione

Questa sezione descrive come utilizzare il client di configurazione per configurare il controllo dei log in tempo reale. Selezionare Log di Sistema dall'albero di navigazione del client di configurazione. Fare doppio clic sull'icona della cartella di file per espandere la vista. Fare clic su **Soglie per il controllo log**.

Dalla casella di dialogo **Gestione delle Soglie per il Controllo Log**, è possibile aggiungere, modificare o eliminare una definizione di soglia.

Aggiunta di un controllo dei log

Per aggiungere una definizione di soglia, selezionare **NUOVO** dalla casella di dialogo **Soglie per il Controllo Log** e fare clic su **Aprire**. Viene visualizzata la casella di dialogo **Aggiungere Controllo Log**. Completare i seguenti campi:

1. Fare clic sulla freccia **Tipo di classe** per scegliere un tipo di classe dal rispettivo elenco. I tipi di classe sono:
   - Notifica tramite posta
   - Comando eseguibile
   - Per soglia utente
   - Soglia tentativi autenticazione mancati totali
   - Per soglia host
   - Soglia messaggi
2. Se si seleziona il tipo di classe Notifica tramite posta, immettere un indirizzo di posta elettronica. È possibile definire più classi di notifica postale.

   Tutti i messaggi di violazione di soglia sono inviati all'indirizzo di posta elettronica specificato.
3. Se si seleziona il tipo di classe Comando eseguibile, immettere il nomefile del comando.

   Il programma di controllo dei log eseguirà questo comando con il messaggio di avviso come primo parametro. È possibile definire una sola classe di comando eseguibile.
4. Se si seleziona il tipo di classe Soglia messaggi, immettere una tag di messaggio, vale a dire una tag standard dei messaggi di log di IBM Firewall che si desidera controllare.
5. Se si seleziona una delle classi di soglia, compilare il campo relativo al conteggio di soglia.

   Il conteggio di soglia è il numero massimo di eventi non riusciti consentiti entro il periodo di tempo specificato.
6. Se si seleziona una delle classi di soglia, compilare il campo relativo al tempo di soglia.

   Il tempo di soglia è il numero di minuti a partire dalla prima ricorrenza di un evento.

7. Se si seleziona una delle classi di soglia, fare clic su Sì o su No per indicare se si desidera che venga attivata la notifica tramite cercapersone o meno.
8. L'immissione di un commento è facoltativa.
9. Fare clic su **OK**.

Modifica di una definizione di soglia

Per modificare una definizione di soglia, selezionare la voce da modificare dalla casella di dialogo **Gestione delle Soglie per il Controllo Log** e fare clic su **Aprire**. Viene visualizzata la casella di dialogo **Modificare Controllo Log**.

1. Immettere le modifiche desiderate per i campi relativi al conteggio di soglia ed al tempo di soglia.

   Il conteggio di soglia è il numero massimo di messaggi di autenticazione non riuscita da rilevare entro il periodo di tempo specificato. Il tempo di soglia è il numero di minuti a partire dalla prima ricorrenza di un messaggio.
2. Fare clic su **OK**.

Eliminazione di una definizione di soglia

Per eliminare una definizione di soglia, selezionare la voce da eliminare dalla casella di dialogo **Soglie per il Controllo Log** e fare clic su **Eliminare**. Viene richiesta la conferma dell'eliminazione. Fare clic su **Sì** per confermare. Eliminazione non significa eliminazione dal file di log. Significa solo eliminazione della definizione.

Supporto di notifica tramite cercapersone

Quando si verificano episodi di intrusione sul firewall, il firewall può avvisare un responsabile di sistema inviando un messaggio sul cercapersone. Per impostare il supporto di notifica tramite cercapersone, è necessario configurare i seguenti tre componenti del cercapersone.

1. Personalizzazione dei Comandi - Questo componente deve essere creato e modificato utilizzando il client di configurazione. Mediante questo componente vengono impostati i valori assunti relativi al comando del cercapersone, che viene utilizzato dal controllo del log e può essere utilizzato dalla riga comandi. Questo componente conterrà un'entrata univoca che definisce l'ambiente del cercapersone. Per ulteriori informazioni sulla definizione e la personalizzazione di questo componente, consultare la sezione “Personalizzazione comandi” a pagina 101.
2. Gestione della Portante - Occorre definire una portante idonea prima di collegare il modem. Questo componente contiene un elenco di portanti assunte utilizzate negli USA. Se la portante che si sta utilizzando non è una di queste, aggiungerla a questo componente. Per ulteriori informazioni, consultare la sezione “Gestione della portante” a pagina 102.

   Verificare i numeri di telefono esistenti relativi alle portanti prendendo tali numeri dalle portanti stesse. Quando si stabilisce una comunicazione con le portanti, accertarsi di ottenere il numero di telefono del modem della portante ed altre informazioni valide per il servizio utilizzato.
3. Gestione del Modem - Prima di collegare il modem, occorre creare delle definizioni di modem adatte. Queste definizioni devono contenere tutte le

informazioni principali sul modem che saranno utilizzate dal supporto di notifica tramite cercapersone. Questo componente contiene un elenco di modem da cui è possibile effettuare una scelta. È possibile aggiungere a questo elenco alcuni modem che potrebbero, tuttavia, essere incompatibili con il supporto della portante. Per ulteriori informazioni sulla gestione delle definizioni di modem, consultare la sezione “Gestione del modem” a pagina 103.

Nota: IBM Firewall supporta il protocollo per le comunicazioni TAP (Tele-AlphaNumeric Protocol) relativo al supporto di notifica tramite cercapersone.

Portanti e modem supportati

Il file di database delle portanti contiene un elenco delle portanti ed i parametri di trasmissione ad esse correlati. È possibile aggiungere altre portanti. Alcuni dei parametri, oltre al nome della portante ed al numero di telefono dei modem, sono:

- La lunghezza massima del messaggio per un cercapersone alfanumerico ed il numero massimo di cifre per un cercapersone numerico
- La velocità in baud, la parità e la lunghezza dei bit di dati e di stop

Prima di utilizzare una determinata portante, accertarsi che tale portante utilizzi il protocollo TAP.

Il codice del cercapersone presenta definizioni di modem assunte. Queste sono:

- IBM MOD 448 14400 bps
- IBM 5853 2400 bps
- IBM 7852 28800 bps
- IBM 7855 2400 bps
- Generic Hayes compatible
- US Robotics Courier 9600 bps
- Zoom V.34

Configurazione del supporto di notifica tramite cercapersone

L'opzione Impostazione cercapersone è utilizzata per configurare il file di personalizzazione dei comandi e per gestire le portanti ed i modem. Se si sta utilizzando un cercapersone, è necessario utilizzare l'opzione Impostazione cercapersone per personalizzare l'ambiente del cercapersone prima di utilizzare il controllo dei log.

Prima di iniziare, è necessario ottenere dalla portante i numeri di telefono del modem, l'ID del cercapersone e i parametri del modem.

Per configurare il supporto di notifica tramite cercapersone, selezionare Gestione del Sistema dall'albero di navigazione del client di configurazione. Fare doppio clic sull'icona della cartella di file per espandere la vista. Selezionare **Log di sistema**. Fare doppio clic sull'icona della cartella di file per espandere la vista. Selezionare **Impostazione cercapersone**.

Personalizzazione comandi

Quando si seleziona **Impostazione cercapersone**, è possibile selezionare una portante ed un modem da utilizzare e scrivere un messaggio per il cercapersone.

Impostazioni di personalizzazione comandi

Quando si seleziona **Impostazione cercapersone** dall'albero di navigazione, viene visualizzata la casella di dialogo **Impostazione cercapersone** con un pannello Impostazioni di Personalizzazione Comandi simile alla casella di dialogo illustrata nella Figura 26.

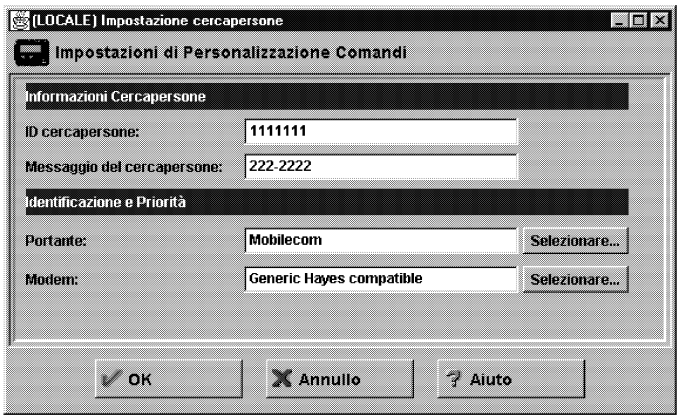

Figura 26. Impostazione cercapersone

Digitare o selezionare i valori da aggiungere nei campi di immissione.

1. Immettere l'ID del cercapersone. In genere di tratta di un PIN univoco assegnato al cercapersone dall'azienda della portante.
2. Immettere il messaggio per il cercapersone. Si tratta di una stringa contenente il messaggio assunto che l'utente desidera inviare. Per i cercapersone numerici, tale messaggio può essere solo un numero. Per i cercapersone alfanumerici, il messaggio può essere costituito da un testo. Non superare la lunghezza massima specificata nell'impostazione della portante, altrimenti il messaggio può risultare troncato. Non utilizzare i due punti (:). In caso contrario, verranno sostituiti da uno spazio vuoto.
3. Se non esiste alcun nome di portante, fare clic su **Selezionare** per definire una portante. Viene visualizzata la casella di dialogo **Gestione Portante Cercapersone**. Per i dettagli su come completare questo pannello, consultare la sezione “Gestione della portante” a pagina 102.
4. Se non esiste alcun nome di modem, fare clic su **Selezionare** per definire il modem. Viene visualizzata la casella di dialogo **Gestione Modem Cercapersone**. Per i dettagli su come completare questo pannello, consultare la sezione “Gestione del modem” a pagina 103.
5. Fare clic su **OK**.

Modifica della personalizzazione comandi

Quando si seleziona Impostazione cercapersone dall'albero di navigazione, viene visualizzata la casella di dialogo **Impostazione cercapersone** con il pannello Impostazioni di Personalizzazione Comandi.

1. Digitare o selezionare i valori nei campi di immissione per modificare i valori esistenti dei campi di immissione per la personalizzazione.
2. Fare clic su **OK**.

Eliminazione della personalizzazione comandi

1. È possibile eliminare un'entrata dalla casella di dialogo **Gestione Portante Cercapersone** o dalla casella di dialogo **Gestione Modem Cercapersone** selezionando una voce dall'elenco e facendo doppio clic su **Eliminare**.

   Viene richiesta la conferma dell'eliminazione.
2. Fare clic su **Sì** per confermare l'eliminazione o su **No** per ritornare alla casella di dialogo **Impostazione cercapersone**.

Se non esiste alcuna immissione di personalizzazione, il supporto di notifica del cercapersone non potrà inviare una chiamata.

Gestione della portante

Dalla casella di dialogo **Impostazione cercapersone**, andare sul campo relativo al nome della portante e fare clic su **Selezionare**. Viene visualizzata una casella di dialogo **Gestione Portante Cercapersone** simile a quella visualizzata nella Figura 27.

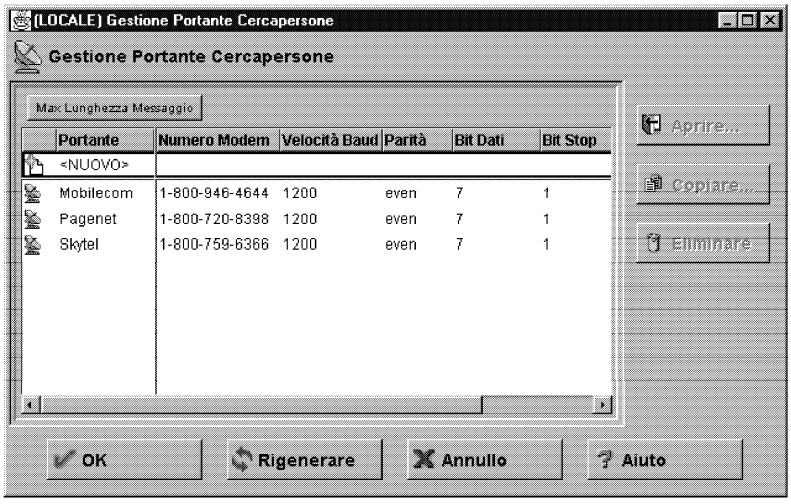

Figura 27. Gestione Portante Cercapersone

Aggiunta di una portante

Per aggiungere una nuova portante, selezionare **NUOVO** dalla casella di dialogo **Gestione Portante Cercapersone** e fare clic su **Aprire**. Digitare o selezionare i valori nei campi di immissione appropriati:

1. Immettere il nome della portante. Tale nome deve essere univoco e deve fornire informazioni sufficienti per poter riconoscere la portante.

2. Immettere il numero di telefono della portante, vale a dire il numero di telefono di un modem della società della portante, in opposizione al numero di paginazione della voce o al numero di altri servizi. Il numero di telefono del modem deve essere adeguato ad una copertura regionale o nazionale e ad un cercapersone numerico o alfabetico, come richiesto dall'unità e dal servizio di paginazione utilizzato.
3. Immettere TAP per il metodo di paginazione (unico valore consentito).
4. Immettere la parola d'ordine, se la portante consente o richiede una parola d'ordine.
5. Immettere la lunghezza massima del messaggio per un cercapersone alfanumerico ed il numero massimo di cifre per un cercapersone numerico.
6. Immettere la velocità in baud. Fare clic sulla freccia e scegliere un valore dall'elenco.
7. Fare clic su **Pari**, **Dispari** o **Nessuno** per il campo relativo alla parità.
8. Scegliere i bit di dati assunti (fare clic su **7** o su **8**).
9. Scegliere i bit di stop assunti (fare clic su **1** o su **2**).
10. Fare clic su **OK**.

Modifica della portante

1. Selezionare la portante che si desidera modificare dalla casella di dialogo **Gestione Portante Cercapersone** e fare clic su **Aprire**.
2. Per una spiegazione degli altri campi che è possibile modificare, consultare la sezione “Aggiunta di una portante” a pagina 102. Non è possibile modificare il nome della portante. Questo campo viene disabilitato.
3. Eseguire le modifiche desiderate.
4. Fare clic su **OK**.

Eliminazione di una portante

1. Selezionare la portante che si desidera eliminare dalla casella di dialogo **Gestione Portante Cercapersone** e fare clic su **Eliminare**.
2. Viene richiesta la conferma dell'eliminazione. Fare clic su **Sì** per confermare.

   Nota: Il database delle portanti deve sempre contenere almeno una portante. Se non è stata definita alcuna portante, il supporto di notifica tramite cercapersone non funzionerà.

Gestione del modem

Il manuale del modem contiene informazioni importanti relative all'inizializzazione. È necessario coordinare le impostazioni del modem con quelle della stampante. In generale, vengono supportati solo i modem Hayes compatibili, che utilizzano i comandi standard del modem.

Dalla casella di dialogo **Impostazione cercapersone**, andare al campo relativo al nome del modem e fare clic su **Selezionare**. Viene visualizzata una casella di dialogo **Gestione Modem Cercapersone** simile a quella visualizzata nella Figura 28 a pagina 104.

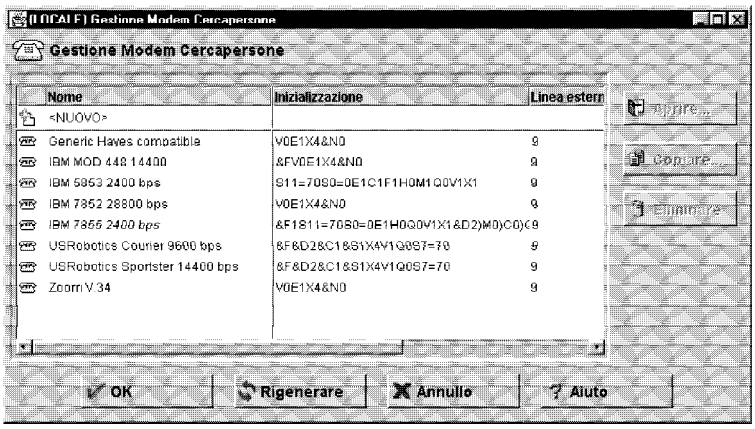

Figura 28. Gestione Modem Cercapersone

Utilizzando questa casella di dialogo, è possibile aggiungere, modificare o eliminare vari modem.

Aggiunta di un modem

Per aggiungere un file di definizione di un nuovo modem, selezionare **NUOVO** dalla casella di dialogo **Gestione Modem Cercapersone** e fare clic su **Aprire**. Nella casella di dialogo **Aggiungere Modem**, immettere o selezionare i valori nei campi di immissione.

1. Immettere il nome del modem. Tale nome deve essere univoco tra le altre definizioni e deve fornire informazioni sufficienti per poter riconoscere il modem.
2. Immettere il numero di porta COM che definisce la porta COM seriale a cui viene collegato il modem. Immettere un numero inferiore a 10. Mentre il modem deve avere una configurazione hardware adeguata a questa porta, la porta non deve essere definita su Windows NT, altrimenti l'accesso alla porta verrà negato alle funzioni del cercapersone. Se le impostazioni del modem non corrispondono a quelle dell'hardware, al codice del cercapersone, dopo numerosi tentativi, viene impedito l'accesso.
3. Immettere la stringa di inizializzazione, che definisce il modem come un modem di dati con eco su X level4 ed una velocità in baud fissa definita dal sito locale. Non includere il comando AT. La funzione del cercapersone inserisce tale comando all'inizio della stringa di inizializzazione.
4. Immettere il prefisso della linea esterna. Il prefisso è il numero che viene composto per collegarsi con l'esterno.
5. Fare clic su **OK**.

Modifica del modem

1. Selezionare il nome di un modem dalla casella di dialogo **Gestione Modem Cercapersone** e fare clic su **Aprire** per modificare il file di definizione del modem.

   Nella casella di dialogo **Modificare Modem**, viene visualizzato un elenco di campi che è possibile modificare relativi alla definizione del modem. Per una descrizione su questi campi, consultare la sezione “Aggiunta di un modem”.
2. Fare clic su **OK**.

Eliminazione di un modem

1. Selezionare il nome di un modem dalla casella di dialogo **Gestione Modem Cercapersone** e fare clic su **Eliminare** per eliminare un file di definizione del modem.
2. Viene richiesta la conferma dell'eliminazione. Fare clic su **Sì** per confermare.

Log di notifica tramite cercapersone

Il processo di notifica tramite cercapersone utilizza la funzione di log del firewall per scrivere i log di emissione. Tutti i messaggi e gli errori del cercapersone sono scritti nella funzione syslog generale del firewall. Per ulteriori informazioni sulle modalità di impostazione e l'utilizzo dei file di log del firewall, consultare il Capitolo 15, “Gestione dei file di log e di archivio” a pagina 107.

Verifica dell'impostazione del cercapersone

È possibile verificare l'impostazione del cercapersone utilizzando il comando `pager`. Per i dettagli, consultare *IBM eNetwork Firewall - Manuale di riferimento*. Si consiglia di utilizzare il comando pager ogni volta che viene definita o modificata l'impostazione per accertarsi che il sistema, il modem, la portante e le unità del cercapersone comunichino fra loro correttamente e che le chiamate vengano effettivamente inviate e ricevute.

Comandi eseguibili

È possibile specificare un programma che viene richiamato ogni volta che viene raggiunta una soglia di avviso. Per specificare un programma:

1. Fare clic sulla casella relativa alla gestione del controllo dei log, quindi fare doppio clic su **NUOVO**.

   Viene visualizzata la casella di dialogo **Aggiungere Controllo Log**.
2. Nella casella a discesa **Tipo di classe**, selezionare **Comando eseguibile**. Viene abilitato il campo **Nomefile del comando** di questo pannello.
3. Nel campo **Nomefile del comando**, immettere il percorso completo del programma che si desidera richiamare quando viene raggiunta una soglia di avviso.

   Il firewall trasmette tutti i messaggi di attenzione come primo parametro del programma, come di seguito riportato:

   ```
   Numero totale di errori di autenticazione: ICA0001e
   Errori di autenticazione per utente: ICA0002e
   Errori di autenticazione da host: ICA0003e
   Soglia messaggio: ICA0004e
   ```

Per una descrizione completa di questi messaggi, consultare *IBM eNetwork Firewall - Manuale di riferimento*.

Capitolo 15. Gestione dei file di log e di archivio

Questo capitolo descrive il modo in cui utilizzare le funzioni di log tramite il client di configurazione. Quando gli utenti tentano di accedere agli host tramite i vari server IBM Firewall, IBM Firewall scrive le entrate nel file di log gestito dal `servizio di log di IBM Firewall`.

A seconda del modo in cui è stata eseguita la configurazione del firewall, IBM Firewall può generare grossi volumi di informazioni. Le entrate di log possono avere diverse fonti, quali i socks ed i filtri avanzati. Inoltre, i file di log possono essere scritti con vari livelli di gravità; ad esempio *debug, informazione* o *errore*. Questo capitolo descrive anche il modo in cui utilizzare le funzioni di gestione dei log e degli archivi dei log per gestire la dimensione dei file di archivio e di log.

Creazione dei file di log e di archivio utilizzando il client di configurazione

È possibile utilizzare il client di configurazione per la gestione dei log e degli archivi dei log. Si presuppone che lo spazio su disco disponibile sia sufficiente a contenere tutte le informazioni sui log. Il firewall genera informazioni sugli errori ed il debug di routine con la funzione `log firewall`. Solo il responsabile principale del firewall può accedere alla funzione `log firewall`. I messaggi di avviso vengono registrati con la funzione log avvisi . Le informazioni sui log di controllo di gestione vengono registrate nella funzione `audit log` **.**

Per un corretto funzionamento dei programmi di utilità per i prospetti, è importante che solo i messaggi di log firewall compaiano nei rispettivi file di immissione. Nessun'altra funzione deve essere indirizzata allo stesso file di `log firewall`; impostare quindi il log del firewall adeguatamente.

Se si desidera visualizzare gli avvisi sul pannello principale del client di configurazione, occorre indirizzarli su un file indicato come funzione `log avvisi`. Non specificare altro per questo file.

I seguenti livelli di priorità comprendono anche il livello *debug* che raccoglie la maggior parte delle informazioni. Il livello *Condizione critica* raccoglie solo gli eventi firewall più gravi.

- Debug
- Informazione
- Avvertenza
- Errore
- Condizione critica

Si consiglia di iniziare con il livello *informazione* fino a quando le procedure firewall non diventano stabili. È quindi possibile passare al livello *avvertenza* o *errore* per ridurre l'attività di log e la dimensione del log di sistema.

I livelli di priorità non corrispondono esattamente al suffisso della tag di messaggio *(i,e,w,s..)*. Può essere necessario fare degli esperimenti per determinare come *eliminare* alcuni messaggi.

Aggiunta delle funzioni di log

Dall'albero di navigazione del client di configurazione, fare doppio clic sull'icona della cartella di file Gestione del Sistema per espandere la vista. Fare doppio clic sull'icona della cartella di file Log di sistema per espandere la vista. Selezionare Funzioni di Log. Viene visualizzata la casella di dialogo **Funzioni di log** che mostra l'insieme delle funzioni di log attualmente abilitate.

1. Selezionare **NUOVO** dalla casella di dialogo **Funzioni di log** e fare clic su **Aprire** per aggiungere un'entrata syslog a quelle attualmente abilitate.

   Viene visualizzata la casella di dialogo **Aggiungere Funzioni di Log**, come illustrato nella Figura 29.

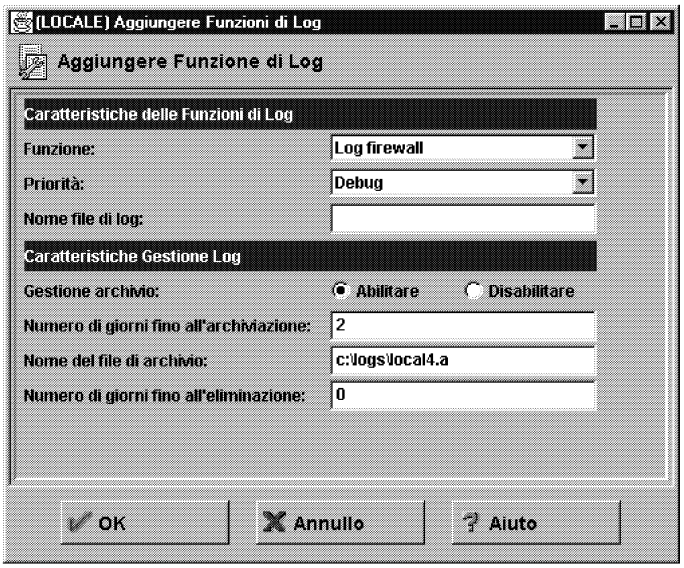

Figura 29. Aggiungere Funzioni di Log

2. Fare clic sulla freccia **Tipo** per selezionare un tipo. Il tipo è Nomefile.
3. La funzione di log determina il tipo e l'origine delle informazioni di cui viene eseguito il log. Fare clic sulla freccia **Funzione** per selezionare una delle seguenti funzioni:
   - Log firewall - log di firewall generali, log di filtro inclusi
   - Log avvisi - lo stato del daemon di controllo log e le avvertenza delle violazioni di soglia forniti in Visualizzazione avvisi
   - Posta
4. Fare clic sulla freccia **Priorità** per scegliere la priorità. Le priorità di log sono elencate in ordine crescente di gravità. La priorità selezionata corrisponderà al livello minimo su cui viene eseguito il log.
5. Immettere il nome del file di log. Il nome del file di log deve avere un percorso assoluto (che inizi con un'unità e con una barra retroversa '\') ed il percorso al file deve essere un percorso esistente.
6. La gestione degli archivi può essere utilizzata solo con una funzione di log di tipo *nomefile*. Quando abilitate, le dimensioni del file di log possono essere ridotte periodicamente. Abilitare la gestione degli archivi significa impostare i parametri dai quali dipende il comando `fwlogmgmt`. Consultare la sezione “Log

di archiviazione” a pagina 109. È possibile abilitare o disabilitare i parametri di gestione degli archivi.

7. Selezionare il numero di giorni dopo i quali i record presenti in un log di archivio devono essere archiviati. Il valore deve essere uguale a zero o maggiore di zero. L'archiviazione si verifica quando con il comando `fwlogmgmt -l` vengono ritrovati dei record di log attivi qualificati in base a questo criterio. La gestione dei log non include il giorno corrente quando viene eseguito il calcolo del numero di giorni di conservazione del record di log.
8. Immettere un nomefile di archivio ed un percorso completo. IBM Firewall fornisce una funzione di archiviazione assunta, che utilizza un indirizzario. Tuttavia, se si desidera, è possibile utilizzare funzioni di archiviazione interne.
9. Selezionare il numero di giorni dopo i quali un file di log archiviato deve essere eliminato dall'archivio. Il valore deve essere uguale a zero o maggiore di zero. L'eliminazione si verifica quando con il comando `fwlogmgmt -a` vengono ritrovati dei file archiviati qualificati in base a questo criterio. La gestione dei log non include il giorno corrente quando viene eseguito il calcolo del numero di giorni di conservazione di un file archiviato.
10. Fare clic su **OK**.

Modifica delle funzioni di log

1. Selezionare l'entrata relativa alla funzione di log del firewall che si desidera modificare dalla casella di dialogo **Funzioni di log** e fare clic su **Aprire**.

   Viene visualizzata la casella di dialogo **Modificare le Funzioni di Log**.
2. Modificare i campi desiderati. Per una spiegazione sugli altri campi, consultare la sezione “Aggiunta delle funzioni di log” a pagina 108.
3. Fare clic su **OK**.

Eliminazione delle funzioni di log

1. Selezionare un'entrata relativa alle funzioni di log del firewall da quelle attualmente abilitate nella casella di dialogo **Funzioni di log** e fare clic su **Eliminare**.

   Viene visualizzato il pannello **Avvertenza eliminazione**.
2. Fare clic su **OK** se si desidera continuare con l'eliminazione. In caso contrario, fare clic su **Annullo**. Questa operazione non elimina il file di log corrente.

Log di archiviazione

Il processo di archiviazione:

- Rimuove i record di qualificazione da un log attivo
- Inserisce i record di qualificazione in un file diverso
- Compatta il file risultante
- Inserisce il nuovo file in un indirizzario di archivio

Per avviare un programma di gestione dei log per l'archiviazione dei record di log accumulati, esistono due opzioni:

1. Eseguire il comando `fwlogmgmt -l` dalla riga comandi di volta in volta

2. Impostare il comando `fwlogmgmt -l` come un NT Scheduled Service.

L'eliminazione degli archivi di log consiste nell'eliminare i file di qualificazione archiviati dall'indirizzario di archivio.

Per eliminare i file archiviati, esistono due opzioni:

1. Eseguire il comando `fwlogmgmt -a` dalla riga comandi di volta in volta
2. Impostare il comando `fwlogmgmt -a` come un servizio pianificato di NT.

I record ed i file di qualificazione vengono determinati dai valori specificati nelle definizioni delle funzioni di log, come descritto nella sezione “Aggiunta delle funzioni di log” a pagina 108.

Il modo più efficiente o conveniente per eseguire il processo di gestione dei log consiste nell'impostarlo come servizio pianificato di NT. Avviare il processo utilizzando l'oggetto Servizi sul pannello di controllo.

Ad esempio, se si desidera impostare l'esecuzione del processo di archiviazione della gestione dei log ogni giorno alle 3:00, immettere

```
at 3:00 /every:M,T,W,Th,F,S,Su fwlogmgmt -l
```

DLL interno

Consultare *IBM eNetwork Firewall - Manuale di riferimento* per informazioni sulla DLL direttamente collegata che può essere utilizzata per sostituire la DLL assunta del firewall.

Emissioni della gestione dei log

La funzione di gestione dei log esegue alcuni controlli di integrità preliminari prima di procedere alle attività di gestione dei log. Se viene riscontrato qualche problema, i messaggi di diagnostica vengono inviati alla funzione di log del firewall quando si esegue il comando `fwlogmgmt` dalla riga comandi.

Le funzioni di log della posta o di controllo del responsabile (local0) sono soggette a regole di archiviazione differenti dalle altre funzioni. Per poter essere archiviate, le funzioni di log richiedono che l'archiviazione venga abilitata. Tuttavia, i record di log firewall (local4) e avvisi (local1) vengono archiviati soltanto se le loro date superano i criteri specificati nella definizione delle funzioni al momento dell'esecuzione del processo di archiviazione; mentre l'*intero* file di log di controllo o di posta viene archiviato ogni volta. Inoltre, le informazioni contenute nel log di posta sono rivolte soprattutto alle attività di debug, pertanto non sono così importanti da essere archiviate. Invece, le informazioni di posta più utili sono registrate nel log firewall (local4).

Programmi di utilità per i prospetti

È possibile utilizzare le funzioni dei programmi di utilità per prospetti per un ausilio nella creazione di prospetti dai file di di log correnti o archiviati. I programmi di utilità per i prospetti creano dei file disposti in tabelle di informazioni sulla gestione che sono organizzati e formattati in modo da consentire una semplice mappatura alle tabelle del database relazionale. Queste tabelle consentono al responsabile del firewall di analizzare:

- l'utilizzo generale del firewall
- gli errori nel processo del firewall
- i tentativi di accesso non autorizzati alla rete sicura

Utilizzando i programmi di utilità per i prospetti ed il log del firewall, il responsabile può creare un file di testo regolare dei messaggi. È possibile, inoltre, creare ed importare i file disposti in tabelle in altre tabelle presenti all'interno di un sistema di database relazionali, come ad esempio la famiglia di prodotti DB2. Il responsabile può quindi utilizzare SQL (Structured Query Language) per interrogare i dati e generare i prospetti.

I programmi di utilità per i prospetti sono installati come parte dell'installazione del firewall. È anche possibile installarli separatamente ed eseguirli su un host non firewall. È possibile utilizzare il client di configurazione per eseguirli su un firewall. Su una macchina non firewall, utilizzare la riga comandi.

Per un corretto funzionamento dei programmi di utilità per i prospetti, è importante che solo i messaggi di `log firewall` vengano visualizzati nei rispettivi file di immissione. Nessun'altra funzione deve essere indirizzata allo stesso file di `log firewall`; impostare quindi log firewall adeguatamente.

Non tentare di usare i programmi di utilità per i prospetti sui file di log precedenti a IBM Firewall per AIX V3R1. È possibile, tuttavia, utilizzare i programmi di utilità per i prospetti per elaborare i file di log di IBM Firewall per AIX V3R1 o successiva. È anche possibile utilizzarli per elaborare il log su AIX. Per informazioni più dettagliate sui programmi di utilità per i prospetti, consultare *IBM eNetwork Firewall - Manuale di riferimento*.

Esecuzione dei programmi di utilità per i prospetti utilizzando il client di configurazione

Dall'albero di navigazione del client di configurazione, fare doppio clic sull'icona della cartella di file Gestione del Sistema per espandere la vista. Fare doppio clic sull'icona della cartella di file Log di sistema per espandere la vista. Selezionare **Programmi di utilità per i prospetti**. Viene visualizzata la casella di dialogo **Programmi di utilità per i prospetti**, come illustrato nella Figura 30 a pagina 112.

1. Per il programma di archiviazione assunto fornito con IBM Firewall, il nome percorso di archivio dei log rappresenta l'indirizzario contenente i file di log compressi. Nel campo Nome percorso di archivio dei log, immettere l'indirizzario specificato nel campo relativo all'indirizzario di archivio della casella di dialogo **Funzioni di log**. Immettere il nome percorso assoluto per l'indirizzario di archivio. Se si desidera visualizzare un file di log che non è archiviato, lasciare questo campo vuoto.
2. Selezionare **Tipo di prospetto**. Per visualizzare il testo del messaggio di log per esteso, selezionare **Log di testo**. Per creare dei file disposti in tabelle da utilizzare con il DB2, selezionare **Log tabella**. Se si importano i file risultanti in DB2, è possibile eseguire delle interrogazioni SQL sui dati dei log. Per ulteriori informazioni, consultare *IBM Firewall eNetwork - Manuale di riferimento*.
3. Il nomefile di log è uno dei file di log archiviati compressi, un altro `log firewall` valido oppure il nome di un file di log su AIX. Se è stata selezionata un'entrata nel campo relativo all'indirizzario di archivio dei log, è possibile fare clic sulla freccia **Nomefile di log** per scegliere il log da utilizzare. Se non si immette un archivio dei log al passo 1, il nomefile di log immesso deve essere

il nome di un file di log del firewall non compresso e valido oppure un file di log su AIX. Occorre specificare un percorso completo.

4. Selezionare il **tipo di log**, **firewall** o **su AIX**.
5. Immettere **Percorso e nomefile per testo di emissione**.
6. Selezionare **Sì** per accodare i risultati di una richiesta di log in tabella ai file disposti in tabelle esistente oppure **No** per sostituire i file esistenti.
7. Questo campo consente di selezionare alcuni tipi di messaggi da inserire nel file di testo di emissione. Il contenuto di questo campo viene considerato come i parametri presenti nel comando `Trova` di Windows NT standard. Ad esempio, se nel campo si immette "ICA0" (è necessario immettere anche i doppi apici), è come se si eseguisse il seguente comando:

   ```
   fwlogtxt < my.log | find "ICA0"
   ```

   Di seguito vengono riportate alcune entrate di esempio che vengono inserite in questo campo con i relativi risultati:

   ```
   FILTRO                          RISULTATO
   "ICA0"          Mostra i messaggi di attenzione per la soglia del controllo log
   "ICA3"          Mostra i messaggi Socks (#ICA3000 - 3999)
   "ICA2010"       Mostra solo le ricorrenze del messaggio ICA2010
   /V "ICA3"       Mostra tutti i messaggi eccetto i messaggi Socks
   /C "ICA001"     Conta il numero di messaggi ICA0001
   ```

8. Facendo clic su **OK** i file richiesti vengono inseriti nell'indirizzario di emissione specificato sulla macchina firewall.
9. Nell'area Risultati dei Programmi di Utilità per Prospetti viene visualizzato qualsiasi messaggio di errore del programma di utilità per i prospetti in esecuzione. Per visualizzare il testo di log risultante dal tipo di prospetto Log di testo, fare clic su **Visualizzazione log** nel pannello principale del client di configurazione del firewall ed immettere il nome del file di emissione completo. I file .tbl risultanti dal tipo di prospetto Log tabella, possono essere caricati in un database, come descritto in *IBM eNetwork Firewall - Manuale di riferimento.*.

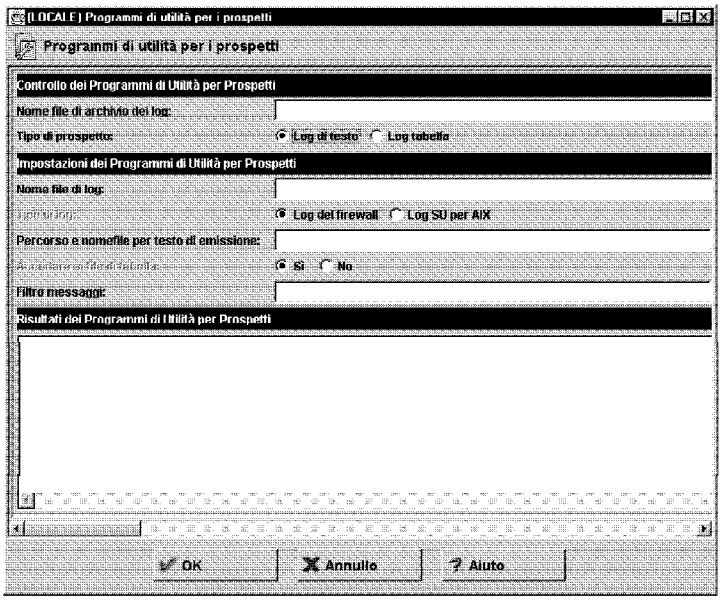

Figura 30. Programmi di Utilità per Prospetti

Bibliografia

Per ulteriori informazioni relative alla sicurezza su Internet, fare riferimento alla pagina iniziale di IBM eNetwork Firewall su **http://www.software.ibm.com/enetwork/firewall**.

Informazioni contenute nelle pubblicazioni IBM

Di seguito sono riportate ulteriori fonti di informazioni IBM sui firewall, sulla sicurezza Internet e su argomenti relativi alla sicurezza in generale.

Argomenti relativi al firewall

Questi documenti sono disponibili sul CD-ROM di IBM Firewall ed alla pagina iniziale di IBM eNetwork Firewall.

- *IBM eNetwork Firewall - Guida per l'utente*, GC13-2748-00
- *IBM eNetwork Firewall - Manuale di riferimento*, SC13-2750-00

Argomenti relativi ad Internet e Web (World Wide Web)

- *A Guide to the Internet Connection Servers*, SG24-4805
- *Accessing CICS Business Applications from the World Wide Web*, SG24-4547
- *Accessing OS/390 OpenEdition MVS from the Internet*, SG24-4721
- *Accessing the Internet*, SG24-2597
- *Building the Infrastructure for the Internet*, SG24-4824
- *Cool Title about the AS/400 and Internet*, SG24-4815
- *The Domino Defense: Security in Lotus Notes and the Internet*, SG24-4848
- *Examples of Using MQSeries on WWW*, SG24-4882
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Lotus Domino Server Release 4.5 on AIX Systems: Installation, Customization, and Administration*, SG24-4694
- *Netscape Proxy Server*, SK2T-7444
- *Running CICS Transactions through the Web: The CICS Internet Gateway to VSE/ESA*, SG24-4799
- *Safe Surfing: How to Build a Secure World Wide Web Connection*, SG24-4564
- *Teach Yourself CGI Programming with PERL in a Week*, SR23-7343
- *Using the Information Super Highway*, GG24-2499
- *World Wide Web Access to DB2*, SG24-4716

Argomenti relativi alla sicurezza

- *The Basics of IP Network Design*, SG24-2580
- *Elements of Security: AIX V4.1*, GG24-4433
- *Enterprise-Wide Security Architecture and Solutions Presentation Guide*, SG24-4579
- *HACMP/6000 Customization Examples*, SG24-4498
- *IBM Global Network (IGN) Security Policy*, GC34-2206
- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC24-8135
- *IBM Systems Monitor: Anatomy of a Smart Agent*, SG24-4398
- *Security Overview of Open Systems Networking*, GG24-3815
- *Systems Monitor for AIX User's Guide*, SC31-8173
- *TCP/IP Tutorial and Technical Overview*, GG24-3376

Informazioni contenute in altre pubblicazioni

Le seguenti pubblicazioni fanno riferimento a TCP/IP e UNIX:

- Albitz, Paul, and Cricket Liu. *DNS and BIND*. Sebastopol, CA: O'Reilly and Associates, 1997. (ISBN: 1-56592-236-0)
- Costales, Brian with Eric Allman. *Sendmail*. O'Reilly and Associates, Inc. (ISBN: 1-56592-222-0)
- Hunt, Craig. *TCP/IP Network Administration*. O'Reilly and Associates, Inc. (ISBN: 0-937175-82-X)
- Nemeth, Snyder, et al. *UNIX System Administration Handbook*. Prentice Hall. (ISBN: 0-13-151051-7

Le seguenti pubblicazioni fanno riferimento ai firewall ed alla sicurezza su Internet:

- Ahuja, Vijay. *Network and Internet Security*. Boston: Academic Press Professional, 1996. (ISBN: 0120455951)
- Ahuja, Vijay. *Secure Commerce on the Internet*. Boston: Academic Press Professional, 1997. (ISBN: 0120455978)
- Anderson, Bart, et al. *The Waite Group's UNIX Communications and the Internet*. Indianapolis, IN: Sams Pub., 1995. (ISBN: 0672305372)
- Atkins, Derek, et al. *Internet Security: Professional Reference*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562055577)
- Chapman, D. Brent, and Elizabeth D. Zwicky. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly and Associates, 1995. (ISBN: 1565921240)
- Cheswick, Willam R., and Steven M. Bellovin. *Firewalls and Internet Security*. New York: Addison-Wesley, 1994. (ISBN: 0201633574)
- Cooper, Frederic J., et al. *Implementing Internet Security*. Indianapolis, IN: New Riders Publishing, 1995. (ISBN: 1562054716)
- Curry, David. *UNIX System Security: Guide for Users and Systems Administrators*. Sebastopol, CA: O'Reilly and Associates, 1994. (ISBN: 0201563274)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX Security*. Sebastopol, CA: O'Reilly and Associates, 1991. (ISBN: 0937175722)
- Garfinkel, Simson, and Gene Spafford. *Practical UNIX and Internet Security*. Sebastopol, CA: O'Reilly and Associates, 1996. (ISBN: 1565921488)
- Hare, Chris, and Karanjit Siyan. *Internet Firewalls and Network Security*. Indianapolis, IN: New Riders Publishing, 1996. (ISBN: 1562056328)
- Randall, Neil. *Teach Yourself the Internet in a Week*. Indianapolis, IN: Sams.Net, 1995. (ISBN: 0672307359)
- Stallings, William. *Internet Security Handbook*. Foster City, CA: IDG Books, 1995. (ISBN: 0077092546)
- Stevens, W. Richard. *TCP/IP Illustrated*. Reading, MA: Addison-Wesley, 1994. (ISBN: 0201634953)

Glossario

Per accedere al glossario software IBM, andare all'indirizzo **http://www.networking.ibm.com/nsg/nsgmain.htm**.

Indice analitico

M

N

O

P

R

S

T

U

V

Riservato ai commenti del lettore

IBM eNetwork Firewall per NT
Guida per l'utente
Versione 3 Rilascio 2 **GC13-2748-00**

Commenti relativi alla pubblicazione in oggetto potranno contribuire a migliorarla.
Si invita il lettore ad usare lo spazio sottostante citando, ove possibile, i riferimenti alla pagina ed al paragrafo; i suggerimenti ed i commenti inviati potranno essere usati liberamente dall'IBM e dalla Selfin e diventeranno proprietà esclusiva delle stesse.
Si prega di non utilizzare questo foglio per richiedere informazioni tecniche su sistemi, programmi o pubblicazioni; per tali esigenze si consiglia di rivolgersi al punto di vendita o alla filiale IBM interessata.

Commenti:

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

Nome . . . . . .

Mansione/Titolo . . . . . .

Indirizzo . . . . . .

. . . . . Piegare . . . . . Piegare . . . . . .

. . . . . Piegare . . . . . Piegare . . . . . .

SELFIN S.p.A.

Translation Assurance

via F. Giordani, 7

80122 - N A P O L I

Printed in Denmark by IBM Danmark A/S

GC13-2748-00