

TerminET

Firewall personale

Guida utente

Sommario

1	INTRODUZIONE	3
1.1	INFORMAZIONI SU TERMiNET	3
1.2	FUNZIONALITÀ PRINCIPALI	3
2	OPERAZIONI PRELIMINARI	3
2.1	INSTALLAZIONE DI TERMiNET	3
2.2	CONNETTERSI A TERMiNET	4
2.2.1	<i>Windows 95/98</i>	4
2.2.2	<i>Windows NT/2000</i>	4
2.3	MODALITÀ AMMINISTRATORE	4
2.4	L'INTERFACCIA TERMiNET	4
3	UTENTI E GRUPPI. GESTIONE DI UTENTI E GRUPPI	7
3.1	AGGIUNTA DI UTENTI	7
3.2	CREAZIONE DI GRUPPI	8
4	REGOLE TRAFFICO	8
4.1	REGOLE NORMALI:	8
4.2	REGOLE AVANZATE:	8
4.3	CREAZIONE DI REGOLE:	8
5	ELENCHI WEB	11
5.1	ELENCO PROIBITI	11
5.2	ELENCO CONSENTITI	11
5.3	ELENCHI GLOBALI E LOCALI	11
6	PROBLEMI CON NETBIOS	12

1 Introduzione

1.1 Informazioni su TermiNet

TermiNET è uno strumento di protezione personale (firewall) ideato per proteggere il computer dalle aggressioni esterne durante i collegamenti a Internet, la consultazione sul Web o l'accesso ad altri servizi internet. TermiNet può essere installato in una delle seguenti modalità:

1. La modalità Chiusa blocca, per impostazione predefinita, tutto il traffico da e verso il computer locale. L'amministratore può decidere di permettere l'accesso in modo selettivo, ad esempio per consentire solo le comunicazioni FTP oppure l'accesso FTP, Telnet e Web. I genitori possono inoltre impostare l'accesso limitatamente ad un determinato gruppo di pagine. Le pagine possono essere immesse direttamente sotto forma di regole specifiche o prese da un elenco di URL consentite
2. La modalità Aperta non prevede condizioni di blocco iniziali. L'amministratore può decidere in modo selettivo di chiudere l'accesso in base all'applicazione, alla porta e al protocollo, ad esempio: bloccare tutte le comunicazioni Telnet e FTP, bloccare tutte le comunicazioni entranti sulla porta 25, bloccare l'accesso ad un determinato gruppo di pagine web che possono essere immesse sotto forma di regole specifiche o prese da un elenco di URL proibite
3. La modalità Protetta permette tutto il traffico in uscita ma blocca tutte le connessioni in entrata a meno che non siano state avviate localmente. In questa modalità il computer può essere utilizzato per una normale attività sul Web, FTP, ecc. e nel contempo è protetto dalle aggressioni dall'esterno durante i collegamenti ad Internet.

TermiNET è una soluzione economica ideale per le piccole aziende e per gli utenti domestici che desiderano collegarsi ad Internet ma non dispongono delle risorse necessarie per un sistema di protezione più complesso.

1.2 Funzionalità principali

Tra le principali funzionalità di TermiNET:

- Regole standard e avanzate: delle normali caselle di opzione, facilmente **attivabili** o **disattivabili**
- La funzionalità Elenco proibiti/Elenco consentiti che permette di impedire l'accesso a determinati siti o di consentirlo a siti ritenuti accettabili.
- Un controllo elastico dell'accesso che consente di definire le regole sulla base di indirizzi IP, URL, Porte e/o Protocolli.
- Le regole basate sui giorni possono essere impostate in modo da entrare in vigore solo in determinati giorni.
- L'interfaccia semplice ed intuitiva di TermiNET, tipo "Windows Explorer", lo rende un programma facile da installare ed utilizzare, anche per gli utenti non particolarmente tecnici.

2 Operazioni preliminari

2.1 Installazione di TermiNet

Inserire il CD TermiNET nel lettore corrispondente nel computer. Il programma di installazione dovrebbe lanciarsi automaticamente; in caso contrario, fare clic su "Start" ->"Esegui" e digitare "D:\setup" dove D: è l'identificativo di unità del lettore CD. Seguire le istruzioni visualizzate per installare il prodotto. Durante l'installazione è possibile specificare la posizione e scegliere una delle tre modalità predefinite di protezione: Aperta, Chiusa o Protetta descritte in precedenza.

Una volta terminata la procedura d'installazione, è **necessario** riavviare il computer per portare a termine l'installazione.

2.2 Connettersi a TermiNET

2.2.1 Windows 95/98

All'avvio del sistema, TermiNET è avviato con una serie predefinita di regole in base a quanto definito dall'amministratore. Se sono stati creati più profili utente TermiNET, gli utenti definiti possono collegarsi a scelta in due modi: facendo doppio clic sull'icona TermiNET nella barra delle applicazioni oppure facendo clic con il pulsante destro del mouse sull'icona TermiNET e selezionando "Logon". In entrambi i casi comparirà una finestra di connessione nella quale immettere l'ID utente e una password. L'immissione dell'ID e della password attiverà il profilo di sicurezza per quel determinato utente.

2.2.2 Windows NT/2000

Gli utenti sono connessi automaticamente a TermiNET sulla base del profilo di connessione NT.

2.3 Modalità amministratore

La modalità Amministratore permette la definizione del profilo di sicurezza predefinito degli utenti, la creazione di nuovi profili utenti e l'impostazione di regole avanzate per determinati utenti. Per entrare nella modalità Amministratore, fare clic con il pulsante destro del mouse sull'icona TermiNET nella barra delle applicazioni e selezionare "Modalità Amministratore". Verrà chiesto di immettere la password di amministratore. Dopo aver immesso la password, compare la finestra di configurazione di TermiNET dove eseguire tutte le attività di amministrazione.

Per uscire dalla modalità Amministratore, basterà chiudere la finestra di configurazione utilizzando l'opzione di menu "File -> Esci da Amministratore".

2.4 L'interfaccia TermiNET

L'interfaccia TermiNET (Figura 1) è accessibile solo tramite la password dell'amministratore. Uno strumento grafico permette di semplificare la definizione dei profili di sicurezza per un computer.

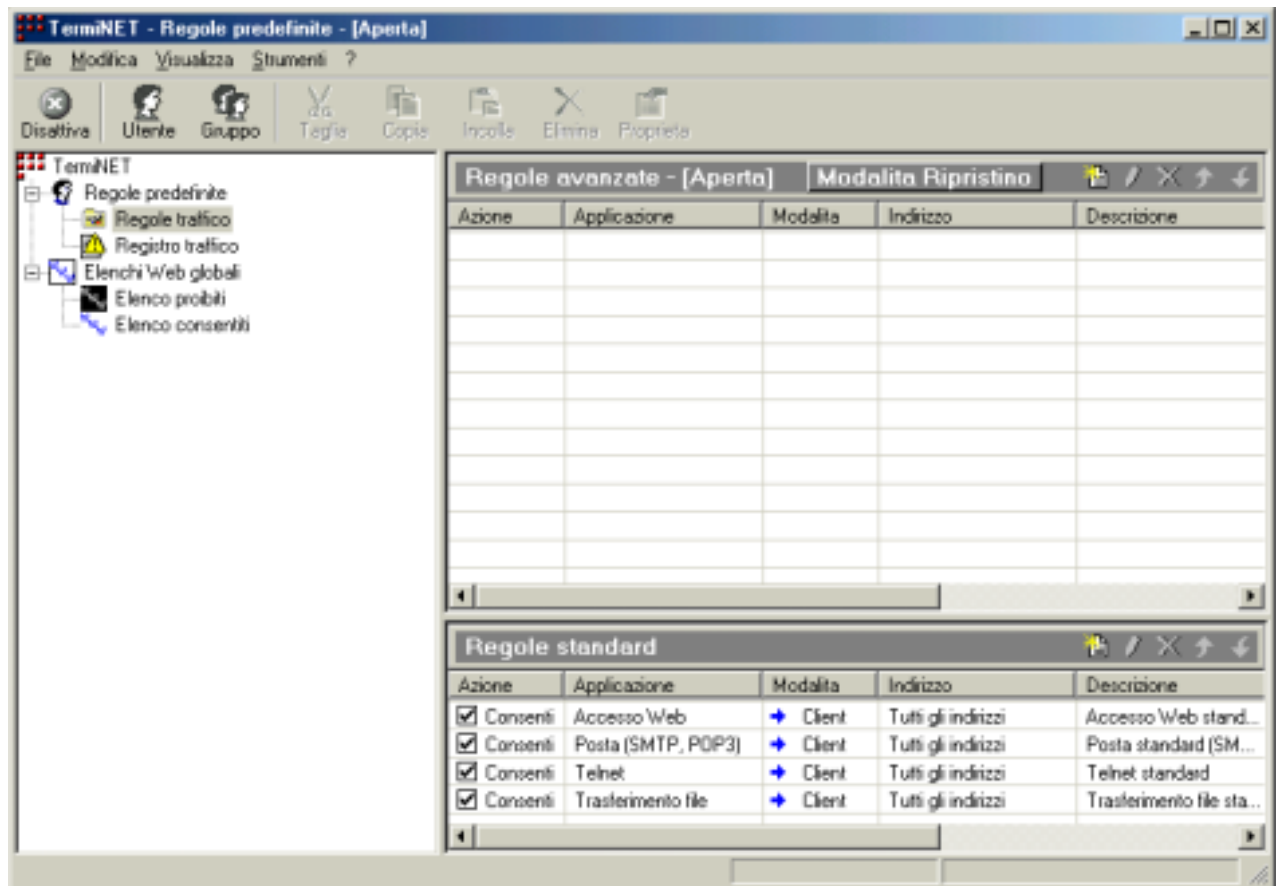


Figura 1

L'interfaccia è divisa in tre sezioni: la sezione di sinistra visualizza la struttura ad albero del sistema di sicurezza definito. La sezione nella parte inferiore destra visualizza le "Regole standard" preimpostate dal sistema. Le sezioni superiori a destra visualizzano le eventuali regole avanzate che sono state create. Se si seleziona un utente nella finestra di sinistra, in quella di destra verranno visualizzate le condizioni delle regole avanzate e standard per l'utente selezionato.

I menu File, Modifica e Visualizza permettono di personalizzare l'interfaccia in base alle preferenze degli amministratori. Il menu "Strumenti" ->"Opzioni" permette di impostare le proprietà generali del sistema.



Figura 2

La scheda Controllo (Figura 2) permette di accedere alle seguenti opzioni.

- | | |
|--|--|
| Mostra notifica di blocco: | Quando la casella di controllo Registro traffico è selezionata verrà visualizzato il traffico bloccato e consentito. Quando la casella è deselezionata verrà registrato solo il traffico consentito. |
| Crea file registro errori di sistema: | Quando la casella è selezionata gli errori di sistema verranno scritti nel file \Program Files\Infotecs\Terminet\Data\errorlog.txt. |
| Mostra schermata iniziale Infotecs all'avvio: | Deselezionare per evitare che lo schermo Infotecs Splascreen appaia all'avvio di Terminet. |
| Modifica password: | Permette di cambiare la password amministratore. |
| Numero di file registro: | Imposta il numero di file registro del traffico registrati. Una volta che il numero indicato è stato raggiunto e che l'ultimo file ha raggiunto le dimensioni massime, il primo file viene sovrascritto. |
| Dimensioni (in kilobyte): | Imposta la grandezza massima in kilobyte di un file. Quando il file raggiunge questa dimensione, il file è salvato e viene registrato un altro file. |

La scheda Applicazione (Figura 3) permette di creare nuove applicazioni standard.

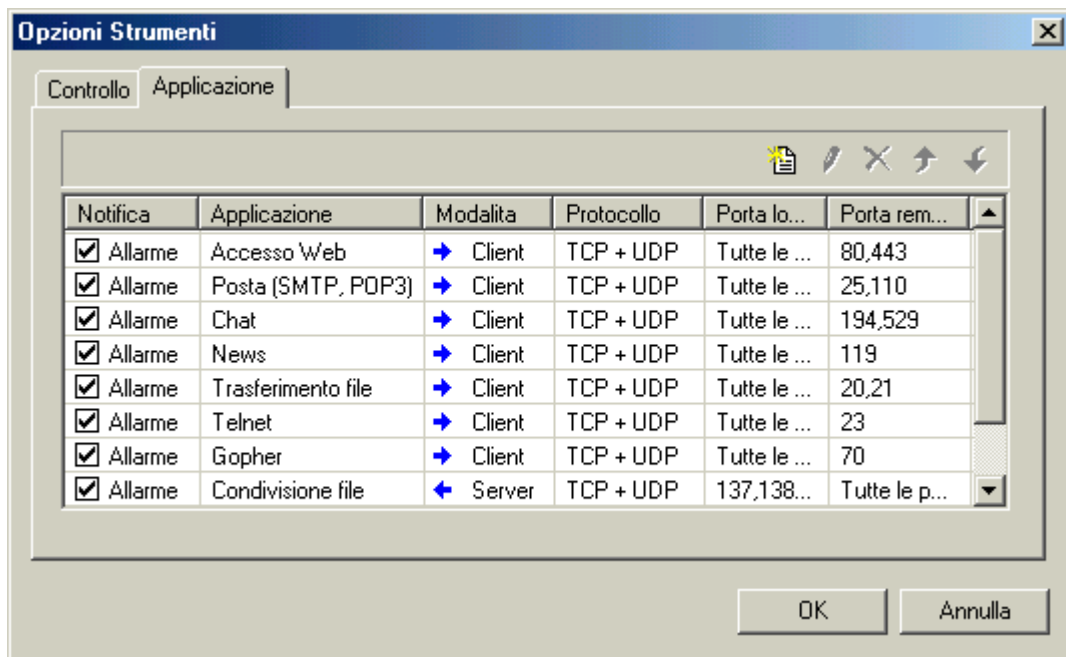


Figura 3

Fare clic sul pulsante Aggiungi applicazione  per aprire la finestra di dialogo Personalizza applicazione (Figura 4).

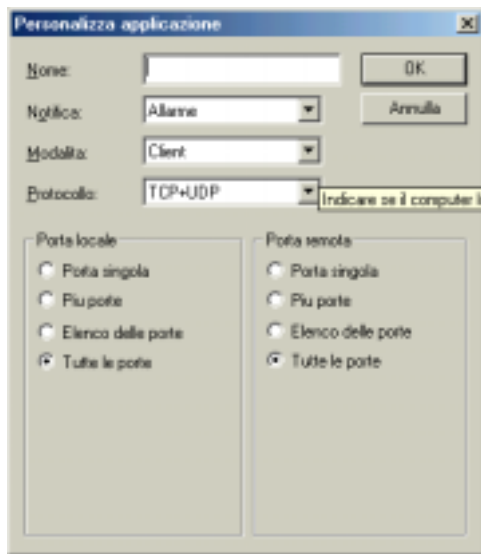


Figura 4

Questa finestra permette di impostare le seguenti opzioni.

- **Nome:** Indicare il nome dell'applicazione personalizzata.
- **Protocollo:** Selezionare il protocollo desiderato per l'applicazione nell'elenco di riepilogo a discesa.
- **Notifica:** Selezionare Allarme o Ignora nell'elenco di riepilogo a discesa. Se viene selezionato Allarme, comparirà un messaggio di avvertimento quando il traffico di questo tipo è bloccato.
- **Direzione:** Selezionare In entrata o In uscita nell'elenco di riepilogo a discesa.
- **Porta remota:** Indicare le impostazioni della porta applicabili al computer remoto per l'applicazione corrente.
- **Porta locale:** Indicare le impostazioni della porta applicabili al computer locale per l'applicazione corrente.

3 Utenti e gruppi. Gestione di utenti e gruppi

3.1 Aggiunta di utenti

Per aggiungere un profilo utente, fare clic con il pulsante destro del mouse nel punto più alto della struttura ad albero di TermiNET e selezionare "Aggiungi utente" nel menu a comparsa o fare clic sul

pulsante Utente nella barra degli strumenti. Verrà visualizzata la finestra di dialogo Proprietà utente (Figura 5)



Figura 5

Sono disponibili i seguenti campi.

- **Nome utente:** Immettere il nome attribuito all'utente.
- **Password:** Immettere la password che l'utente dovrà inserire.
- **Conferma password:** Immettere la password una seconda volta per confermarla.
- **Modo protezione:** Selezionare la modalità di protezione predefinita per questo utente.
- **Elenchi URL:** Determina se questo utente utilizzerà gli elenchi di URL proibiti o consentiti e se l'elenco globale, locale o entrambi.

3.2 Creazione di gruppi

I gruppi possono essere utilizzati per organizzare elenchi di utenti nella struttura ad albero di TerminiNET. Per creare un nuovo gruppo, fare clic con il pulsante destro del mouse nel punto più alto della struttura e selezionare "Aggiungi gruppo" dal menu a comparsa quindi immettere il nome del gruppo. Gli utenti potranno essere inseriti nei gruppi facendo clic sul nome dell'utente e trascinandolo nel gruppo desiderato. È possibile creare un utente in un gruppo esistente facendo clic con il pulsante destro del mouse sul gruppo nella struttura e selezionando "Aggiungi utente" nel menu a comparsa.

4 Regole traffico

In TerminiNet è possibile definire due tipi di regole del traffico.

4.1 Regole normali:

Sono applicate a tutti gli indirizzi IP e possono essere utilizzate per consentire o proibire l'accesso a determinati servizi. Quattro regole standard sono preimpostate dal sistema: Accesso Web, Posta, FTP e Telnet. Per aggiungere altre regole selezionare un utente nella struttura ad albero, fare clic con il pulsante destro del mouse nel riquadro Regole standard e selezionare "Aggiungi regola" nel menu a comparsa per aprire la finestra di dialogo Aggiungi regola. (Figura 6)

4.2 Regole avanzate:

Sono applicate a determinati indirizzi IP o URL e sono utilizzate per consentire o proibire l'accesso a determinati servizi e siti. Per aggiungere le regole, selezionare l'utente al quale verrà applicata la regola, fare clic con il pulsante destro del mouse nel riquadro Regole avanzate e selezionare "Aggiungi regola" dal menu a comparsa per aprire la finestra di dialogo Aggiungi regola. (Figura 6)

Se TerminiNET è installato in modalità Protetta, si possono configurare solo le regole avanzate.

4.3 Creazione di regole:

La finestra di dialogo Aggiungi regola (Figura 6) permette di creare e definire nuove regole.

Figura 6

Sono disponibili i seguenti campi.

- **Descrizione:** Immettere la descrizione della regola in corso di creazione
- **Azione:** Indicare se la regola consentirà o bloccherà il traffico definito.
- **Applicazione:** Selezionare un'applicazione tra quelle predefinite o immettere un nuovo nome per l'applicazione cui viene applicata la regola.
- **Modalità:** Indicare se il computer locale sarà client o server per la regola in corso di definizione. Se si indica "client" la regola verrà applicata al traffico in uscita, se si indica "server" la regola verrà applicata al traffico in entrata.

Le schede Indirizzo (Figura 7), Porta (Figura 8) e Giorni (Figura 9), permettono di impostare le funzioni avanzate della regola.

Indirizzo:

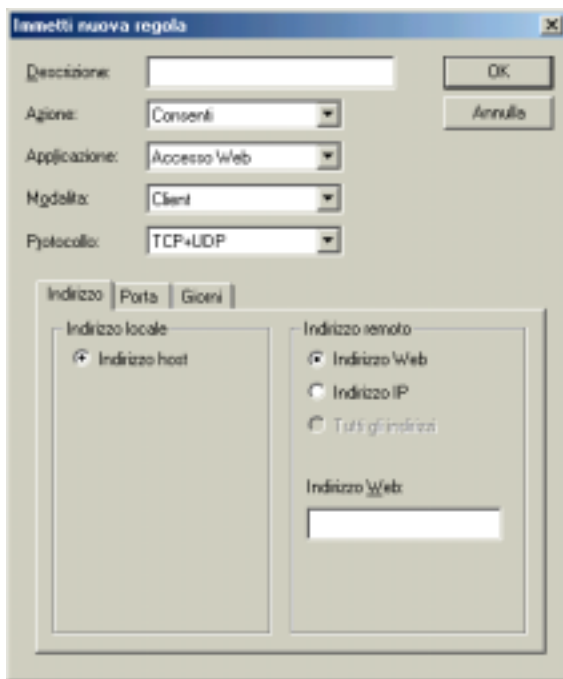


Figura 7

Per una regola standard l'unica opzione disponibile in questa scheda è "Tutti gli indirizzi"

Per le regole avanzate, è possibile indicare il sito cui è applicata la regola, specificando l'URL o l'indirizzo IP.

Se si seleziona il pulsante di opzione URL si potrà immettere un valore corrispondente nel campo Indirizzo.

Se si seleziona il pulsante Indirizzo IP il campo Indirizzo cambia in un campo per un indirizzo IP.

Porta:

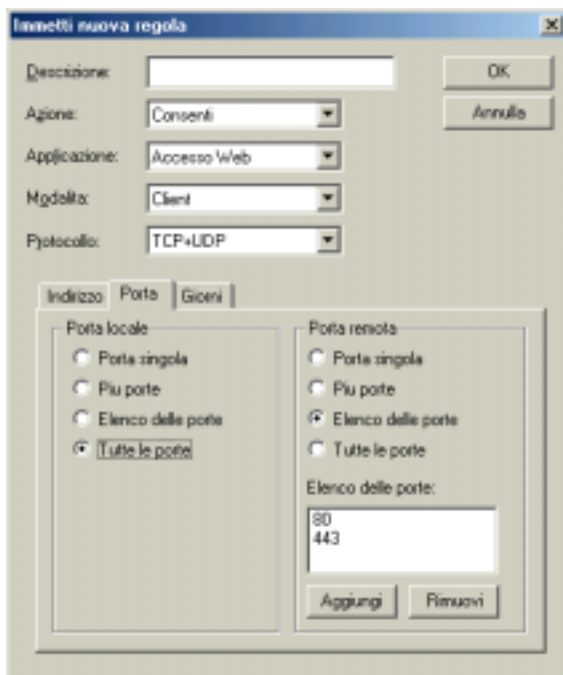
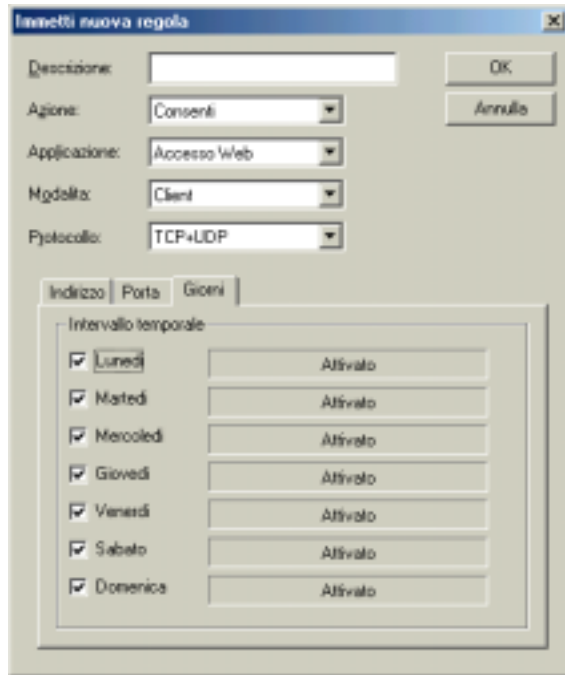


Figura 8

La scheda Porta (Figura 8) viene utilizzata per indicare la porta o la serie di porte cui è applicata la regola. Le impostazioni della porta devono essere configurate sia per i computer locali sia per quelli remoti. Sono disponibili le seguenti opzioni.

- **Porta singola:** Permette di indicare un solo numero di porta cui applicare la regola
- **Più porte:** Permette di indicare una serie di porte cui applicare la regola.
- **Elenco delle porte:** Permette di indicare un elenco di porte cui applicare la regola.
- **Tutte le porte:** La regola viene applicata a tutte le porte.

Giorni:



Intervallo temporale	
<input checked="" type="checkbox"/> Lunedì	Attivato
<input checked="" type="checkbox"/> Martedì	Attivato
<input checked="" type="checkbox"/> Mercoledì	Attivato
<input checked="" type="checkbox"/> Giovedì	Attivato
<input checked="" type="checkbox"/> Venerdì	Attivato
<input checked="" type="checkbox"/> Sabato	Attivato
<input checked="" type="checkbox"/> Domenica	Attivato

Questa scheda permette di attivare la regola solo in determinati giorni.

Figura 9

5 Elenchi Web

Gli elenchi Web possono essere utilizzati per consentire o proibire l'accesso a determinati siti. Gli elenchi URL possono essere Elenchi proibiti o Elenchi consentiti. I due tipi di elenchi si escludono a vicenda, vale a dire che un utente configurato per utilizzare un Elenco proibiti non potrà essere configurato per utilizzare un Elenco consentiti e viceversa.

5.1 Elenco proibiti

Gli elenchi proibiti sono utilizzati per impedire l'accesso a siti che invece una regola renderebbe accessibili. Ad esempio si può configurare una regola standard che consente l'accesso al Web e allo stesso tempo impedire l'accesso ad un determinato sito, ad esempio www.proibito.com, inserendolo in un Elenco proibiti. In questo modo l'utente potrà consultare tutti i siti Internet ad eccezione di www.proibito.com.

5.2 Elenco consentiti

Gli Elenchi consentiti sono utilizzati per consentire l'accesso a siti che invece una regola renderebbe inaccessibili. Ad esempio si può configurare una regola standard che impedisce l'accesso a tutti i siti Web e allo stesso tempo consentire l'accesso ad un determinato sito, ad esempio www.disney.com, inserendolo nell'Elenco consentiti.

5.3 Elenchi globali e locali

Esistono due tipi di Elenchi proibiti e consentiti: Locali e Globali. Un elenco globale viene creato dall'amministratore e può essere applicato a tutti gli utenti; il contenuto dell'elenco globale sarà valido per tutti gli utenti per i quali l'amministratore ha impostato un elenco URL globale. Un elenco locale è creato solo per un determinato utente e quindi il contenuto dell'elenco sarà valido solo per l'utente per il quale è stato creato l'elenco.

6 Problemi con NetBios

Si potrebbero incontrare dei problemi di accesso a host utilizzando NetBIOS su una connessione TCP/IP e in modalità Protetta. Il problema si verifica quando il computer utilizza messaggi broadcast per riconoscere l'indirizzo IP di un host sulla rete. In modalità Protetta TermiNET blocca i messaggi restituiti dall'host e impedisce quindi la comunicazione.

In questo caso sarà necessario inserire una voce nel file "HOSTS" che associ gli indirizzi IP degli host richiesti ai corrispondenti nomi NetBIOS. "HOSTS" è un normale file di testo che di solito si trova nella directory C:\windows in Win'98 o nella directory c:\system32\drivers\etc in Win NT e può essere modificato tramite un editor di testo. Consultare il file di esempio denominato hosts.sam nella directory per avere informazioni sulla struttura del file. Un file host potrebbe presentarsi come segue:

```
192.168.25.2 mioserver.miaorg.com
192.168.56.10 nt_server_1
```

Per aggiungere un host denominato nt_server_2 con indirizzo IP 192.168.35.23 modificare il file come segue:

```
192.168.25.2 mioserver.miaorg.com
192.168.55.10 nt_server_1
192.168.35.23 nt_server_2
```

Non si incontrerà questo problema se nella rete è stato configurato un server WINS.