Firewalls
Firewall

I ***firewall*** sono una componente o un insieme di componenti che limitano l'accesso tra una rete protetta ed ***Internet***. Essi proteggono le organizzazioni in ***Internet*** fornendo accessi sicuri: garantendo che utenti validi possano accedere alle risorse di rete di cui hanno bisogno.

Determinare chi sia un utente valido è compito del sistema di autenticazione; mentre determinare quali risorse un utente possa accedere è compito del sistema di autorizzazione (*Access Control*). Per fornire meccanismi di *Access Control*, un ***firewall*** richiede una comprensione profonda dei servizi e delle applicazioni utilizzati in rete.

Ci sono fondamentalmente due tipi di ***firewall***, quelli personali e quelli commerciali.

I firewall personali

I ***firewall*** **personali** sono programmi che proteggono un *computer* quando questo è collegato ad una rete. Un *personal* ***firewall*** analizza i canali di comunicazione, negando l'elaborazione del traffico ritenuto rischioso sia in ingresso che in uscita. Di seguito si analizzano le caratteristiche di alcuni prodotti molto diffusi e si riassumono le caratteristiche comparate, in una tabella.

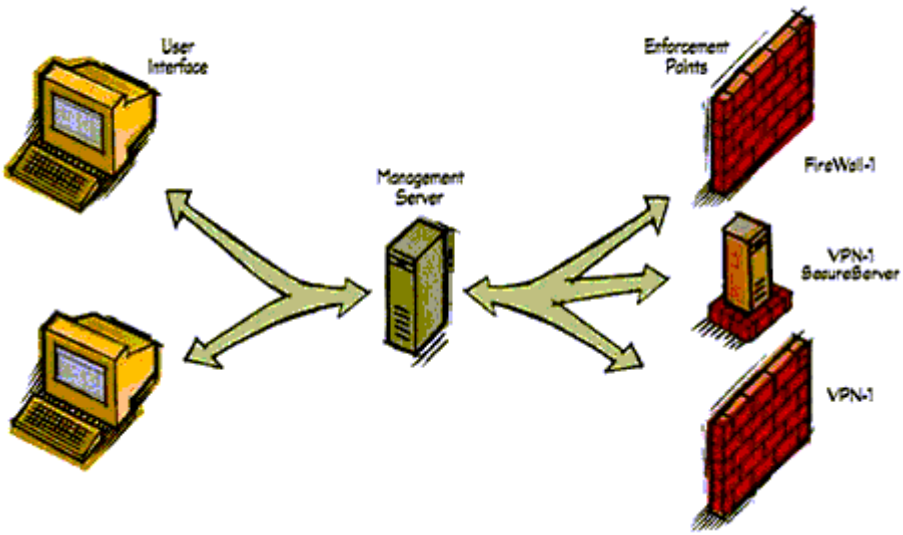
- ***Tiny Personal Firewall*** è un prodotto facile da configurare ed utilizzare che protegge completamente un *computer* dagli attacchi. *Tiny Personal Firewall* include dei *wizard* semplici per il rilevamento delle intrusioni che individuano attività sconosciute e chiedono all'utente di impostare i parametri del ***firewall***. Appositi *wizard* rilevano i tentativi di connessione alle porte di comunicazione e creano delle regole di *filtering* in base all'indicazioni dell'utente. Per garantire che dei cavalli di Troia non si nascondano all'interno di applicazioni viene utilizzata la firma digitale con algoritmo MD5.
- ***Norton Personal Firewall*** è un prodotto che controlla tutte le connessioni tra il *computer* e la rete. Fornisce dei *tool* e dei *wizard* per la configurazione automatica delle regole di *filtering*.
- ***Zone Alarm*** è simile ai precedenti per quel che riguarda protezione e *tool* di configurazione.

La tabella di seguito riportata elenca le caratteristiche dei prodotti considerati, in termini comparativi.

Caratteristica	***Tiny PF***	***Norton PF***	***Zone Alarm***
Firma Digitale	SI	NO	SI
Applicazioni *trusted*	SI	SI	SI
Indirizzi fidati	SI	SI	SI
Rilevamento intrusioni	SI	SI	SI
Amministrazione remota	SI	NO	NO
Log su Syslog	SI	NO	NO
Validità temporale delle regole	SI	NO	NO
Autenticazione	SI	NO	SI
In esecuzione come servizio	SI	SI	SI
Sistemi operativi supportati	95, 98, NT, 2000, Me	95, 98, NT, 2k, Me	95, 98, NT, 2000, Me
Freeware	SI	NO	NO

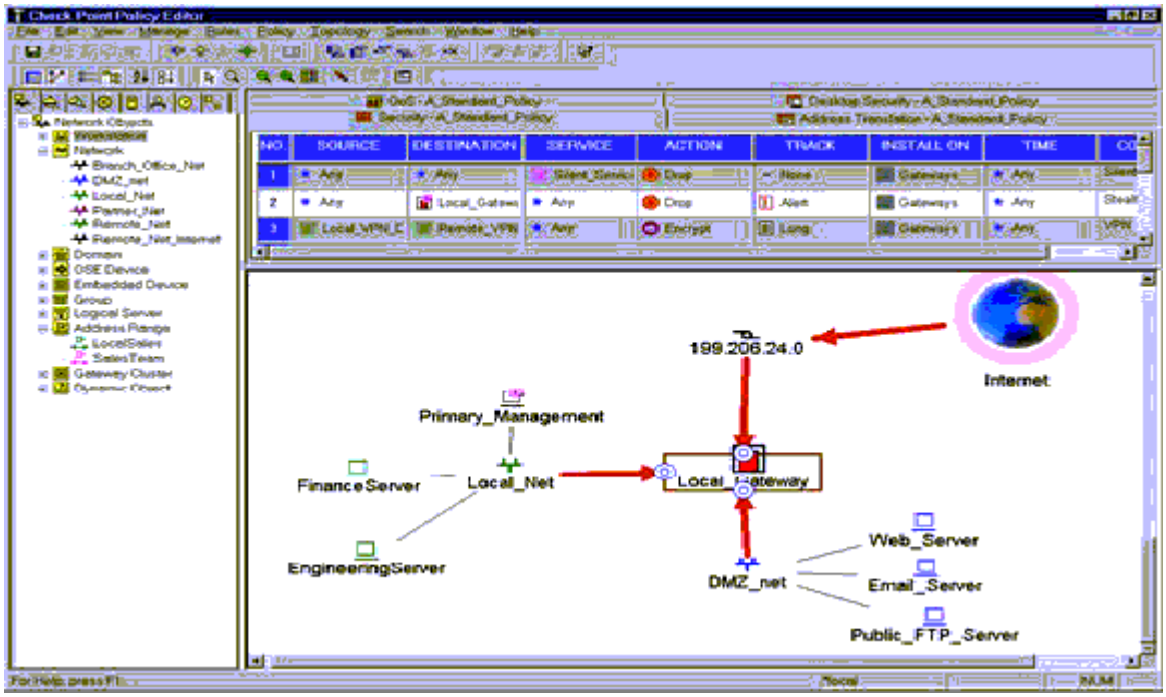
I firewall commerciali

Una soluzione per la sicurezza di un'organizzazione deve essere in grado di dichiarare una politica a livello di organizzazione, distribuirla e ricevere i *log*. Deve inoltre consentire all'organizzazione di controllare l'intera infrastruttura di sicurezza (i ***firewall*** dell'organizzazione, le reti private virtuali) da un unico punto di amministrazione.

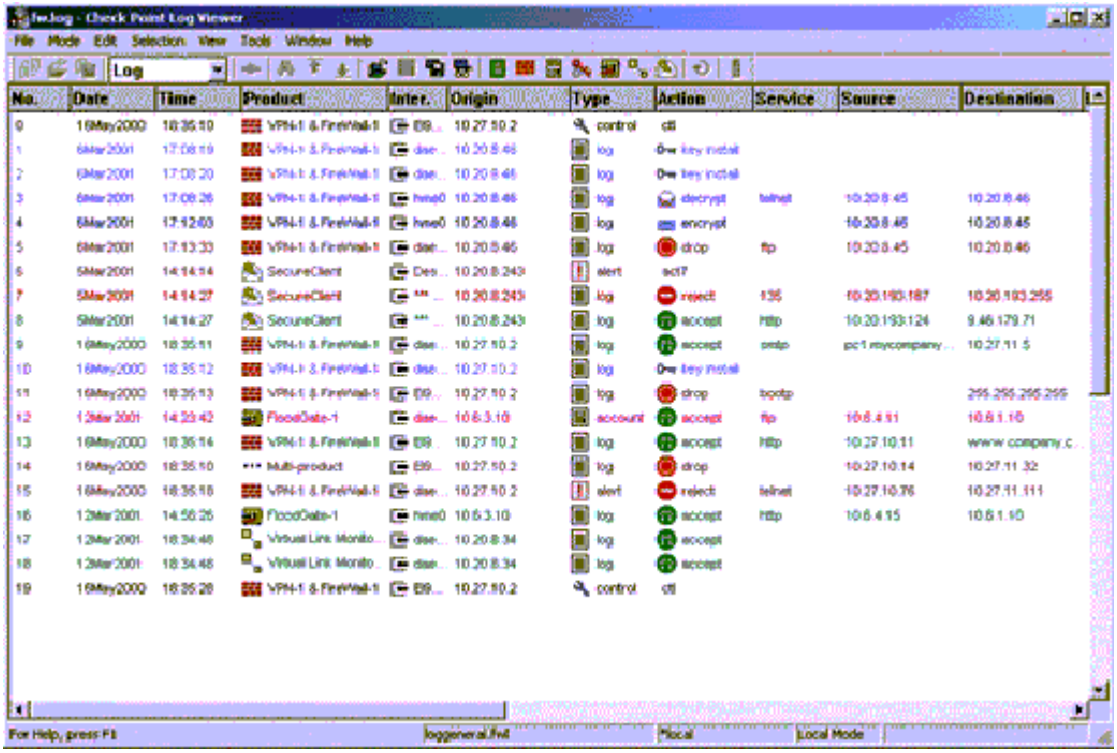


Esistono diversi prodotti che soddisfano i requisiti di sicurezza e che forniscono i *tool* per la protezione delle reti private delle organizzazioni. Si analizzano a titolo di esempio le caratteristiche di due prodotti commerciali molto diffusi: *Cisco PIX* e *Checkpoint Firewall 1*.

- ***Firewall Cisco***. Le principali caratteristiche sono:
  - *Context-Based Access Control*: fornisce agli utenti interni un controllo di accesso sicuro per tutto il traffico attraverso il ***firewall***.
  - Rilevamento delle intrusioni: fornisce il monitoraggio, l'intercettazione e la risposta in tempo reale agli abusi nella rete rilevando un vasto insieme di attacchi comuni.
  - *Proxy* di autenticazione: fornisce meccanismi di autenticazione e autorizzazione degli utenti per quel che riguarda le comunicazioni di rete e/o *dial-up*.
  - Rilevamento e prevenzione di attacchi di tipo DOS: difende e protegge le risorse del *router* da attacchi comuni.
  - Assegnazione dinamica delle porte.
  - Blocco delle ***applet Java***.
  - Supporto per reti VPN, cifratura IPSec e qualità del servizio.
  - *Alert* in tempo reale.
  - Funzionalità di *auditing* dettagliati: memorizza la data, l'***host*** di origine, l'***host*** di destinazione, le porte, la durata e il numero totale di *byte* trasmessi.
  - *Logging* degli eventi: consente agli amministratori di rilevare in tempo reale, potenziali buchi di sicurezza o altre attività non *standard* effettuando il *logging* dei messaggi di errore di sistema su un *Syslog* ***server***.
  - Funzionalità di gestione del ***firewall***: *tool* di configurazione che offre la possibilità di definire passo passo le azioni necessarie per la protezione della rete.
  - Strategie di *filtering* del traffico base ed avanzate.
  - Ridondanza/*fileover*: dirotta automaticamente il traffico ad un *router* di *backup* nell'eventualità in cui il ***firewall*** vada in errore.
  - Funzionalità NAT.
  - Regole per il *filtering* temporizzato.
- ***Checkpoint Firewall-1***. Un ***firewall*** *Cisco* è un dispositivo *hardware* per la protezione di una rete, *Checkpoint Firewall-1* è invece un'**applicazione** *software*. La *console* di *management* di *Checkpoint Firewall-1* fornisce una singola interfaccia grafica per definire e gestire molti elementi di una rete. Tutte le definizioni degli oggetti sono condivise tra tutte le applicazioni.



Gli amministratori della sicurezza possono selezionare la locazione degli oggetti oppure modificarne le caratteristiche utilizzando l'*editor* visuale per la definizione delle politiche di sicurezza. *Checkpoint Firewall-1* fornisce anche un *editor* visuale per i *log* che consente un'analisi in tempo reale delle informazioni relative al *tracking*, al monitoraggio e all'*accounting* di tutte le connessioni. Il modulo per la generazione dei *report* permette agli amministratori di trasformare i dettagliati *log* del ***firewall*** in *report* di gestione che rappresentano le informazioni mediante tabelle e grafici.



Installazione e configurazione di firewall

Per essere efficace un ***firewall*** deve essere ben installato e configurato, altrimenti rischia di essere o troppo restrittivo o troppo permissivo. Per evitare installazioni e configurazioni maldestre, prodotti di

cui si è detto in precedenza (***firewall*** personali e commerciali) hanno procedure automatiche di installazione: una volta scaricato il *software* da CD o da ***Internet***, è sufficiente lanciare il *set-up* corrispondente.

Windows XP offre un servizio di ***firewall*** per le connessioni ad ***Internet*** (ICF, *Internet Connection Firewall*). Questo *software* permette di limitare le informazioni scambiate tra ***Internet*** e la rete locale, proteggendo anche un singolo *computer*. Descriviamo i passi più importanti per abilitare o disabilitare un ***firewall*** in *Windows XP*. Per effettuare questi passi, è necessario avere l'accesso al *computer* con un *account* di amministratore.

1. Selezionare *Start*, scegliere Pannello di controllo e selezionare Connessioni di rete.
2. Selezionare il tipo di connessione che si possiede, quindi in Operazioni di rete, selezionare Cambia impostazioni connessione.
3. Nella cartella Avanzate in *Firewall* connessione *Internet*, selezionare una delle seguenti opzioni:
    - per abilitare i *firewall*, selezionare la casella di controllo **Proteggi il *computer* e la rete limitando o impedendo l'accesso al *computer* da *Internet***.
    - Per disabilitare i *firewall*, deselezionate la casella di controllo **Proteggi il *computer* e la rete limitando o impedendo l'accesso al *computer* da *Internet***. Disattivando il *firewall* i *computer* e la rete saranno esposti a intrusioni dall'esterno.