

L'obiettivo

Con la diffusione delle reti e la necessità di condividere informazioni verso l'esterno, oggi l'azienda ha esigenze di sicurezza sempre più pressanti. E' necessario quindi definire e proteggere la propria rete da intrusioni di applicazioni potenzialmente dannose. Quindi l'azienda deve poter disporre di livelli di sicurezza nella propria rete e soprattutto definire regole che diventino parte integrante della propria infrastruttura.

Il firewall è sicuramente un elemento essenziale per raggiungere un elevato livello di sicurezza su una rete locale. Il modello di firewall che si può implementare dipende molto dalle politiche di sicurezza, che come detto, devono essere decise a priori ed applicate con coerenza.

Il firewall è una struttura che si interpone fra sistemi differenti quali una rete locale (LAN) e una rete pubblica ed implementa un instradamento vincolato verso le risorse di rete operando delle restrizioni. Il firewall implementa una politica di sicurezza attraverso restrizioni e controlli degli accessi limitando l'esposizione della rete locale rispetto all'esterno.

Assyrus Firewall si articola in due prodotti distinti, ma caratterizzati da funzionalità comuni:

- **Intranet Network Firewall:** per collegare in modo sicuro reti Intranet a reti Internet (o ad una DMZ aziendale)
- **Internet Firewall:** per proteggere e controllare il traffico dei server Internet aziendali (o dei server nella DMZ)

L'utilizzo combinato dei due prodotti permette di definire un'architettura a DMZ per incrementare il livello di sicurezza della propria rete.

Funzioni base

Le due linee di prodotto sono caratterizzate dalle seguenti funzioni comuni:

- Packet Filtering (statefull), per il controllo della sicurezza a livello perimetrale
- Proxy Filtering, per il controllo della sicurezza a livello applicativo
- Funzioni specifiche per proteggere la rete da attacchi di varia natura (spoofing, flooding, smurf...), in particolare filtri anti IP-Spoofing e anti DoS
- Immunità del firewall ad attacchi sniffing
- QoS e controllo di banda
- Integrabilità con un NIDS
- Stack TCP/IP ottimizzato, con sistema per impedire la previsione del numero di sequenza delle connessioni TCP
- Preconfigurazione per una protezione ottimale della propria rete
- Interfaccia utente web per la configurazione e la gestione, tramite protocollo sicuro HTTPS
- Opzionalmente, interfaccia utente grafica, con funzionalità di wizard, per la configurazione e la gestione (da installare su una macchina Windows 9x/NT/2000)
- Gestione e manutenzione sicura da remoto, tramite protocolli sicuri (SSH)
- Sistema operativo sicuro con funzioni di controllo di integrità
- Scalabilità, con funzioni di aggregazione di schede di rete per aumentare il throughput totale
- Interoperabile con diversi standard della famiglia IEEE 802
- Funzioni di routing per collegare reti diverse
- Funzioni di log a livello di rete (indirizzi IP), a livello di trasporto (porte utilizzate) e a livello applicativo (URL visitati)
- Messaggi d'allarme tramite console di gestione, e-mail e, opzionalmente, SMS
- Upgrade automatico dei pacchetti software
- Monitoraggio attivo del funzionamento del firewall (utilizzo processore, memoria, disco) e del funzionamento delle reti (traffico su ciascuna rete, traffico filtrato dal firewall, ...)
- Supporto opzionale per VPN basate su standard IPSec (VPN IPSec Ready)
- Opzionalmente, funzionalità di Fail-over/ hot standby per l'affidabilità di rete, applicazioni mission critical

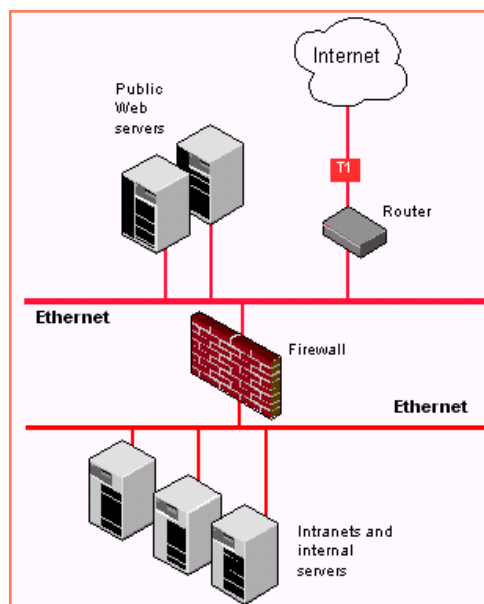
NOTA: Il pacchetto di manutenzione prevede la gestione remota e l'upgrade automatico del software per mantenere il firewall immune ad attacchi



Funzioni Internet Firewall

Oltre alle funzioni base, sopra menzionate, tale prodotto implementa tali funzioni specifiche:

- Si inserisce tra la rete Internet aziendale (o la DMZ) e il router di accesso a Internet e comprende opzioni di collegamento LAN TokenRing, Fast Ethernet o Ethernet
- DMZ ready
- Funzionalità di NAT (Network Address Translation)
- Funzionalità di PAT (Port Address Translation) per “redirigere” le porte locali verso porte della rete interna
- Funzionalità di “firewall trasparente” (t-firewall) che permette di sostituire il firewall con un cavo cross in caso di problemi o malfunzionamenti
- Opzionalmente, modalità stealth che permette al firewall di funzionare senza IP e quindi in modalità “invisibile”



Funzioni Intranet Firewall

Oltre alle funzioni base, sopra menzionate, tale prodotto implementa tali funzioni specifiche:

- Si inserisce tra la rete intranet aziendale e il router di accesso a Internet (o la rete DMZ) e comprende opzioni di collegamento LAN TokenRing, Fast Ethernet o Ethernet
- Funzionalità di “proxy trasparente” che permette di forzare l’utilizzo del proxy anche senza riconfigurare i client
- Filtraggio attivo degli URL, controllando i siti visitabili dagli utenti, in base ad alcune black-list automatiche, a black-list personalizzabili, a criteri di orario, a criteri specifici per ogni utente
- Funzionalità di NAT (Network Address Translation) per “mascherare” gli indirizzi privati della rete intranet in indirizzi pubblici Internet
- Funzionalità di PAT (Port Address Translation) per “redirigere” le porte locali verso porte della rete interna
- Opzionalmente, DHCP Server per la gestione semplificata delle rete interna
- Opzionalmente, Server Mail per la gestione della posta interna/esterna con controllo Antivirus
- Opzionalmente, File Server