

Introduzione ai Firewall

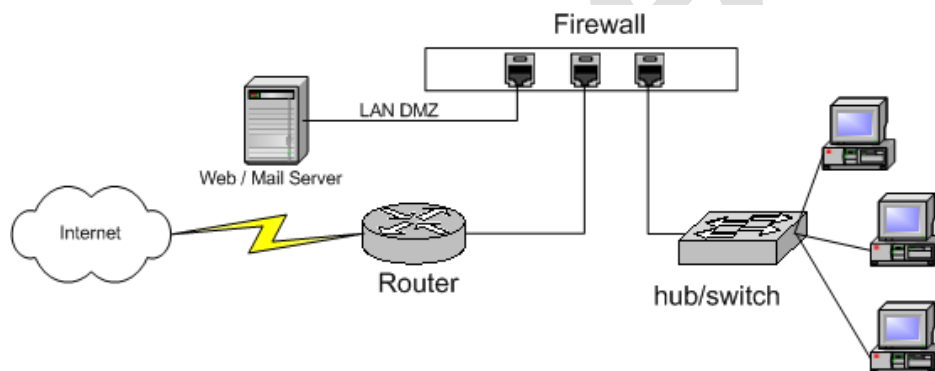
Il Firewall e' un sistema (hardware e software) posto sul "confine" tra una rete pubblica (vedi Internet) e una rete locale (o una sua parte "protetta") in modo che tutti i dati da e per un qualsiasi computer siano costretti a passare attraverso il firewall stesso. In tal modo i dati possono essere esaminati per stabilire se sono autorizzati o meno a transitare. Lo scopo del firewall e' quindi di ergere una "barriera virtuale" contro qualunque accesso non autorizzato in modo da proteggere il sistema locale da ogni indebita intrusione.

Ovviamente queste barriere sono bidirezionali, per cui un firewall potrà essere utilizzato anche per gestire l'uso di Internet da parte degli utenti della propria rete.

In sintesi: *"Un firewall è un sistema o un gruppo di sistemi che impone una politica di controllo dell'accesso tra due o più reti".*

Questo tipo di protezione può essere realizzato attraverso specifici software installati su computer "multihomed" (più schede di rete) o con appliance dedicati.

L'architettura più ricorrente utilizzando questi dispositivi è mostrata nella figura che segue:



Ma chi ci garantisce che un firewall faccia il suo dovere e ci protegga dalla rete? Questo non è semplice e riguarda almeno due aspetti: la sicurezza e affidabilità del firewall e il modo con cui è stato installato. Per il primo fattore esistono degli organismi (generalmente formati dai principali produttori) che certificano che il firewall ha passato determinati test. Uno di questi organismi è l'ICSA. Il secondo aspetto riguarda la professionalità e la competenza dell'installatore. La cosa migliore è sicuramente affidarsi a persone preparate che abbiano comprovata esperienza in questo settore.

Firewall Packet Filter

Un firewall è in genere in grado di analizzare il contenuto di ogni pacchetto che lo attraversa. Questo è fondamentale per bloccare il traffico indesiderato o gli attacchi di hacker Internet senza complicare eccessivamente le configurazioni. L'utilizzo di questa tecnica è particolarmente utile per filtrare gli attacchi Internet di tipo "denial of service" (il firewall riconosce che è in corso un tentativo di attacco verso una macchina Interna e lo blocca), la possibilità di verificare il sito in cui si sta navigando e il contenuto dello stesso per eventualmente bloccare o registrare comportamenti non consentiti. Il **packet filter** è realizzato mediante Access Control List opportunamente configurate.

Attacchi DoS

Denial of Service è l'identificativo di una particolare tipologia di attacchi che non mirano alla distruzione o al furto di dati bensì determinano un'interruzione del servizio. Il **Ping of Death** è uno degli attacchi DoS più noti e più semplici: si tratta di inviare all'host preso di mira un pacchetto ICMP con un carico di dati maggiore di 64Kb. Spesso questo "bombardamento" crea delle difficoltà ai sistemi di sicurezza soprattutto quelli meno recenti. Molti produttori di sistemi operativi hanno ovviato a questo problema rendendo disponibili apposite patch.

Il **SYN Flood** è un secondo tipo di attacco DoS che sfrutta una particolare procedura nell'avvio delle transazioni TCP (tecnicamente conosciuta handshake a tre vie). Questa procedura viene eseguita ogni volta che due host stabiliscono una sessione: il primo host invia un pacchetto che contiene una richiesta SYN (richiesta di sincronia); la macchina a cui viene spedito il pacchetto risponde con un pacchetto che contiene messaggi sia SYN e ACK (acknowledge); la terza fase della procedura prevede la risposta del primo host con un nuovo messaggio di ACK in modo da far partire la sessione.

Prima di inviare la risposta, le macchine che ricevono una richiesta di apertura di una sessione, accantonano in una zona della memoria la richiesta fino a quando la procedura di avvio della sessione non viene completata correttamente. Gli attacchi SYN Flood si basano proprio su questo particolare: la procedura di avvio della sessione viene eseguita più volte sempre per due terzi creando un collassamento dell'host remoto.

IP Spoofing è una tecnica di attacco molto complessa, in pratica, chi attacca cerca di collegarsi ad un server o ad un host "rubando l'identità" di una macchina nota. In una prima fase viene "bloccata" una macchina con un attacco DoS, quindi si presenta alla vittima con l'identità della macchina bloccata (questo avviene simulando il traffico di ritorno che il vero host non sta più generando). Questa tecnica viene generalmente utilizzata per guadagnare l'accesso di amministratore su una rete protetta.

I firewall sono sempre più affiancati da altre applicazioni che integrano e intensificano le politiche di sicurezza. I **server proxy** sono un esempio ormai consolidato. La differenza fondamentale tra i due moduli sta nel funzionamento: il firewall controlla il traffico di rete e verifica la conformità alle regole definite aprendo o meno un canale tra il client di rete e il server remoto. Il proxy, invece, raccoglie le richieste dei client delle rete e recupera direttamente le informazioni, mascherando la struttura della rete interna.

Documentazione prodotta dallo staff Netexpert.it.

La documentazione può essere riprodotta ed utilizzata liberamente per scopi istituzionali e formativi, e altresì rigorosamente vietato l'uso a fine di lucro. Gli autori non sono responsabili per danni recati a software o hardware causati da eventuali informazioni errate presenti in questo documento. Tutti i nomi o marchi registrati sono proprietà delle rispettive aziende.

Chiunque voglia segnalare errori, omissioni o suggerimenti può farlo all'indirizzo net001@netexpert.it