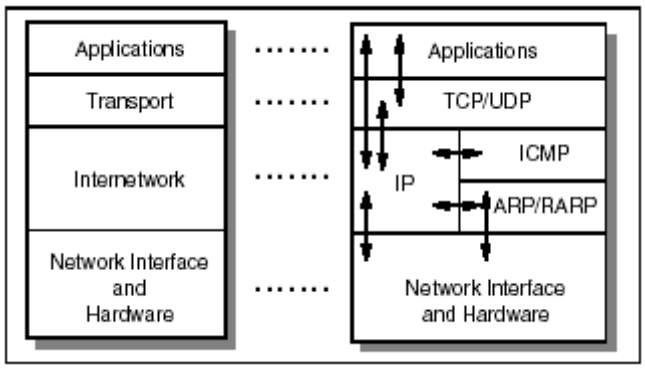
INTRODUZIONE ALLA SICUREZZA: IL FIREWALL

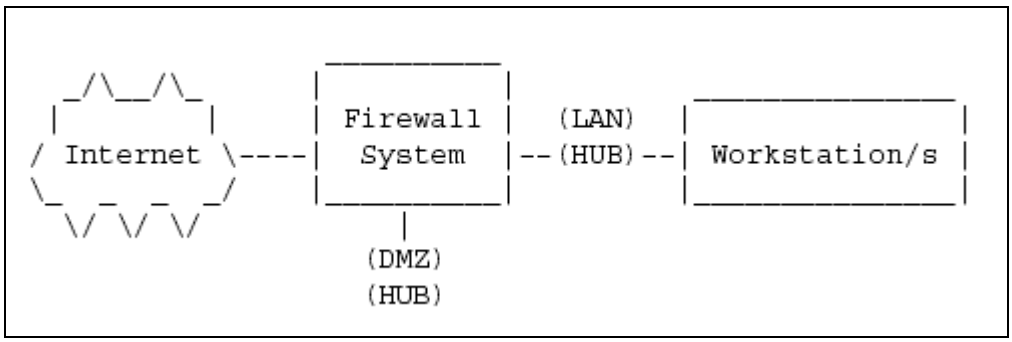
Fino a qualche anno fa la comunicazione attraverso le reti di computer era un privilegio ed una necessità di enti governativi e strutture universitarie. La sua natura intrinseca orientata primariamente alla connettività la rendeva semplice, non vincolata ad hardware e software specifici e poco costosa.
Proprio per questa sua filosofia di funzionamento la rete non ha mai avuto tra le caratteristiche principali quella relativa alla sicurezza.
Ovviamente, nel corso di questi anni, proprio la sua principale funzione di collegamento ha portato alla luce un nuovo fenomeno, Internet, ed esteso l'utilizzo di questo mezzo di comunicazione tra computer a livello mondiale.
Del resto i suoi punti di forza, come appunto la semplicità, hanno reso questo nuovo metodo di scambio dati adatto ad ogni esigenza.
Siamo addirittura arrivati al paradosso positivo della dipendenza dalla rete: tutto comunica e se non ne sei parte sei fuori da ogni cosa.
La rete, come molti di voi sapranno, si basa sullo standard di comunicazione **ISO/OSI** che prevede uno schema a pila.
Il modello viene definito come struttura stratificata, in cui ogni livello fornisce servizi essenziali al successivo e deve essere visto partendo dal basso della pila verso l'alto della pila.
Dalla pila OSI nasce successivamente il **modello TCP/IP**, che ne ricalca le teorie semplificandone la struttura e riducendo i livelli utilizzati da sette a quattro.



Non è scopo dell'articolo scendere nel dettaglio teorico del funzionamento delle reti, ma è di fondamentale importanza avere bene a mente **la struttura ISO/OSI** ed il **modello di rete TCP/IP**, in quanto **i firewall agiscono proprio a livelli o layer**.
I firewall sono dispositivi hardware e/o software che ci permettono di creare una barriera tra due o più reti.
Grazie a queste barriere definite "taglia fuoco" siamo in grado di tenere sotto controllo il traffico tra le due reti e creare politiche di sicurezza al fine di limitare alcuni tipi di comunicazione.
I motivi che ci portano ad utilizzare questa barriera possono essere molteplici, ma in definitiva si riassumono in un unico concetto: proteggere.
È un dato di fatto il crescente numero di attacchi verso reti e sistemi al fine di carpire dati, informazioni riservate, o peggio ancora DDos (Distribuited Denial of Service).

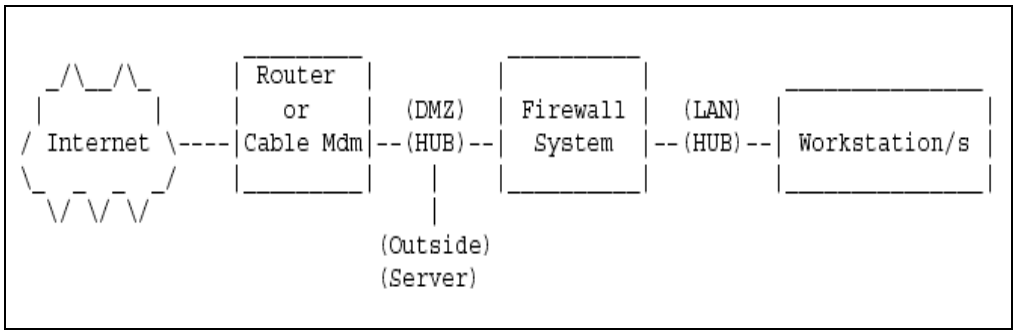
Alcuni tipi di firewall vengono anche utilizzati come **filtro verso informazioni ritenute dannose** (si pensi a determinati siti a cui i nostri figli non devono avere accesso) **o come ottimizzatori di reti** al fine di diminuire il traffico ridondante.

Vale sempre e comunque questo pensiero: se la rete che intendiamo amministrare non è in grado di reggere ad un possibile attacco o controllo completo da parte del suo amministratore, tanto vale non crearla per niente, in quanto quasi sicuramente non riusciremo e gestirla e ad offrire quei servizi che ci eravamo prefissati.
La figura sottostante presenta uno schema semplificato di divisione di reti attraverso il sistema di **firewalling**.



In questo articolo prenderò in considerazione **due reti che tra loro necessitano di una separazione**: **Internet** ed una **LAN**.
Con il termine **LAN**, nel nostro caso, si parla di **rete sicura**, e per **Internet** di **rete non sicura**, in quanto aperta a tutti.
Ovviamente l'utilizzo dei firewall non si limita a questo singolo esempio, ma essendo il più diffuso mi sembra giusto basarmi su questo schema.
Esistono **diversi tipi di firewall**, ognuno dei quali ha delle specifiche funzioni ed ovviamente pregi e difetti: in questo articolo esaminerò i **tre principali firewall**.

Il primo tipo di firewall è detto packet filtering e lavora **a livello di rete**.



Un **packet filter** esamina gli indirizzi Ip sorgente e destinazione del pacchetto e le porte coinvolte nella comunicazione.
Esso quindi considera **solo alcune informazioni che compongono il pacchetto**.
Successivamente attraverso un elenco di access control list (ACL) il firewall decide se accettare o scartare il pacchetto in questione.
Le regole di accesso permettono quindi al firewall di sapere quale pacchetto in ingresso e/o in uscita filtrare (accettare o rifiutare) ed anche di inibire l'utilizzo di alcuni servizi attraverso il controllo delle porte di comunicazione.
Per esempio posso creare la seguente regola: il pacchetto con indirizzo Ip sorgente 192.168.10.3 destinato ad un server esterno con indirizzo Ip 152.18.16.2 deve essere scartato nel caso in cui la richiesta avvenga per il servizio di invio e ricezione di posta, ovvero le porte Tcp ed Udp 25 e 110; tutte le altre comunicazioni sono accettate.

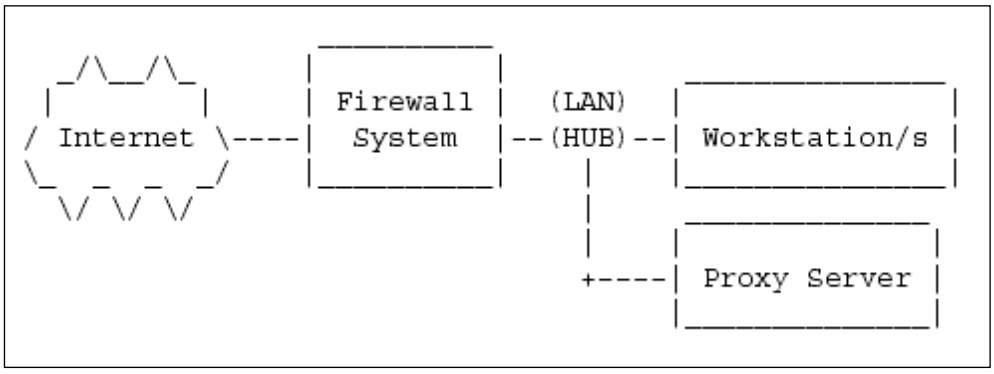
Oppure bloccare qualsiasi richiesta in ingresso da qualsiasi indirizzo Ip che fa capo alle porte Tcp ed Udp 137 e 139.
Il **packet filtering** è un sistema molto diffuso, che supporta ogni sistema operativo ed applicazione ed è estremamente veloce e di facile configurazione.

Purtroppo il suo metodo "semplice" di analisi del traffico e di filtraggio lo pone come sistema "discreto" di protezione. Il motivo è dovuto dal fatto che esso agisce a livello di rete, quindi analizza solo l'intestazione del pacchetto, senza sapere cosa esso effettivamente contiene.

L'altro **aspetto negativo del sistema a filtraggio di pacchetti** è che esso rende possibile ricostruire dall'esterno la topologia della nostra LAN; ogni computer usa il suo indirizzo Ip per comunicare con Internet: se n computer della nostra LAN accedono al medesimo server per il servizio di posta elettronica, il server ed il suo amministratore in brevissimo tempo potranno disegnare e sapere quali e quanti sistemi operativi e computer fanno parte della nostra rete.
Sempre in riferimento alla trasparenza di questo sistema c'è anche da dire che saremmo costretti a comperare Ip pubblici per ogni macchina che vuole collegarsi ad Internet, rendendo quindi onerosa in altri termini la nostra struttura.
Esistono infine in rete molti programmi che permettono di confezionare ad hoc pacchetti che al loro interno nascondono dati in grado di generare **buffer overflow** o **errori a livello di applicazioni e sistema operativo**; pensate cosa succederebbe se un malintenzionato sapesse anche uno solo degli indirizzi Ip che possono accedere alla vostra rete interna.

Possiamo porre quindi il **packet filter** come **sistema intermedio di protezione ma non sufficiente**.

Il secondo tipo viene identificato con il nome di **application gateway** o **proxy**.



Questo tipo di firewall agisce per procura e **si pone come intermediario delle comunicazioni in ingresso ed in uscita**.
Il **proxy** riceve la richiesta da un computer della rete interna ed effettua la richiesta sostituendo l'indirizzo Ip del pacchetto sorgente con il proprio. Successivamente invia il pacchetto verso l'esterno ed attende la risposta.
Il pacchetto di ritorno, una volta ottenute le credenziali per poter accedere alla LAN, passa attraverso il proxy e raggiunge la macchina locale da cui è partita la comunicazione.

Si nota subito che esso lavora ad un livello più alto del packet filter, tanto che viene anche chiamato **application proxy**.

Il primo evidente **pregio** è che il proxy nasconde ad Internet la topologia della nostra rete interna, facendo figurare come unico punto di accesso se stesso: questo sistema viene chiamato **NAT** (Network Address Translation) o **Ip masquerading**.
In pratica il NAT modifica l'indirizzo Ip nelle intestazioni dei pacchetti in uscita, ed attraverso un apposito registro memorizza le modifiche effettuate. Successivamente, quando avviene la risposta ad un pacchetto inviato, esso, analizzando il suo registro, lo re-indirizza alla macchina che in origine ha generato il pacchetto in uscita. In più esegue il controllo anche a livello di applicazione: se per esempio viene richiesta una sessione Ftp, il proxy si preoccupa anche di controllare che vengano inviati i comandi corretti per tale comunicazione e che le risposte siano altrettanto corrette.

Infine esegue un log estremamente accurato che ci permette di conoscere ogni minimo movimento da e verso la LAN.

I **difetti** sono anch'essi evidenti: per prima cosa **richiede un'elaborazione dei dati maggiore** che incide quindi sulla velocità del firewall stesso di processare ogni singola comunicazione e pacchetto.
Risulta **non trasparente come il packet filter**: ogni applicazione su ogni client dovrà essere settata per lavorare con il nostro proxy, rendendo di fatto la manutenzione non semplice.

Per ogni tipo di applicazione il proxy deve essere in grado di svolgere le funzioni dell'applicazione in questione: in sostanza deve esistere un procuratore per ogni tipo di applicazione che necessita di comunicare attraverso la rete.

Come evoluzione successiva esiste **un terzo tipo di firewall** chiamato **stateful inspection**.
Il suo ingresso si è reso necessario come **compromesso tra sicurezza e velocità**.
Esso lavora a livello di pacchetti non analizzandoli singolarmente, ma prendendo come insieme la comunicazione completa.

Per comprendere meglio il suo funzionamento, basta un semplice paragone con il sistema del **packet filter**: il filtraggio esamina singolarmente il pacchetto e decide se deve essere scartato o meno; lo **stateful inspection** invece **controlla anche lo stato della comunicazione** scartando per esempio pacchetti di risposta a richieste mai avvenute.
Esso si pone quindi come **livello intermedio tra il packet filter ed il proxy** (livello di rete e livello di applicazioni)**.**

Il **difetto** è che questo sistema **non permette di autenticare gli utenti**, ma se il suo utilizzo avviene in reti domestiche e non aziendali, questo particolare risulta ininfluente.

La realtà è ben diversa dalla teoria e questo articolo è solo un preludio ad un mondo estremamente delicato e complesso.

Non basta conoscere il funzionamento di un firewall per diventare dei "maestri" di sicurezza. Saper configurare una rete affinché la possibilità di intrusioni ed attacchi ricadano in una scala di minima eventualità richiede molte prove e molti attacchi subiti.

Infine bisogna saper leggere i log dei nostri sistemi e **rendersi conto di cosa si vuole proteggere**.
Come valore principale vale sempre la consapevolezza di ciò che si vuole proteggere e cosa si vuole offrire.

Per chi volesse approfondire la materia vi consiglio le seguenti letture:

Building Internet Firewalls
di *D. Brent Chapman* e *Elizabeth D. Zwicky*
http://www.oreilly.com/catalog/fire

Firewall and proxy server How-To
di *Mark Grennan*
http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/Firewall-HOWTO.html

TCP/IP Tutorial and Technical Overview
di *Adolfo Rodriguez*, *John Gatrell*, *John Karas* e *Roland Peschke*
http://www.ibm.com/redbooks

Roberto Del Bianco

Porta Zero

http://www.portazero.info/modules.php?name=Sections&sop=viewarticle&artid=56