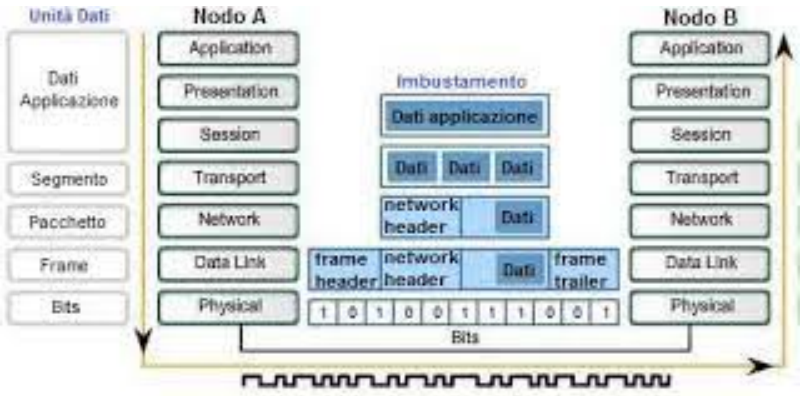
Packet Filter e Application Proxy

Modello OSI



Concetto di regola.

Una regola è una legge che stabilisce se un determinato pacchetto può attraversare o meno il firewall. In pratica un firewall è un insieme di regole che vengono applicate ai pacchetti.

Possiamo distinguere **2 tipi fondamentali di firewall**:

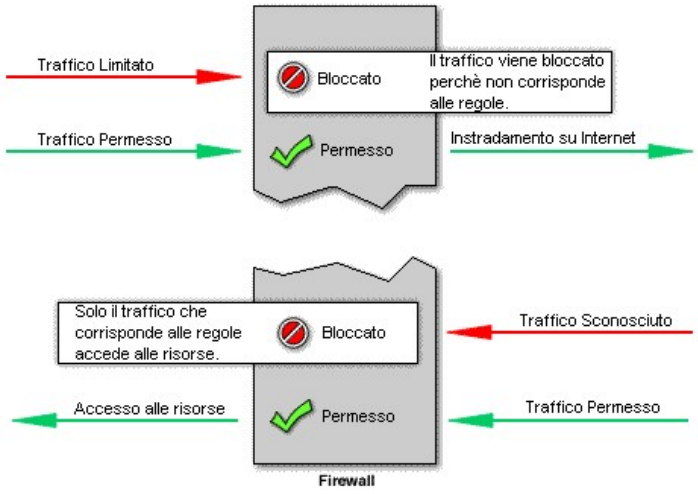
Packet Filter Firewall
Application Proxy Firewall

Packet Filter

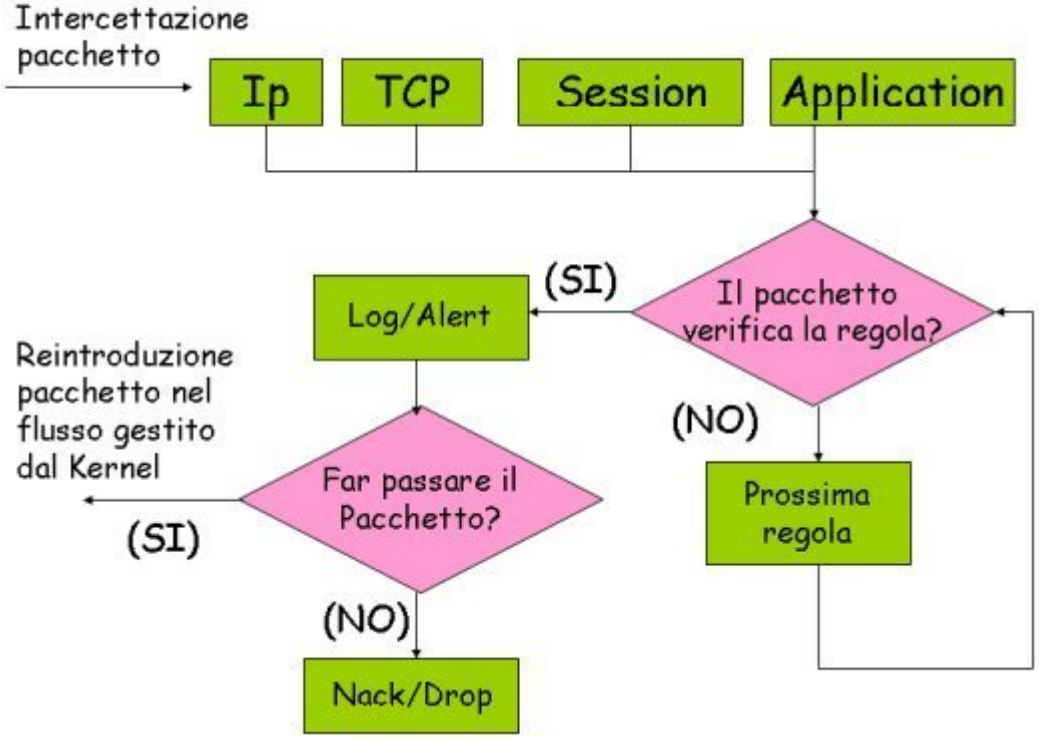
Il Packet Filter o filtro dei pacchetti, altro non è che una parte di software che guarda le intestazioni (header) dei pacchetti decidendone il destino. Risiede nel livello di rete del modello OSI. Può decidere di

- scartare (deny) il pacchetto,
- accettarlo (accept),
- scartarlo dando una notifica al mittente (reject);

tutto ciò sempre in accordo con le regole definite dall'amministratore. Se un pacchetto ottiene il permesso viene instradato direttamente a destinazione.



Da sempre implementati sui routers si occupano di filtrare il contenuto dei pacchetti in transito basandosi sugli indirizzi IP (livello di rete) e sulle porte (livello di trasporto) sorgente e destinazione, il che vuol dire che sono del tutto indipendenti dall'applicazione. Tutto ciò comporta da un lato che i Packet Filter abbiano ottime prestazioni e dall'altro l'inconveniente relativo al non controllo del contenuto del pacchetto, ovvero la parte attinente ai dati, che viene ignorata. I firewall che fanno uso di tale tipo di tecnologia lavorano al livello di rete (livello 3) e sono più veloci dei proxy firewalls. Ora si va più in dettaglio per capire meglio come funziona un Packet Filter:



Da questo schema di può vedere tutto il cammino che segue un pacchetto che arriva all'interfaccia di rete del sistema. Arrivato nel livello di rete si verifica se il pacchetto soddisfa la prima regola:

1) se la verifica ha successo si fa un log di sistema e in base a quanto stabilito dalla regola si decide se farlo passare oppure no;
2) se la verifica non ha successo allora si prosegue nella lista delle regole prendendo la successiva e testando se viene verificata; e così via.

Ci sono packet filter più evoluti che controllano anche alcune parti del quarto livello (trasporto). In conclusione il packet filter risulta essere funzionale e trasparente ma ha alcune limitazioni.

Application Proxy

Gli Application Proxy, detti anche "Application Gateway", implementano il concetto di firewalling a livello 7 (applicazione), aumentando di conseguenza il livello di sicurezza.
L'esame di tale livello consente di sfruttare la conoscenza del contesto della comunicazione nell'ambito del processo decisionale operato dal firewall. D'altro canto la realizzazione di un Application Proxy implica il sezionamento del modello di comunicazione client-server.

Infatti ogni comunicazione di questo tipo richiede due connessioni:

1. una dal client al firewall e
2. l'altra dal firewall al server.

Tutto questo provoca una drastica diminuzione delle prestazioni di tale architettura.

Infine l'utente è costretto a configurare il proprio client per l'utilizzo del Proxy con una notevole mancanza di trasparenza.
Un altro inconveniente di tale tipo di architettura è che per ogni servizio che necessita di passare attraverso **il firewall che utilizza questa tecnologia c'è bisogno di un Proxy dedicato** (uno per l'FTP, un altro per il web e così via dicendo).
Il firewall proxy garantisce oppure blocca gli accessi tenendo conto di regole predefinite. Tali regole possono essere basate su indirizzi IP, protocolli, porte.
Il proxy server connette la macchina richiedente la connessione con quella di destinazione gestendo il trasferimento dei dati da una macchina all'altra.

Vantaggi

Packet Filter	Application Proxy
Basso utilizzo di risorse	Buon livello di sicurezza
Trasparente all'utente	Uso del livello applicazione
Buone Prestazioni	

Svantaggi

Packet Filter	Application Proxy
Basso livello di sicurezza	Proxy dedicato per ogni servizio
Accesso limitato all'header IP	Basse Prestazioni
Poca manipolazione informazioni	Vulnerabile a bug delle applicazioni