Firewall

Il firewall è una linea di difesa che filtra tutti i pacchetti sia in entrata che in uscita da una rete, secondo regole prestabilite che contribuiscono alla sicurezza della rete stessa. Questo si può comunemente realizzare tramite un PC, l'apposito software e le Access Control List che servono per configurarlo. I firewall si possono distinguere in 3 categorie in base al livello dello stack TCP/IP in cui operano:

- Application Level Firewall: intercetta le trasmissioni a livello Application valutando il contenuto applicativo dei pacchetti, come i Proxy;
- Packet Filter Firewall: lavora a livello Network e Transport, è più veloce dell'Application perché controlla solo l'header;
- Stateful Packet Inspection Firewall: agisce solo a livello Transport, controlla e analizza tutto il pacchetto dati, compila una tabella con lo stato delle connessioni;

ACL

L'Access Control List o ACL è un insieme di istruzioni da applicare alle interfacce di un router allo scopo di gestire il traffico. Le ACL forniscono un livello base di sicurezza, aumentano le performance della rete e stabiliscono quali tipi di traffico possono essere trasmessi.

Le ACL vengono elaborate in ordine, e appena una condizione è soddisfatta il pacchetto viene eliminato o inoltrato. L'ultima istruzione di ogni ACL è una negazione implicita 'deny ip any any'.

Le ACL si applicano specificando la direzione (in ingresso o uscita):

- Ingresso: traffico che arriva al router prima della tabella di routing;
- Uscita: traffico già elaborato per l'inoltro;

Tipi di ACL:

- Standard ACL (1-99): controllano solo l’indirizzo IP sorgente;
- Extended ACL (100-199): controllano indirizzi sorgente/destinazione, protocolli TCP/UDP, numeri di porta;

ACL possono essere:

- Numbered: identificativo numerico;
- Named: identificativo con nome;

Ogni router può avere una ACL per ogni protocollo, interfaccia logica e direzione.

Posizionamento:

- Extended ACL: vicino alla sorgente;
- Standard ACL: vicino alla destinazione;

Configurazione di ACL standard numeriche

```
Router(config)#access-list numero_ACL deny|permit ip_sorgente maschera_wildcard
```

Configurazione di ACL extended numeriche

```
Router(config)#access-list numero_ACL [deny|permit] protocollo ip-sorgente wildcard ip-destinazione wildcard
condizione
```

Configurazione di ACL standard con nome

```
Router(config)#ip access-list standard nome_ACL
```

```
Router(config-std-nacl)# [deny|permit] ip-sorgente
```

Configurazione di ACL extended con nome

```
Router(config)#ip access-list extended nome-ACL
Router(config-ext-nacl)# deny|permit protocollo ip_sorgente wildcard_mask ip_destinazione wildcard_mask condizione
```

Proxy

Un proxy è un programma che si interpone tra client e server. Riceve la richiesta dal client, la inoltra al server e poi ritorna la risposta al client. Lavora a livello Application e utilizza tecniche come NAT e PAT. Collocato vicino al client, migliora le prestazioni e riduce il consumo di banda.

Funzioni principali:

- Connettività;
- Privacy;
- Caching;
- Monitoraggio;
- Amministrazione;
- Filtraggio;
- Restrizioni (DMZ);

Topologie di utilizzo:

- Single Proxy Topology: un solo proxy per tutta la rete;
- Multiple Proxy Vertically Topology: proxy secondari si collegano a uno primario;
- Multiple Proxy Horizontally Topology: bilancia il carico tra proxy di pari livello;

NAT e PAT

NAT (Network Address Translation) è una tecnica con cui il router sostituisce l'indirizzo IP del pacchetto. Permette a reti private con indirizzi locali di accedere a Internet tramite un unico IP pubblico.

Vantaggi del NAT:

- Riduce il numero di IP pubblici necessari;
- Mantiene la configurazione degli host;
- Offre sicurezza e flessibilità;

Tipi di NAT:

- Static NAT: un solo IP pubblico usato per tutte le connessioni
- Dynamic NAT: scelta dinamica di un IP pubblico tra un insieme disponibile
- PAT (Port Address Translation): utilizza un solo IP pubblico con porte diverse

NAT in IPv6:

- Dual-stack: doppio stack IP per supportare IPv4 e IPv6;
- Conversion: traduzione tramite NAT-PT;
- Tunneling: incapsulamento IPv6 in IPv4;

Tipi di tunneling:

- 4to6: pacchetti IPv6 incapsulati in IPv4;
- 6to6: tunnel IPv6 attraverso rete IPv4, usato in reti locali;

Il PAT permette di usare un solo IP pubblico per oltre 64.000 connessioni private. Cambia la porta, mantenendo lo stesso IP.

DeMilitarized Zone

Per migliorare la sicurezza, le reti si dividono in zone:

- Zona LAN: rete privata interna;
- Zona WAN: parte esterna collegata a Internet;

DMZ (DeMilitarized Zone) è una terza zona che separa LAN e WAN, limitando il traffico tra loro. Usata per pubblicare servizi all'esterno (SMTP, Webmail, Application Server) senza esporre la LAN.

Tipi di DMZ:

- Vicolo cieco: un firewall con tre interfacce (LAN, WAN, DMZ);
- Zona cuscinetto: due firewall, uno tra WAN e DMZ, l'altro tra DMZ e LAN;