FIREWALL

Separa la LAN aziendale dalla WAN filtrando i pacchetti con delle regole (policy)
La sicurezza di tutta la rete connessa ad Internet viene ricondotta alla sicurezza di un ristrettissimo numero di nodi, molto spesso solamente 1.

- Può essere realizzato con un PC (2 schede di rete in/out + software apposito)
- Nelle reti aziendali può essere incluso nel router o su hardware dedicato

Caratteristiche:

- Strumento efficace per la sicurezza delle reti
- Presenza di meccanismi per il controllo degli accessi
- Possibilità di gestire le regole per la sicurezza
- Configurazione di filtri per l'accesso dei computer di una rete ad Internet
- Protezione da attacchi (ARP spoofing, port scanning, DoS, SQL slammer)

Si possono distinguere in **3 categorie in base al livello TCP/IP** in cui operano:

- **Application Level Firewall**
- **Packet Filter Firewall**
- **Stateful Packet Inspection Firewall**

Application Level Firewall (+ protezione, - prestazioni)

- Intercetta le trasmissioni a livello Application (contenuto del pacchetto)
- Es. blocca i virus noti in una sessione HTTP o SMTP
- A questa categoria appartengono i **proxy** (che fa da tramite tra LAN e WAN)

Packet Filter Firewall (- protezione, + prestazioni)

- Intercetta le trasmissioni a livello Network (header del pacchetto)
- Es. una mail contenente virus può passare se è abilitato il traffico POP/SMTP
- I parametri che controlla sono:
  - IP di origine e di destinazione
  - Numero della porta TCP/UDP di origine e di destinazione)
  - Il protocollo di livello superiore usato

Stateful Packet Inspection Firewall (- protezione, + prestazioni)

- Intercetta le trasmissioni a livello Transport (analizza header e contenuto)
- Può controllare lo stato della connessione TCP e compilare le informazioni

ACL (Access Control List)

Le ACL permettono di esprimere delle **regole** che determinano o meno l'accesso ad alcune risorse, vengono modificate da parte dell'amministratore

- **white list** → indirizzi verso cui è consentito il transito dei dati (blocco altri)
- **black list** → indirizzi verso cui è bloccato il transito dei dati (consentito altri)

Le ragioni per adoperare le ACL sono:

- Fornire un livello base di sicurezza (restringere gli accessi ad una rete)
- Limitare il traffico
- Aumentare le prestazioni (alcuni pacchetti vengano processati prima di altri)
- Decidere quale tipo di traffico può essere trasmesso

Il router-firewall elabora le ACL in modo sequenziale → le + restrittive vanno prima
Appena un pacchetto soddisfa una delle condizioni la valutazione si interrompe
Il pacchetto viene quindi inoltrato o scartato a seconda dell'istruzione eseguita
Se il pacchetto non soddisfa nessuna condizione viene scartato (l'ultima è "deny all")

Esistono 2 tipologie di ACL:

- **Standard (1-99)**
  - Guardano l’indirizzo della sorgente
  - Vanno collocate vicine alla destinazione
- **Extended (100-199)**
  - Limitazioni ai pacchetti (protocollo, IP sorgente, IP destinazione, porta)