

**Ragionamento**

Il Firewall perimetrale si trova tra la WAN (in questo caso internet) e la LAN.

IL Firewall controlla così il traffico in entrata ed in uscita.

Collegata al Firewall, si trova la DMZ, zona demilitarizzata, una zona raggiungibile da chiunque dall’esterno. Questa zona ci serve per poter far raggiungere il server di servizi web (HTTP) e il server di servizi mail (SMTP). La DMZ è protetta dal WAF (Web Application Firewall) che filtra i contenuti dei pacchetti che riceve, attraverso il confronto della sua tabella con una tabella di terzi parti. Per esempio confronta il contenuto del pacchetto con i server di OWASP per capire se ci sono malware nel pacchetto.

Prima di arrivare ai due server, i dati passano anche per l’IPS (Intrusion protection system). L’IPS legge i pacchetti che arrivano e se c’è qualcosa che non va, non solo fa scattare l’allarme per dei problemi ma blocca anche il pacchetto incriminato, proteggendo i server. L’ho posizionato qui perché IPS può controllare meglio l’enorme quantità di flussi e di pacchetti in entrata ed uscita verso server nella DMZ.

Al Firewall sono collegati altri due switch: uno di questi è collegato ai dispositivi dell’azienda che utilizza per lavorare, l’altro è collegato all’IDS e al NAS. Il NAS (Network Access Storage) è il cuore dell’azienda: custodisce tutti i file più sensibili e importanti dell’azienda sugli HDD e SSD ad esso collegati.

Va da sé che è di vitale importanza tenerlo monitorato e al sicuro.

L’IDS (Intrusion detection system) serve a leggere i pacchetti in entrata ed uscita e ci avverte come un allarme se c’è un malware o un intruso in uno dei pacchetti.

A questo punto posso intervenire per capire quale sia il problema.

Non ho collegato l’IPS al NAS perché potrebbe bloccare lo sharing dei file con dei falsi positivi, impedendo il flusso di dati nella LAN e ostacolando così il lavoro.

Con l’IDS collegato al NAS, ho maggiore controllo. Ed avendo anche il Firewall che filtra dinamicamente ciò che il NAS può ricevere, con l’IDS ho una seconda rete di difesa per questo dispositivo assolutamente vitale per l’azienda.