**Relazione: Analisi di un Firewall Perimetrale, DMZ e Sistemi IDS/IPS**

**Cos'è un Firewall:**

Un **firewall** è un sistema di sicurezza informatica progettato per monitorare e controllare il traffico di rete, sia in uscita che in entrata, proteggendo reti e dispositivi da accessi non autorizzati, intrusioni o attacchi informatici. Funziona come una barriera che filtra il traffico sulla base di regole predefinite, consentendo o bloccando determinate comunicazioni.

**Tipi di Firewall:**

1. **Firewall hardware**: Sono dispositivi fisici che proteggono l’intera rete e sono generalmente usati in grandi organizzazioni per gestire un traffico di rete più complesso.
2. **Firewall software**: Sono programmi installati su singoli dispositivi (computer, server) per proteggerli da minacce. Sono più comuni in ambienti domestici o in piccole aziende.

I firewall possono essere classificati in due categorie principali:

* **Firewall perimetrali**: Installati al confine tra reti, come la WLAN e la LAN, per proteggere l’intera rete aziendale dalle minacce esterne.
* **Firewall non perimetrali**: Posizionati all'interno della rete LAN o WLAN, proteggono sezioni più specifiche della rete interna.

**Firewall Perimetrale:**

Nel compito di oggi, analizziamo un **firewall perimetrale** con l’uso di una **DMZ** e di sistemi **IDS/IPS**. Un firewall perimetrale è installato tra una rete interna (ad esempio, aziendale) e una rete esterna, come Internet. Il suo ruolo è quello di agire come una barriera che regola il traffico in entrata e in uscita, proteggendo la rete interna da minacce come virus, malware o tentativi di hacking. Le regole di accesso vengono stabilite in modo da consentire solo il traffico legittimo e bloccare eventuali tentativi di intrusione.

**La DMZ (Demilitarized Zone):**

La **DMZ** è una zona di sicurezza intermedia tra la rete interna e l’esterno (di solito Internet), progettata per esporre servizi pubblici senza compromettere la sicurezza della rete interna. Nel nostro scenario, abbiamo utilizzato:

* Un **server web (HTTP)** per gestire il traffico Internet.
* Un **server di posta elettronica (SMTP)** per la gestione delle email.

La DMZ permette di isolare i servizi accessibili dall’esterno (come il web server o il server email), riducendo i rischi di attacchi diretti ai sistemi interni più sensibili, come il server di dati o il NAS all'interno della rete aziendale.

**NAS (Network Attached Storage):**

All’interno della **rete interna**, abbiamo inserito un **NAS**. Si tratta di un dispositivo di archiviazione di rete che consente di salvare e accedere ai file da diversi dispositivi connessi. Nel contesto di una rete con una DMZ, il NAS viene tipicamente collocato nella rete interna, poiché contiene dati sensibili e privati che devono essere protetti da accessi esterni non autorizzati.

**IDS (Intrusion Detection System) e IPS (Intrusion Prevention System):**

Infine, abbiamo introdotto due tipi di sistemi di sicurezza nella rete interna: **IDS** e **IPS**.

* **IDS (Intrusion Detection System)**: Un IDS è un sistema passivo che analizza il traffico in tempo reale o i file di log storici alla ricerca di attività sospette o comportamenti anomali. Se rileva traffico sospetto, genera un allarme e notifica l’amministratore di rete. Può essere posizionato sia nella rete interna che nella DMZ per monitorare entrambe le aree.
* **IPS (Intrusion Prevention System)**: Un IPS, invece, è un sistema attivo che non solo rileva gli attacchi, ma li blocca in tempo reale, impedendo che traffico malevolo danneggi la rete. Viene spesso installato tra la rete Internet e la DMZ, o tra la DMZ e la rete interna. Se rileva un attacco (come un attacco DDoS), l’IPS blocca immediatamente il traffico sospetto prima che possa raggiungere il server o i dispositivi interni.

**Conclusione:**

Il firewall perimetrale, la DMZ e i sistemi IDS/IPS offrono un approccio multilivello alla sicurezza di rete, garantendo protezione sia a livello di rete esterna che interna. L’uso della DMZ limita l’esposizione della rete interna a minacce esterne, mentre IDS e IPS monitorano e prevengono potenziali attacchi in modo tempestivo, contribuendo a proteggere dati sensibili e servizi critici.

