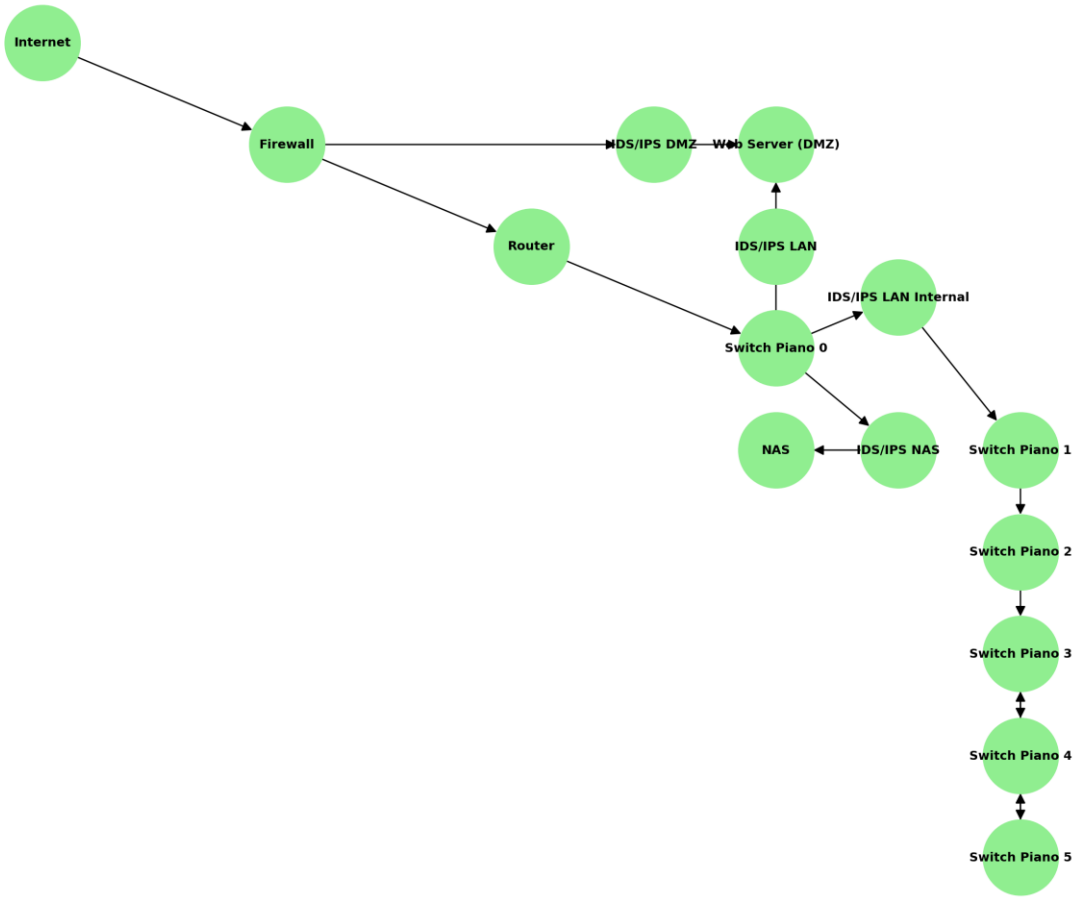
Relazione sulla Configurazione del Firewall, IDS e IPS

"Benvenuto. Ogni elemento della rete è il risultato di un preciso calcolo. Nulla è lasciato al caso." Proprio come l'Architetto ha modellato la Matrice, anche la nostra infrastruttura è stata progettata per garantire sicurezza, controllo e resilienza attraverso firewall, IDS e IPS ben posizionati.



Configurazione del Firewall

"Causa ed effetto, azione e reazione."

Il firewall è il primo guardiano, posto tra il Router e Internet, e gestisce ogni connessione in entrata e in uscita:

Regole di accesso in entrata:

Permessi:

HTTP (porta 80) e HTTPS (porta 443) verso il Web Server nella DMZ.

SSH (porta 22) accessibile solo dalla VLAN Management (VLAN 99).

Blocchi:

Traffico diretto alla LAN e al NAS.

Regole di accesso in uscita:

Consenti:

Accesso a Internet solo per VLAN autorizzate.

Blocca:

IP sospetti rilevati tramite liste di reputazione.

Policy di Default:

"Deny All." Tutto ciò che non è esplicitamente autorizzato è negato.

Configurazione degli IPS (Intrusion Prevention System)

"Tutto ciò che ha un inizio ha una fine. E la fine è sotto il nostro controllo."
Tre IPS sono posizionati strategicamente per bloccare attivamente ogni minaccia rilevata:

IPS DMZ:

Collocato tra il firewall e il Web Server.

Regole principali:

Blocca attacchi specifici: SQL Injection, XSS, brute force.

Rileva accessi non autorizzati.

Prevenzione di scansioni di porta.

IPS NAS:

Posizionato tra lo Switch Piano 0 e il NAS.

Regole principali:

Blocca caricamenti sospetti, come file eseguibili non previsti.

Rileva attività ransomware, come modifiche massicce ai file.

Previene accessi brute force al NAS.

IPS VLAN Aziendale:

Collocato tra la VLAN aziendale principale e il Router.

Regole principali:

Analizza traffico verso Internet per bloccare esfiltrazione di dati.

Rileva tentativi di attacco da botnet o comunicazioni con C2 server.

Configurazione degli IDS (Intrusion Detection System)

"Non è solo una rete. È un sistema pensato per monitorare, rilevare e imparare."
Tre IDS sono stati configurati per garantire una panoramica completa e generare allarmi su ogni anomalia.

IDS LAN:

Posizionato tra il Router e lo Switch Piano 0.

Regole principali:

Rileva attacchi DoS (numero eccessivo di pacchetti).

Segnala scansioni di rete o tentativi di mappatura delle VLAN.

IDS VLAN Interne:

Tra Switch Piano 0 e altri switch aziendali.

Regole principali:

Rileva comunicazioni anomale tra VLAN.

Monitora malware interno generato da dispositivi compromessi.

IDS DMZ:

Collocato tra il Web Server e Internet.

Regole principali:

Segnala tentativi di attacco falliti alla DMZ.

Monitora attività sospette sul Web Server, come comportamenti non previsti delle sessioni attive.

Segmentazione della Rete

"La rete è una mappa. E come ogni mappa, è suddivisa in aree di controllo."

Le VLAN garantiscono un isolamento rigoroso tra i segmenti, rafforzando il controllo e la sicurezza:

DMZ: Isolata dal resto della rete, comunica unicamente con Internet.

VLAN aziendali: Accesso ristretto a risorse specifiche.

VLAN Management: L'unico segmento con accesso amministrativo globale.

Considerazioni Finali

"Scelte, intuizioni, sistemi: tutto è perfettamente bilanciato."
Questa configurazione offre:

Massima Sicurezza: Firewall, IPS e IDS lavorano in sinergia per proteggere ogni segmento della rete.

Monitoraggio Continuo: Gli IDS garantiscono un’analisi proattiva e allarmi tempestivi.

Isolamento: VLAN e DMZ separano risorse critiche per evitare movimenti laterali non autorizzati.

"La perfezione è un’illusione. Ma con questa configurazione, ci avviciniamo molto."