

Progetto di Infrastruttura – Compagnia Theta

1. Analisi dei Requisiti

Il progetto risponde alle esigenze della compagnia Theta di implementare un'infrastruttura IT moderna e resiliente distribuita su **6 piani**, per un totale di **120 utenti** (20 per piano). I requisiti tecnici e di sicurezza stabiliti includono:

- **Segmentazione e automazione:** Utilizzo di VLAN per ogni piano e di un **Server DHCP dedicato** per la gestione centralizzata e l'assegnazione dinamica degli indirizzi IP ai 120 host.
- **Esposizione Servizi:** Configurazione di un **Web Server pubblico (DVWA)** accessibile dall'esterno in totale sicurezza.
- **Protezione Dati:** Protezione rigorosa di un **NAS aziendale** contenente dati sensibili.
- **Difesa Perimetrale e Interna:** Implementazione di **due Firewall** per creare zone di sicurezza distinte (Outside, DMZ, Inside).
- **Monitoraggio:** Controllo costante del traffico tramite **3 sistemi IDS/IPS** posizionati nei punti nevralgici della rete.

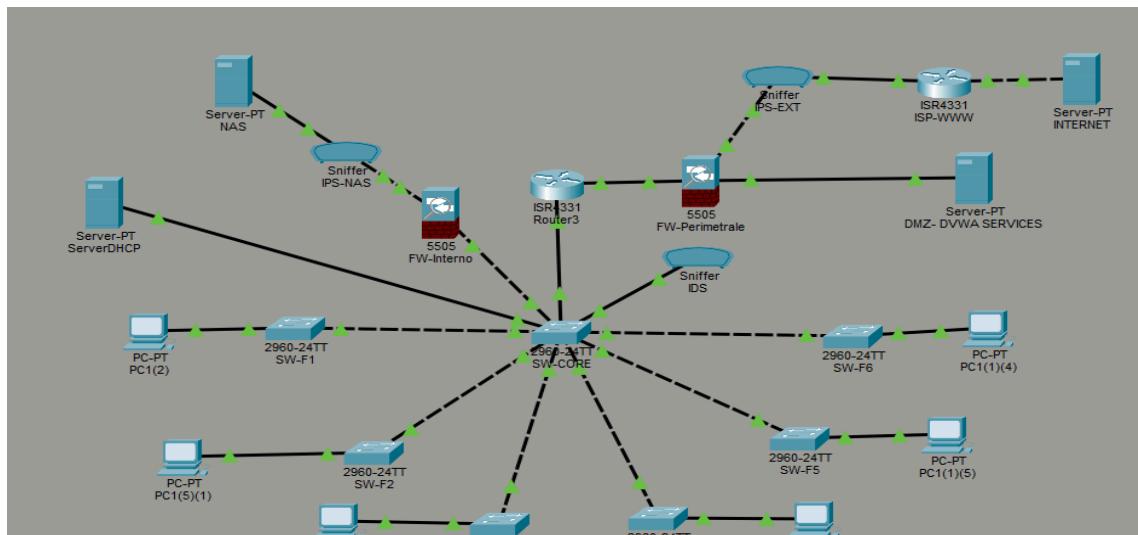
2. Architettura Fisica e Modello Gerarchico

La rete segue il **Modello Gerarchico Cisco**, garantendo scalabilità e gestione semplificata dei guasti:

Access Layer (Livello di Accesso): Composto da 6 switch (uno per piano), ai quali sono collegati i 120 computer totali tramite cavi in rame.

Core Layer (Centro Stella): Uno switch centrale (Core Switch) che aggredisce il traffico di tutti i piani e fornisce connettività verso i server critici e i sistemi di sicurezza.

3. Topologia



4. Segmentazione Logica e Gestione DHCP

Per ottimizzare le prestazioni e la sicurezza interna, la rete è segmentata logicamente:

Creazione VLAN: Abbiamo implementato VLAN dedicate per ogni piano (es. VLAN 10 per il piano 1, VLAN 20 per il piano 2, ecc.). Questo isola il traffico broadcast tra i diversi piani dell'edificio.

Routing Inter-VLAN: Il traffico tra le VLAN è gestito dal router centrale tramite la configurazione di **sub-interfaces**, che fungono da gateway per ogni piano.

DHCP Centralizzato: L'assegnazione automatica degli indirizzi IP è affidata a un **Server**

DHCP dedicato collegato al Core Switch. Grazie al comando **ip helper-address** configurato sul router, il server è in grado di distribuire gli indirizzi IP a tutti i 120 host suddivisi nelle varie VLAN.

VLAN No				
1	default	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	DHCP request successful.
10	FLOOR1	IPv4 Address	192.168.20.18	
20	FLOOR2	Subnet Mask	255.255.255.0	
30	FLOOR3	Default Gateway	192.168.20.1	
40	FLOOR4			
50	FLOOR5			
60	FLOOR6			
70	NAS			
80	MGMT			
90	IDS_IPS			
100	DMZ			

5. Sicurezza Perimetrale e Zona DMZ

La connessione verso l'esterno è protetta da una configurazione a doppia barriera:

Firewall Perimetrale : Gestisce l'uscita verso Internet e applica il **NAT (Network Address Translation)** per mascherare gli IP privati della rete interna.

Zona Demilitarizzata (DMZ): Come richiesto, il **Web Server (DVWA)** è posizionato in una DMZ collegata direttamente al Firewall Perimetrale. Questa zona è isolata dalla rete interna, garantendo che un eventuale attacco al server web non comprometta i PC dei dipendenti o il NAS.

6. Protezione dei Dati e Monitoraggio (IDS/IPS)

Il cuore della sicurezza è focalizzato sulla protezione dello storage aziendale (NAS).

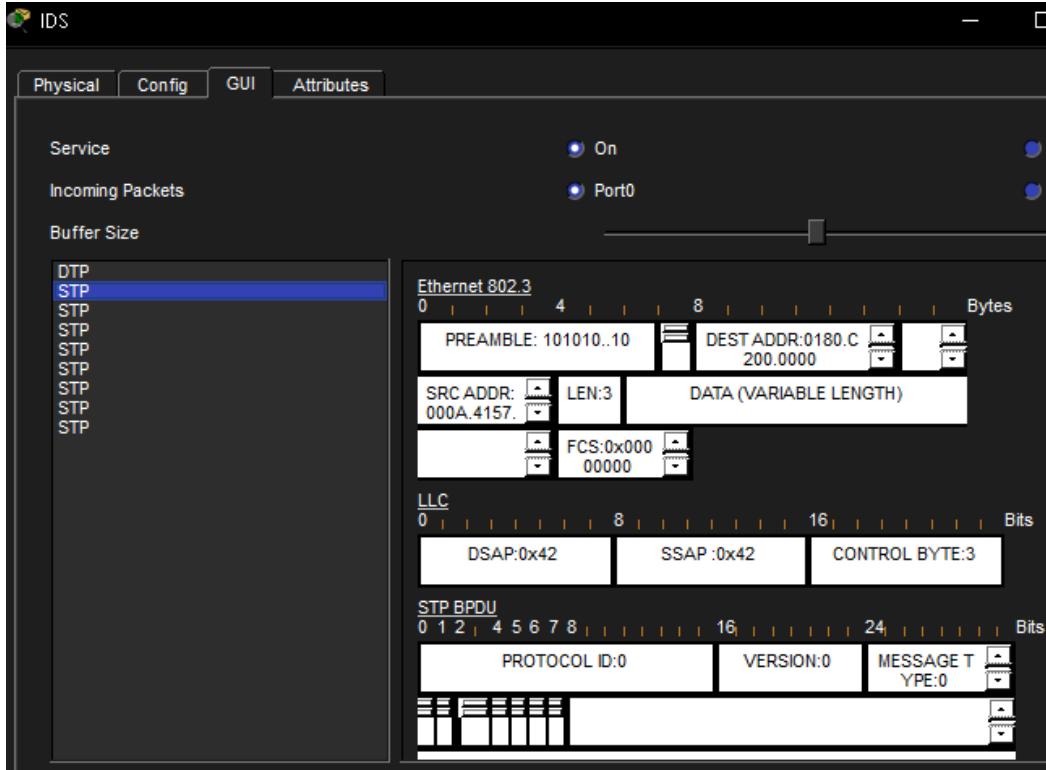
Firewall Interno: protegge l'accesso al **NAS**, filtrando le connessioni provenienti dai PC degli utenti e dalla DMZ.

Sistemi IDS/IPS (3 Dispositivi): Come da specifica, sono stati implementati tre sistemi di monitoraggio tramite Sniffer:

1.Sniffer IPS-EXT: Posizionato sul link tra Router ISP e Firewall Perimetrale per rilevare intrusioni esterne.

2.Sniffer IPS-NAS: Posizionato tra il firewall interno e il NAS per una protezione dedicata dello storage.

3.Sniffer IDS: Collegato allo switch centrale per il monitoraggio del traffico interno tra i 6 piani.



7. Conclusioni

L'infrastruttura Theta combina la segmentazione logica (VLAN/DHCP) con una strategia di difesa in profondità. L'uso integrato di firewall e 3 sistemi IDS/IPS garantisce che sia il Web Server pubblico che il NAS interno siano protetti secondo i più alti standard di sicurezza richiesti.