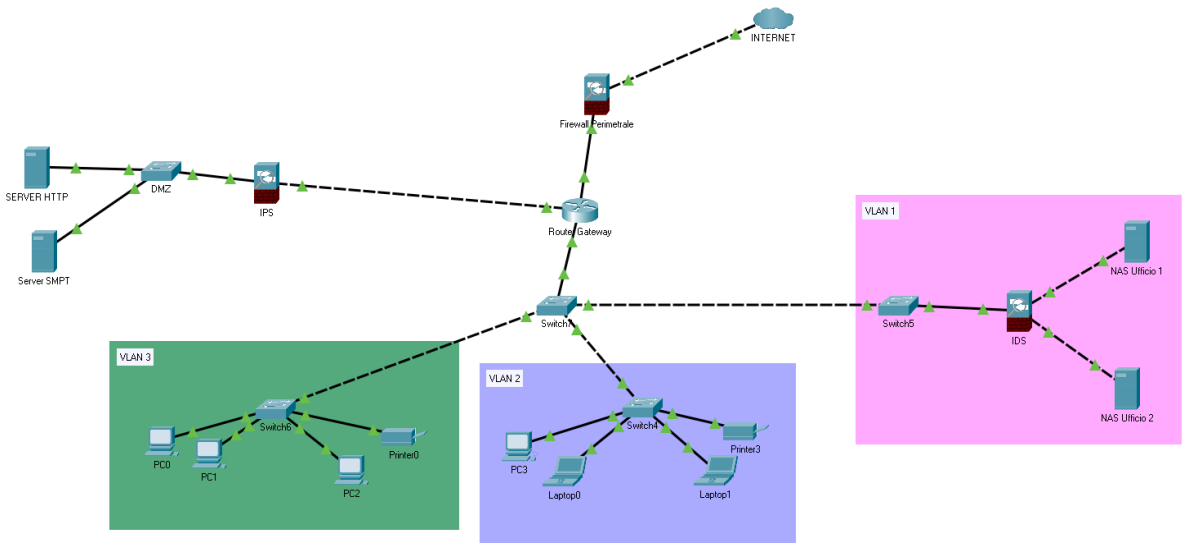
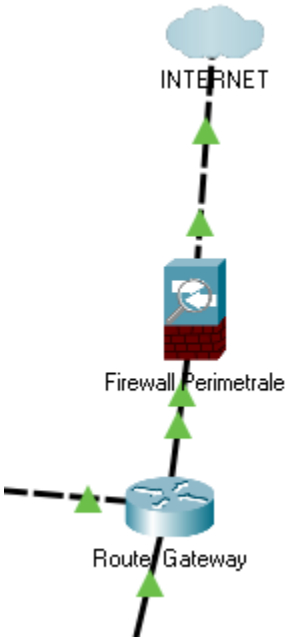
S3 - L5 - Progetto

L’esercizio prevede la segmentazione di una rete con i seguenti elementi: firewall perimetrale, zona DMZ con Server HTTP e SMPT, rete interna con server NAS.

Di seguito la rete completa:



1 INTERNET

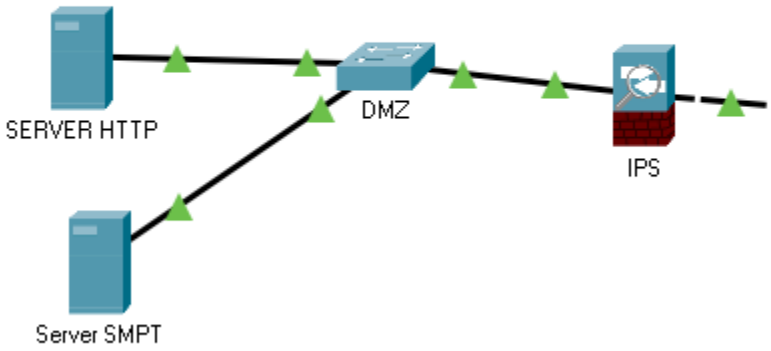


Nell'immagine sopra possiamo vedere il **Firewall perimetrale**, posizionato tra il punto di accesso esterno (internet) e il Router Gateway. Il Firewall perimetrale ha la funzione di filtraggio del traffico in entrata e uscita dalla rete interna proteggendola da eventuali attacchi esterni.

Parlando di filtraggio, possiamo elencare tre metodi diversi:
Filtraggio Statico - filtra i pacchetti in base a parametri come l'IP e le porte.
Filtraggio Dinamico - blocca automaticamente tutte le comunicazioni che arrivano dall'esterno permettendo quelle dall'interno all'esterno, salvando le connessioni nella memoria cache.
WAF - è a difesa dei servizi web, filtra per contenuto i pacchetti attraverso la verifica
Proxy -

In questo caso il Router Gateway collegato al Firewall perimetrale indirizza il traffico della rete interna instradando i pacchetti tra i vari dispositivi e tra le VLAN.

2 DMZ



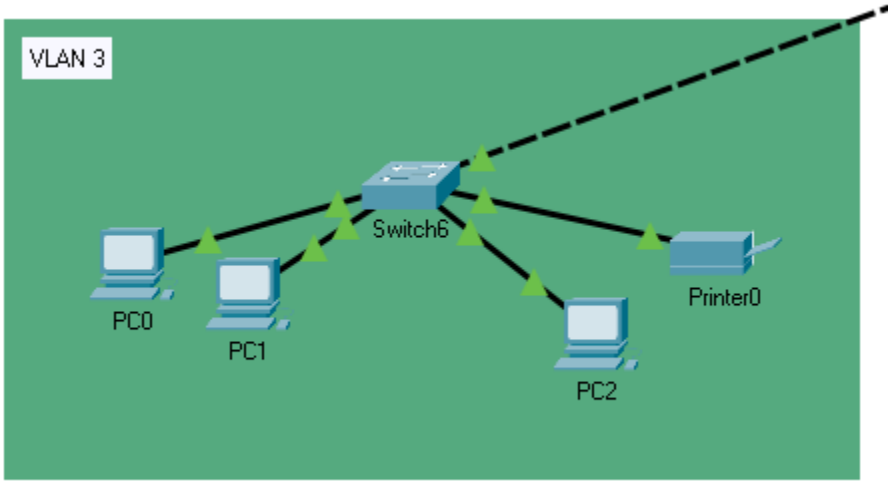
Nell'immagine sopra abbiamo creato una DMZ alla quale sono collegati due server: rispettivamente HTTP e Server di posta SMPT.

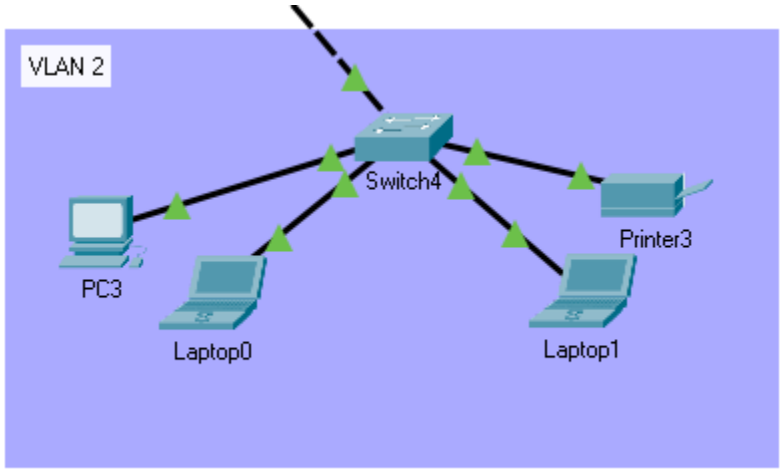
La DMZ permette ai dispositivi collegati di poter essere raggiunti dagli utenti al di fuori della rete LAN, per meglio specificare permette tutte le connessioni in entrata ed uscita dalla rete, in questo caso abbiamo appunto inserito un server di posta e un server web.

A far capo alla DMZ abbiamo il sistema di rilevamento delle intrusioni IPS. Abbiamo scelto l'IPS perchè blocca automaticamente il traffico sospetto prevenendo così gli attacchi, in ogni caso questo sistema può essere soggetto a falsi positivi.

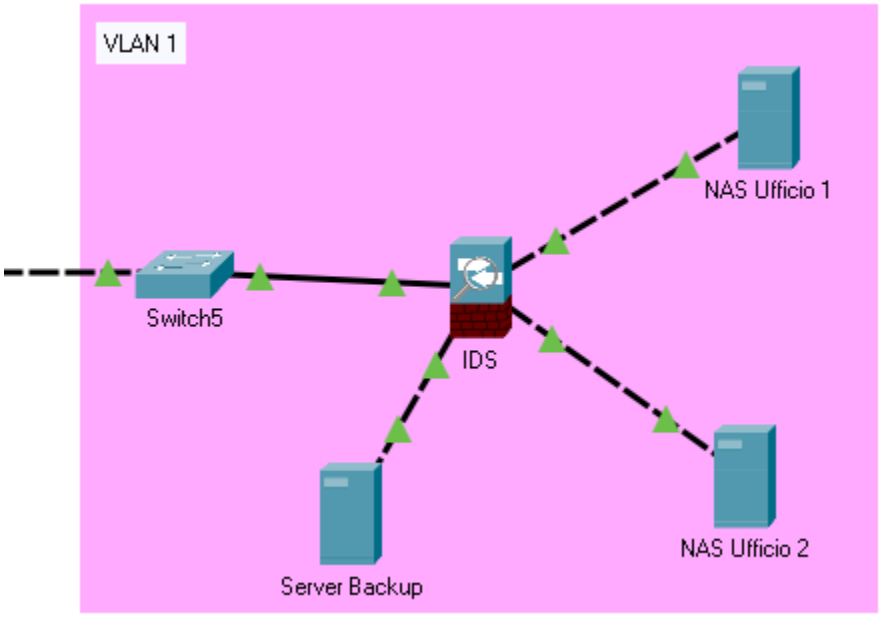
3 VLAN

Per un'ulteriore sicurezza della rete l'ho segmentata creando tre VLAN, rispettivamente una per ufficio alla quale sono collegati come host 3 computer e 1 stampante, entrambe collegate ai rispettivi switch che permettono la comunicazione tra dispositivi appartenenti alla stessa VLAN e poi un'altra VLAN per i server NAS aziendali.





Ho dedicato poi un’altra VLAN dedicata ai server della LAN: Server NAS dell’Ufficio VLAN 3, Server NAS dell’Ufficio VLAN 2 e poi un Server di BACKUP.



A far capo a questo VLAN ho inserito il sistema di rilevamento di intrusione IDS perchè rispetto all’IPS, andando a proteggere i server dell’azienda, essendo i dispositivi più importanti, abbiamo bisogno di una maggiore sicurezza. In questo caso l’IDS è più veloce ma soprattutto la differenza sostanziale è che quando detecta un’anomalia o intrusione, il sistema invia all’amministratore un messaggio con i dettagli sul motivo del blocco, così facendo si ha un feedback su cosa sta succedendo all’interno della rete.

CONCLUSIONE

La rete creata è stata organizzata in modo tale da garantire la miglior sicurezza e gestione del traffico di rete, per farlo abbiamo segmentato la rete con le VLAN e diversi dispositivi di protezione tra cui un Firewall perimetrale che filtra il traffico tra rete LAN e l'esterno, il sistema IPS blocca automaticamente le minacce provenienti dall'esterno verso i servizi pubblici del Server HTTP e SMTP. Il sistema IDS invece monitora e protegge la VLAN 1 alla quale sono collegati i dispositivi più importanti della rete, i Server NAS e il Server di Backup. Le VLAN 2 e 3 invece ospitano i dispositivi appartenenti a due uffici diversi.

In questo modo abbiamo segmentato la rete proteggendo tutti i dispositivi al suo interno "isolando" tramite le VLAN e proteggendo i servizi pubblici.