## S2L1 DISEGNO E REPORT

Disegnare una rete con i seguenti componenti:

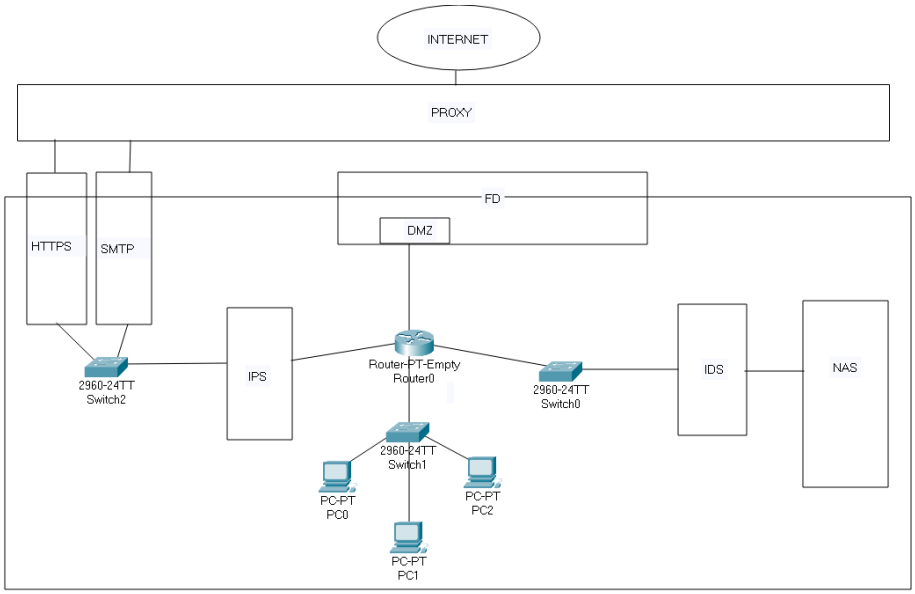
● Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).

● Una zona DMZ con almeno un server web (HTTP) e un server di posta elettronica (SMTP).

● Una rete interna con almeno un server o nas.

● Un firewall perimetrale posizionato tra le tre zone.

● Spiegare le scelte




Nel disegno della mia rete ho posizionato il firewall dinamico perimetrale (FD) a cavallo tra WAN e LAN, questo blocca qualsiasi connessione di origine esterna di arrivare all'interno; siccome quasi tutte le aziende necessitano che una parte del loro sito sia accessibile ad utenti esterni, all'interno del firewall ho posizionato la DMZ che altro non è che una porta raggiungibile dall'esterno. Essendo la DMZ una porta accessibile da tutti, ho posizionato un firewall per contenuto next generation (PROXY, WAF, ANTISPAM, ANTIMALWARE) il cui compito è quello di filtrare il contenuto dei pacchetti in entrata controllandone l'ip, la porta ed anche il contenuto. Se viene reputato malevolo il pacchetto viene bloccato, se invece viene riconosciuto come benevolo viene fatto passare potendosi così connettere ai server https e smtp. Come ulteriore sicurezza ho impostato anche un IPS (Intrusion Protection System) a protezione del web la cui funzione è quella di mandare un avviso e bloccare l'ingresso nel sistema di pacchetti o file non riconosciuti; ed anche un IDS (Intrusion Detection System) a protezione del NAS (Network attached Storage) il cui compito è quello di mandare semplicemente un avviso in caso di file non riconosciuti. La scelta di posizionare un IDS a protezione del NAS e non un IPS è legata alla questione dell'accessibilità: essendo il NAS un archivio condiviso, necessita si di sicurezza ma anche di accessibilità, e l'IPS viste le sue funzioni intaccherebbero quest'ultima.