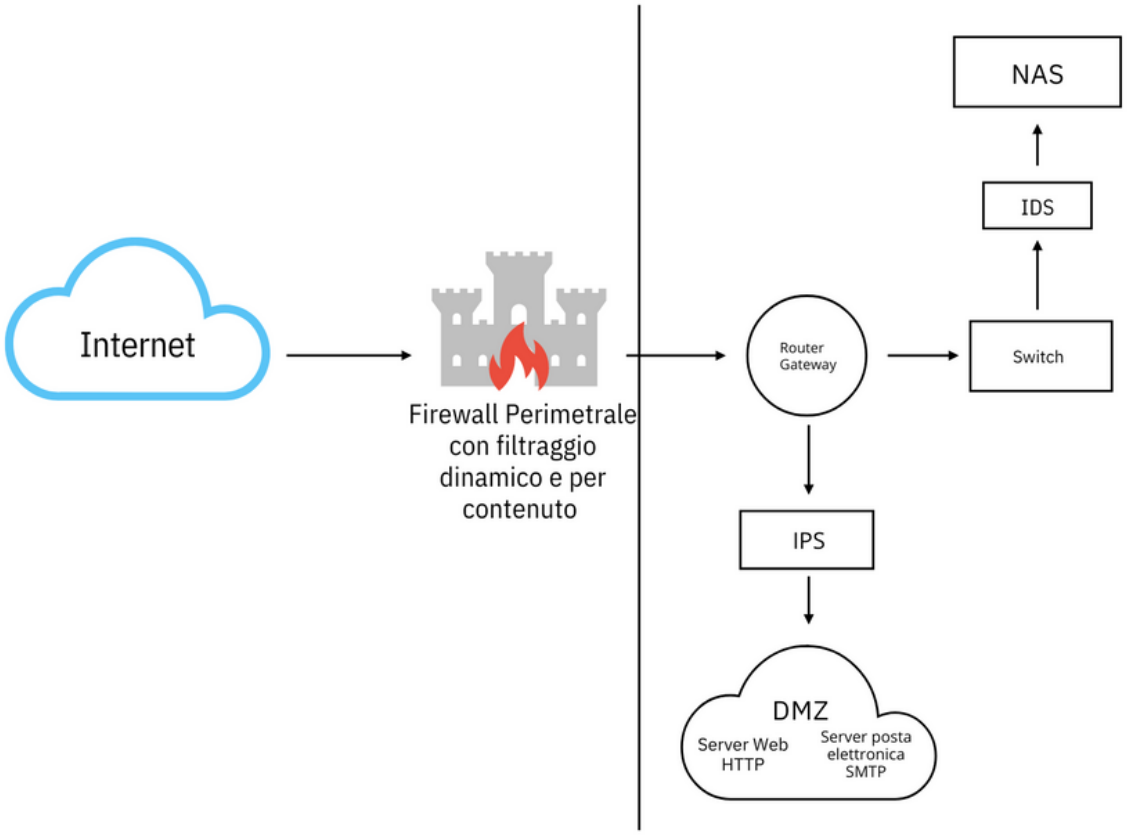
Esercizio S2L1



Per la configurazione di questa rete ho iniziato con l'implementazione di un firewall perimetrale con capacità di filtraggio dinamico la scelta è ricaduta su questa tipologia di firewall perchè si posiziona a cavallo tra la WAN e la LAN cosi riesce a monitorare il traffico in entrata e in uscita, il filtraggio dinamico ha la funzione di bloccare tutte le connessioni in maniera automatica se queste hanno origine dall'esterno verso l'interno e non blocca le connessioni che partono dall'interno verso l'esterno, ma ha la peculiarità di avere una porta chiamata DMZ con la funzione di creare connessioni dall'esterno verso i dispositivi interni che si trovano in questa zona.
Ma questo tipo di filtraggio consente a tutti l'accesso verso i nostri dispositivi quindi per ovviare a questo problema è bene integrare anche il filtraggio per contenuto che ha la funzione di prendere i pacchetti ed analizzare il contenuto (payload) e in base alla tabella che ha in memoria può bloccare il determinato pacchetto se trova una corrispondenza tra nomi quindi bloccare un ipotetica minaccia. Questa tabella aggiornata si può prendere da associazioni come OWASP.
Dopo il router gateway che ha la funzione di dirigere il traffico ho inserito verso la DMZ un IPS e verso il NAS un IDS che hanno la funzione di monitorare il traffico di rete alla ricerca di attività sospette e segnalare minacce. La differenza è che l'IDS avvisa in caso di attacco e l'ho posizionato verso il NAS in modo da intervenire manualmente e garantire comunque l'accessibilità ai dati presenti nel NAS; mentre l'IPS oltre a rilevare la minaccia agisce attivamente ed interviene in modo automatico per questo motivo l'ho posizionato verso la DMZ.
Il NAS è una parte fondamentale da proteggere perchè è un dispositivo che archivia tutti i dati e li rende condivisibili in una LAN tra più dispositivi.