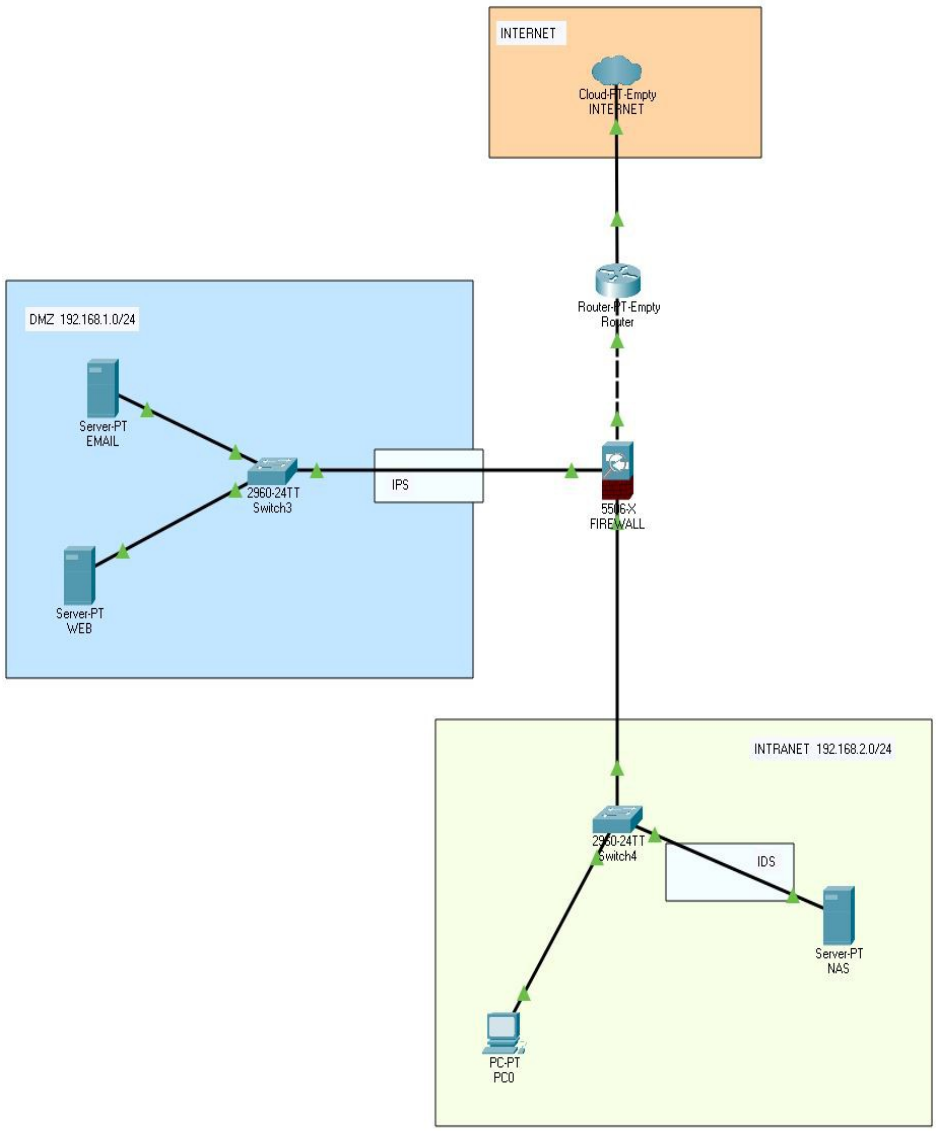
ESERCIZIO S1.L2

Disegnare una rete con i seguenti componenti:

- Una zona di Internet (rappresentata con 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.



All'interno delle infrastrutture si ha bisogno di dividere le due reti Intranet e DMZ per motivi di sicurezza, in modo che non possano comunicare tra di loro.

La DMZ (Demilitarized Zone) è una sottorete dove vengono inseriti servizi raggiungibili tramite internet, tra cui il server WEB (HTTP) e il server per la posta elettronica (SMTP). In quanto il flusso dei dati proviene da internet, quindi dall'esterno, è ideale mettere un firewall perimetrale prima di questa zona.

Il Firewall non è altro che un dispositivo che permette il monitoraggio del traffico in entrata e in uscita. Il Firewall perimetrale si trova a cavallo tra WAN (ovvero internet) e la LAN (rete privata).
Prima di questa zona può essere posizionare un IPS che è un software che previene e blocca le intrusioni tramite l'invio di un allert e bloccando il pacchetto in entrata.

L'intranet invece è una rete privata che non offre servizi alla rete esterna, ed è ad uso interno. In questa rete si trova il NAS (Network access storage) che è un dispositivo dove al suo interno sono posizionati degli storage completamente condivisibili con tutti quelli della rete LAN. Questo dispositivo non deve essere raggiungibile in alcun modo dall'esterno e per questo ci devono essere molti metodi di sicurezza per difenderlo. Prima di esso può essere posizionato un software IDS che ha il compito solo di avvertire con un messaggio di allarme che qualcuno sta cercando di entrare.
Prima del NAS si usa un IDS invece che un IPS perchè quest'ultimo potrebbe bloccare l'accesso ad un utente nella rete interna che ha urgentemente bisogno di un file presente all'interno dello storage.