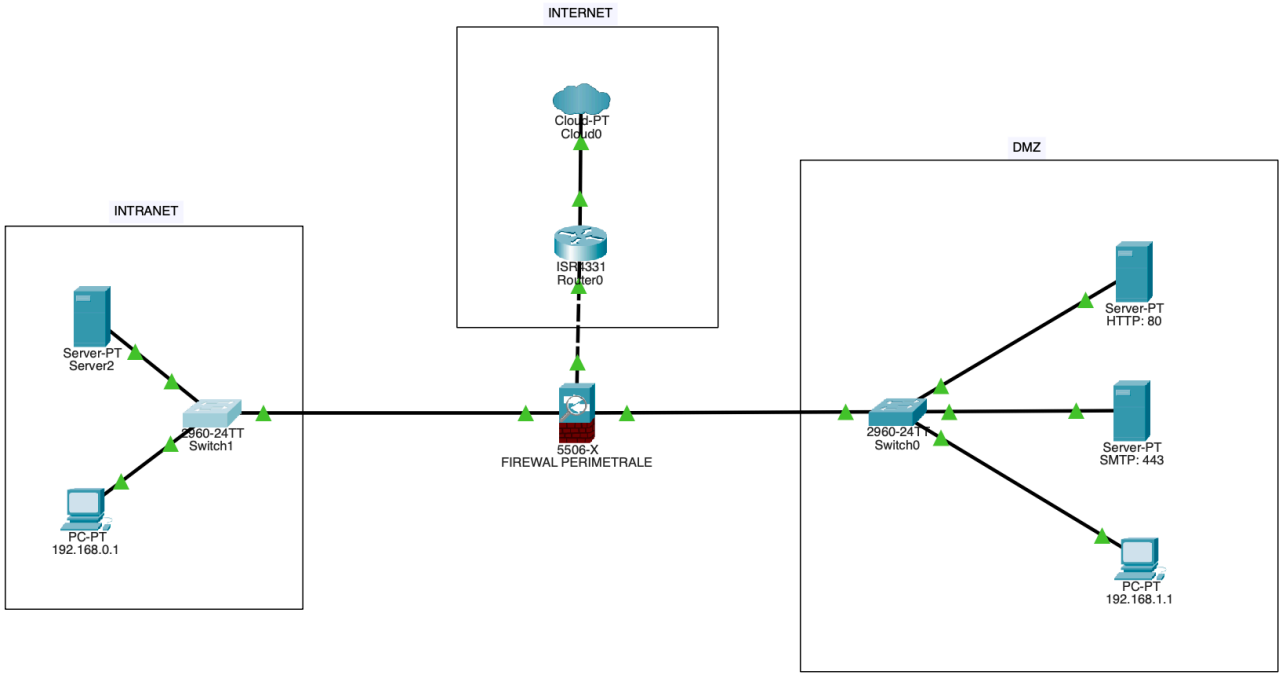
CONSEGNA 29 GENNAIO

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.



In questa rete abbiamo applicato il principio dello zoning dividendo la rete in tre zone diverse, divise a seconda del traffico:
-Zona internet, dove attraverso il router abbiamo l'accesso a internet. In questo caso il Router è di confine, perché è il punto in cui termina la rete privata e inizia l'internet pubblico. È l'ultimo router sotto il controllo della nostra rete ed è collegato alla rete interna ed esterna
-Zona demilitarizzata (DMZ), che contiene il pc, una server WEB (http: 80) ed un server di posta elettronica (SMTP: 443). Questa zona è progettata per ospitare servizi accessibili ai dipendenti, (i due server) isolando la rete privata da potenziale minacce. È importante che questa rete sia efficacemente protetta, vedi firewall perimetrale.
-Zona intranet, rete interna che ospita pc ed un server. In questa zona non ci sono servizi raggiungibili da internet (vedi firewall perimetrale), quindi i flussi di rete sono interni.

Fulcro della nostra rete di oggi è il firewall perimetrale, che si trova al confine della nostra rete privata ed impedisce al traffico dannoso di attraversare tale confine. La funzione principale di questo firewall è di filtraggio dei pacchetti in entrata o in uscita dalla nostre rete , questo processo prende il nome di policy firewall e permette di filtrare i pacchetti sulla base di alcune caratteristiche. Nel nostro caso le action del nostro firewall saranno le seguenti:
- Qualunque pacchetto in entrata dall'esterno diretto verso la zone intranet dovrà essere droppato (drop)
- Per il flusso di pacchetti dalla zona intranet e la zona dmz e viceversa, il firewall dovrà bloccare il flusso di pacchetti delle due zone, sempre attraverso la policy firewall
- Per il flusso di pacchetti dalla zona demilitarizzata ad internet la policy firewall dovrà essere impostata con scrupolosità sopratutto per i pacchetti che arrivano dall'esterno.

Molto importane è avere un sistema di rilevamento/ prevenzione delle intrusioni (IDS/IPS), ed altrettanto importante è che il firewall perimetrale sia ridondante dato che un'interruzione del flusso di pacchetti o un gusto dovuto a fattori esterni potrebbe mettere in crisi il sistema.