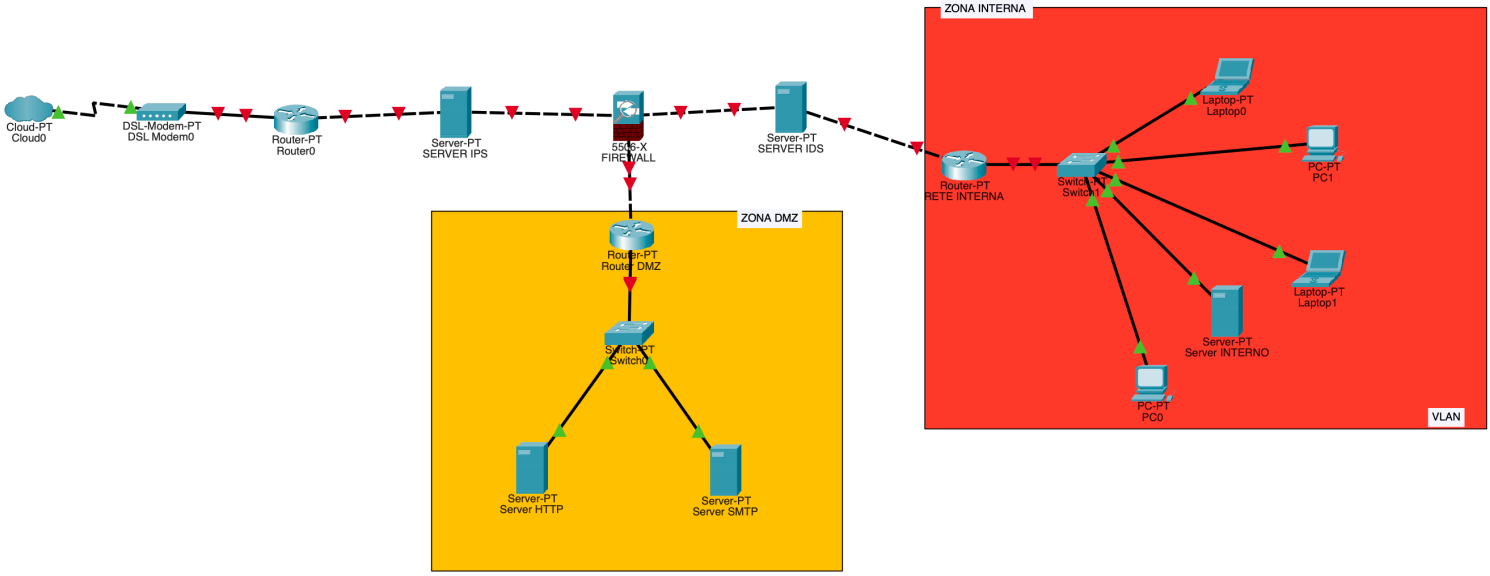
Compito di oggi disegnare una rete con i seguenti componenti:

- **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.**
- **Un Sistema di Rilevamento delle Intrusioni (IDS) posizionato strategicamente nella rete.**
- **Un Sistema di Prevenzione delle Intrusioni (IPS) posizionato strategicamente nella rete.**



Firewall Perimetrale: Il firewall perimetrale è posizionato tra le tre zone (Internet, DMZ e rete interna). La sua funzione è controllare e monitorare il traffico tra queste zone, consentendo o bloccando il passaggio dei dati in base alle regole di sicurezza configurate.

IDS (Intrusion **Detection** System) ovvero il sistema di rilevamento intrusione: rileva come intrusione qualsiasi attività che avviene a livello di network potenzialmente riconducibile a qualcosa di malevolo. Può essere collocato tra la DMZ e la rete interna per identificare minacce prima che raggiungano la rete interna.

IPS (Intrusion **Prevention** System) ha anche funzionalità operativa ed interviene: può bloccare la connessione, è in grado di aggiungere una regola al firewall per bloccare permanentemente un dispositivo e diverse altre cose bloccare o prevenire le potenziali minacce. Può essere collocato in una posizione in cui può agire direttamente per bloccare o mitigare gli attacchi identificati dall'IDS.

Router: un router è un dispositivo che collega due o più reti separate. Il suo compito principale è quello di instradare i dati da una rete all'altra, in base agli indirizzi IP dei dispositivi di destinazione. In questo caso collega la rete interna alla rete esterna.

Switch: è un dispositivo che collega più dispositivi di una singola rete. Il suo compito principale è quello di instradare i dati tra i dispositivi della rete, in base agli indirizzi MAC dei dispositivi. Gli switch sono utilizzati per creare reti locali (LAN). Possono essere utilizzati per collegare dispositivi di qualsiasi tipo, ad esempio computer, stampanti, router e server.

Server: possono essere utilizzati ad esempio per supportare le attività di un'azienda, come l'archiviazione dei dati, l'elaborazione delle transazioni e la gestione dei dipendenti.

Commento
La rete è protetta da un firewall che impedisce agli utenti non autorizzati di accedere ai dispositivi interni. Il firewall è configurato per consentire solo il traffico autorizzato.

Prima della rete interna, che contiene dati sensibili, ho inserito un IDS per monitorare tutto il traffico in entrata così da poter intervenire in caso di tentativi di intrusione. In questo caso ho preferito inserire un IDS e non un IPS perchè avrebbe potuto intervenire nei casi di falsi positivi e credo che questo possa essere controproducente.
Ho comunque inserito il dispositivo IPS nella rete per bloccare il traffico indesiderato in entrata, posizionandolo tra il il firewall e il modem.

Di solito il firewall in quanto “perimetrale” non si troverebbe in mezzo alla rete, per questo motivo si potrebbe considerare di strutturare la rete in modo diverso. Ad esempio a cascata:
-Dal cloud -> si passa al firewall perimetrale -> si passa ad un IDS -> si passa alla DMZ, tramite la DMZ si passa all’IPS (più restrittivo) -> per arrivare alla rete interna.
Quindi per arrivare alla rete interna si dovrà prima passare anche attraverso la DMZ con IDS, IPS e Firewall.