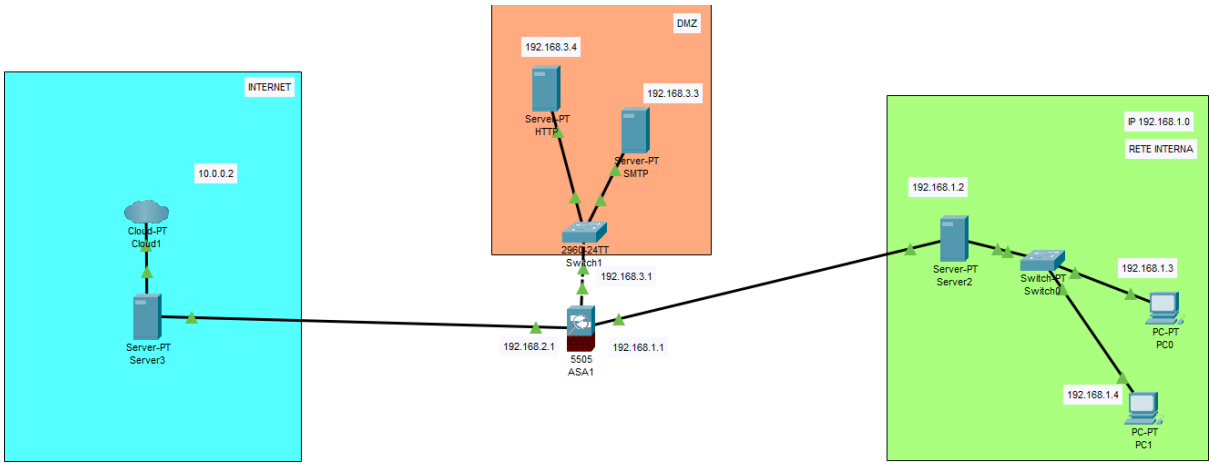
Compito di oggi: disegnare una rete con i seguenti componenti:

- 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.
- Spiegare le scelte.



La dmz è l'area di rete tra tra la parte interna e la rete esterna(internet). Il traffico in questa zona è meno controllato rispetto alla zona di rete interna. È un'area usata per inserire i vari server (in questo caso HTTP e SMTP) che devono essere accessibili.
Creiamo la nostra DMZ usando il firewall fornito da CISCO: l'ASA che lavora con le VLAN > ne ha due di dafault: INSIDE e OUTSIDE. Inside in questo caso sarà la nostra rete interna, e outside sarà internet.

1. Come al solito andiamo a creare la nostra rete:
   - Rete Interna
   - DMZ
   - Zona di Internet

2. Assegnamo i vari IP e configuriamo i dispositivi.

3. Dobbiamo modificare il firewall

La VLAN 1 > inside > è la nostra rete interna è avrà livello sicurezza 100 > a questa non devono poter accedere host esterni.

La VLAN 2 > outside > è internet > livello di sicurezza 0, non è di nostra competenza perché è l'area esterna.

Andiamo da linea di comando a modificare le impostazioni LAN per configurare e dare i valori che desideriamo per regolare l'accesso.

Ed, infine andiamo ad impostare la VLAN 3 > cioè la nostra DMZ che non vogliamo possa comunicare con la rete interna. Per questo sul firewall andremo ad impostare #no forward interface VLAN1 > in questo modo la dmz non parla con la vlan 1(rete interna).

> andrebbero anche configurati gli ACL per regolare il traffico in entrata ed uscita.

Il server DMZ può raggiungere l'esterno, invece la rete esterna (internet) non può raggiungere il server interno.

Il firewall perimetrale quindi ci permette di mitigare e regolamentare il traffico da e verso internet; è il nostro primo livello di protezione. Permette di protegge 3 macroaree dell'infrastruttura: 1. Il traffico effettuato dall'interno dell'azienda verso l'esterno. I collaboratori dell'azienda in questione fruiscono di internet; è il nostro firewall che va a regolamentare e sanificare questo tipo di traffico. 2. Il firewall permette di regolamentare il traffico inverso, quindi che da internet arriva verso i nostri sistemi: un portale che possono usare i clienti dell'azienda ad esempio > grazie ai profili UTM il firewall analizza, regola e tratta questo tipo di dati. 3. La gestione dello smart working > c'è il bisogno di regolarizzare l'accesso alle risorse aziendali da pc esterni: qui entra in gioco la WAF > che protegge l'infrastruttura da una prospettiva applicativa.

Il firewall perimetrale quindi andrebbe posizionato tra la rete interna e la rete esterna perché appunto serve a proteggere la rete interna dalle eventuali minacce proveniente dall'esterno/internet > per questo è anche importante che non comunichi direttamente con la DMZ.
Con il filtraggio statico il firewall viene configurato proprio per consentire la ricezione o meno di un pacchetto andando a verificare se l'indirizzo IP di origine e destinazione è consentito, se la porta di destinazione è autorizzata e se il protocollo usato è permesso. Nella DMZ vogliamo per esempio consentire l'accesso alla porta 80 (HTTP)> per la trasmissione di pagine web su internet e alla porta 25 (SMTP) per l'invio di mail.