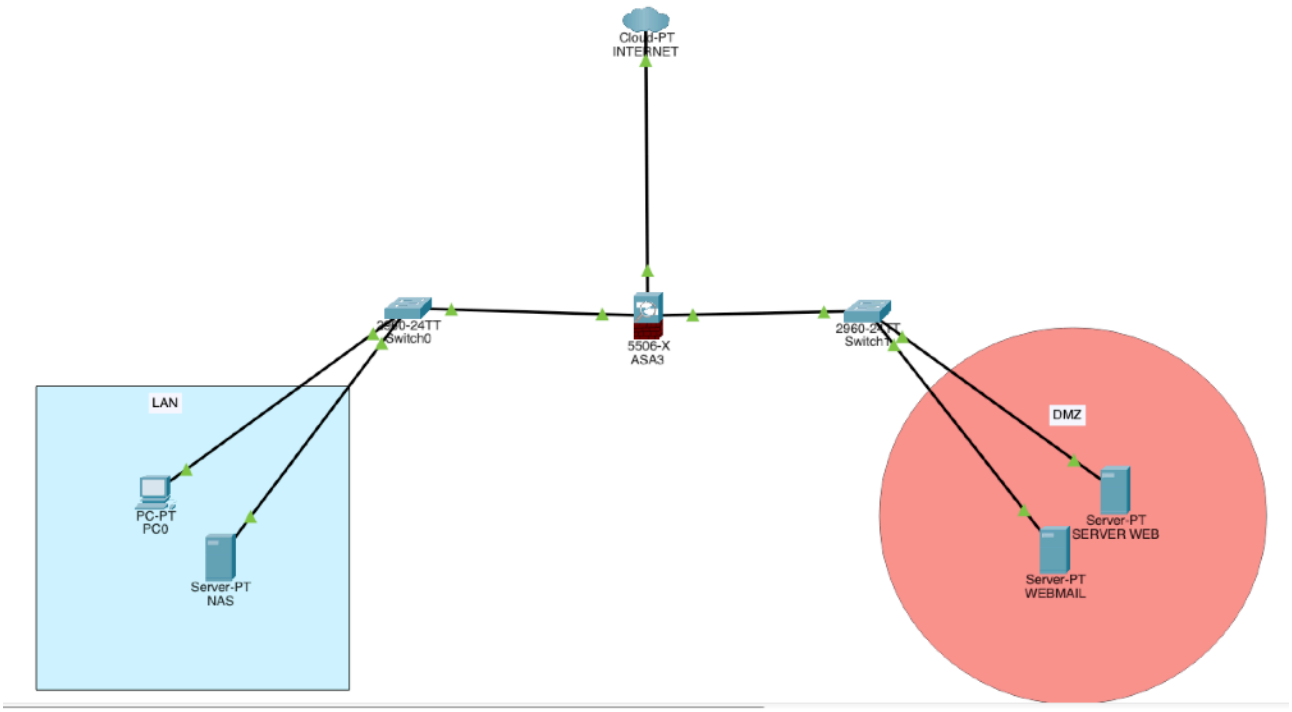
Svolgimento esercitazione S2/L1

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.



Come da richiesta, ho realizzato una zona internet rappresentata dal cloud, alla quale è collegato un firewall ASA 5506 al fine di controllare il traffico in entrata e in uscita. A sua volta, questo è collegato a due switch, ognuno con le due reti richieste:

Rete interna (**192.168.1.0/24**):

- PC utente (192.168.1.2);
- Server NAS (192.168.1.3);

DMZ (**192.168.2.0/24**):

- Server web (192.168.2.2)
- Servizio web mail (192.168.2.3)

In questo caso, configurando opportunamente il firewall, si permette ai servizi della dmz di essere esposti direttamente su internet al fine di rendere i servizi offerti *reperibili a terzi* (in questo caso un server web e una webmail fittizia).

Al contrario, nessun host della rete interna è accessibile da internet o dagli host della dmz per evitare rischi e garantire la sicurezza della rete. In particolare, è fondamentale proteggere il NAS da possibili attacchi esterni.

Ipotetica tabella per le regole:

Ip sorgente	Ip destinazione	Porta	Action
192.168.1.2	192.168.1.3	ANY	ACCEPT
192.168.1.3	192.168.1.2	ANY	ACCEPT
ANY	192.168.2.2	80	ACCEPT
ANY	192.168.2.3	25	ACCEPT
ANY	ANY	ANY	DENY

Tutti gli host della rete interna potranno comunicare tra loro senza che nessun altro (proveniente da Internet o dalla DMZ) possa fare altrettanto. Tutti gli altri host, sia quelli provenienti da Internet che quelli della rete interna, potranno invece comunicare specificamente sulla porta 80 e 25, con il server web e il server di posta.