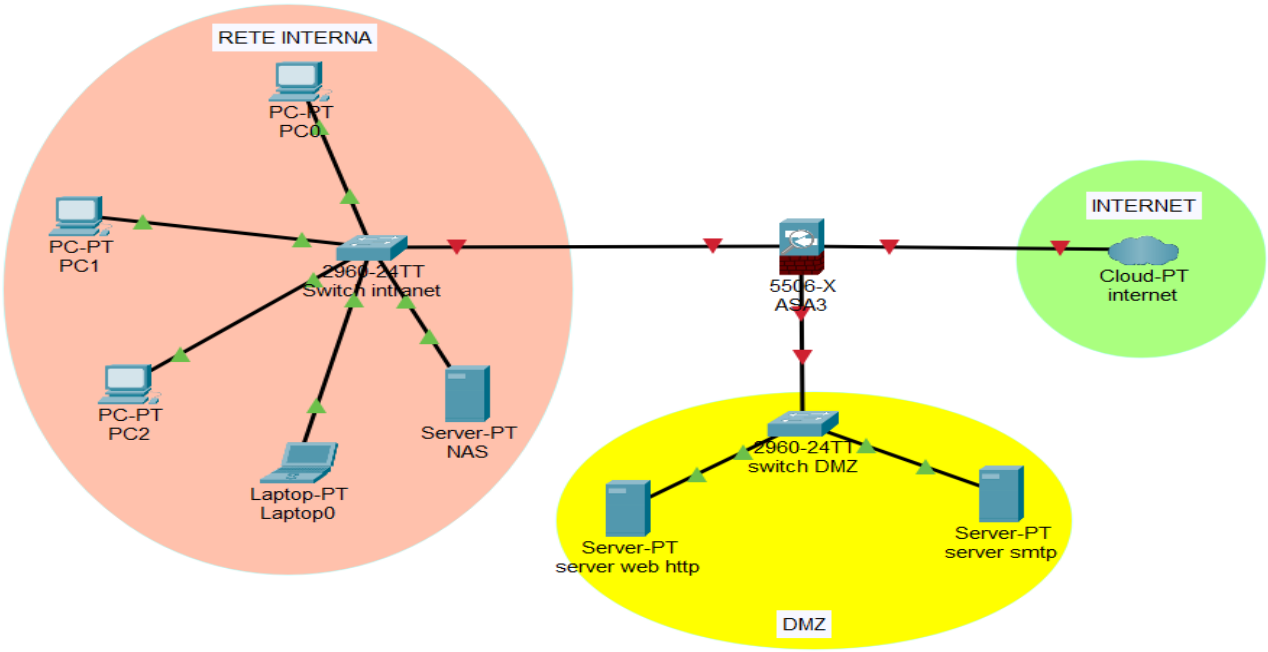
Disegnare una rete con i seguenti componenti:

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.



- Internet (cerchio verde), generalmente fornito da un ISP, e raggiungibile grazie all'utilizzo di un router (non illustrato in figura, in quanto l'hardware firewall 5506 di Cisco può essere utilizzato anche come router)

- La DMZ, o DeMilitarized Zone, è una sottorete, o segmento di essa, in cui possiamo trovare servizi raggiungibili da internet, come possiamo vedere nell'immagine.. Viene separata dal resto della rete per ridurre al minimo il rischio di attacchi e sottrazione di materiale sensibile della rete interna.

- La rete interna, o Intranet, come dice il nome, è una rete interna all'azienda, in cui possiamo trovare i pc dei dipendenti. I flussi di rete sono interni e non presenta servizi direttamente raggiungibili da internet. In questa configurazione si può trovare un server Intranet o NAS, che ospita risorse sensibili dell'azienda.

- Queste tre zone ben distinte vengono messe in comunicazione da un Firewall, che gestisce e filtra il traffico dei pacchetti in entrata e uscita dalle varie zone, in base alle policy che mette in atto l'azienda che gestisce questa rete. Quando un firewall analizza un pacchetto, possono accadere 3 differenti"actions":
-**Allow**, ovvero il pacchetto può passare;
-**Drop**, ovvero il pacchetto non può passare, ma non viene informata la sorgente;
-**Deny**, ovvero il pacchetto non può passare, e la sorgente viene informata dal firewall tramite messaggio diagnostico.

Viene attuata questa scelta di separare distintamente le tre zone, per una maggior sicurezza. Se si desidera un livello di sicurezza più elevato, possono essere implementati ulteriori firewall ed anche altri sistemi, come i proxy.