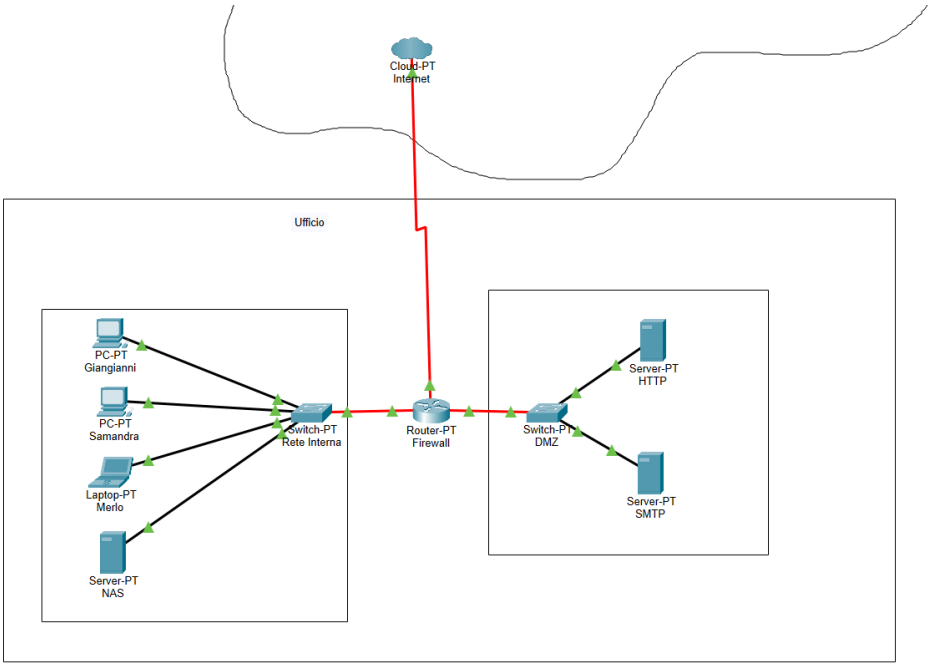
Progetto S3L5

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.



Nel progetto viene inserito un cloud per rappresentare la rete Internet pubblica, una rete interna con un server NAS e delle postazioni PC, e una zona DMZ (Demilitarized Zone) con due server: uno per il servizio web (HTTP/HTTPS) e uno per la posta elettronica (SMTP). Infine, un firewall perimetrale separa le tre zone e gestisce le comunicazioni tra di esse.

I server nella DMZ devono avere degli IP pubblici per poter offrire i loro servizi a chiunque su Internet. Il firewall dovrà consentire l'accesso ai server della DMZ solo sulle porte necessarie, come la porta 80 e 443 per il server web (HTTP/HTTPS) e la porta 25 per il server di posta elettronica (SMTP). In questo modo, i servizi saranno accessibili dall'esterno, ma il traffico non autorizzato verrà bloccato.

Il firewall avrà anche il compito di bloccare qualsiasi comunicazione tra la DMZ e la rete interna. Questo è fondamentale per evitare che un attacco a uno dei server della DMZ possa compromettere la rete aziendale interna. La rete interna contiene dati aziendali sensibili, come documenti e file importanti, che devono essere protetti da accessi esterni non autorizzati.

La rete interna dovrà poter navigare su Internet e accedere ai servizi esterni, ma il firewall dovrà fare in modo che nessuno dall'esterno possa entrare nella rete aziendale. I PC della rete interna potranno uscire verso Internet per navigare o inviare email, ma il firewall bloccherà qualsiasi traffico che provenga dall'esterno verso la LAN.

In conclusione, l'uso del firewall è essenziale per separare le zone della rete e proteggere la rete interna da eventuali attacchi provenienti dalla DMZ o da Internet. Il firewall garantisce che i server nella DMZ siano raggiungibili solo per i servizi necessari, mentre la rete aziendale resta protetta, con un accesso controllato e sicuro a Internet.