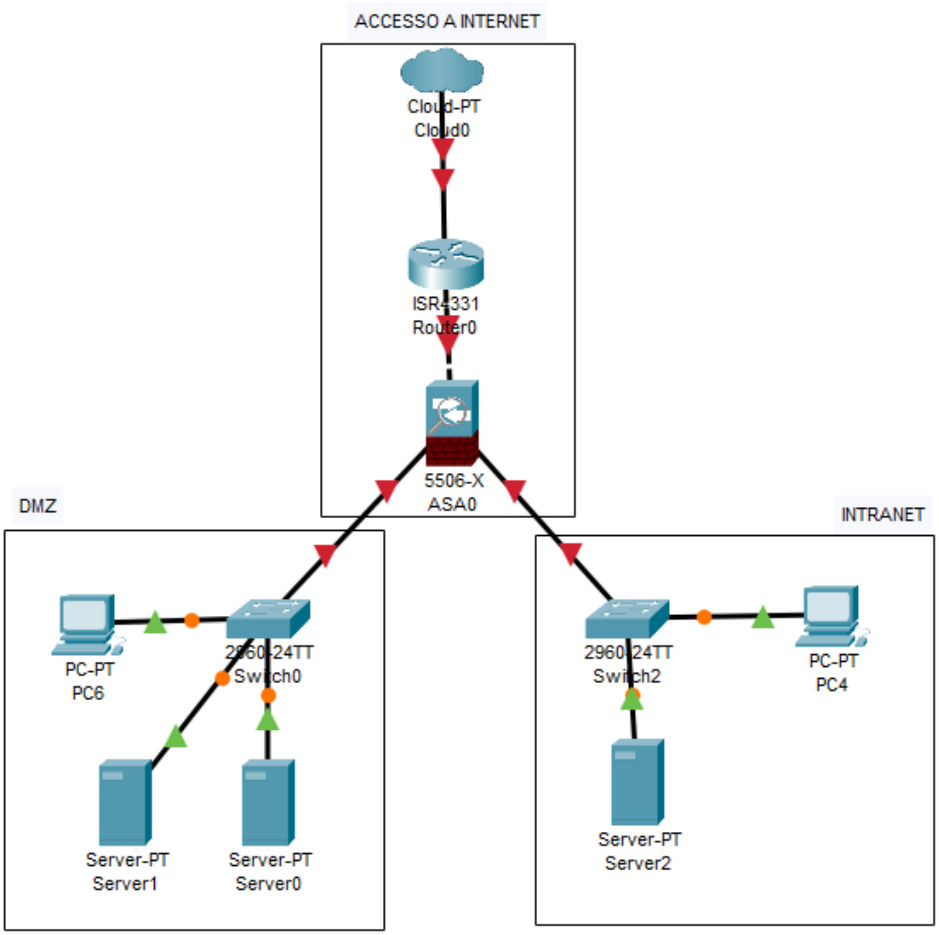

Abbiamo creato una rete con accesso a internet suddivisa in due zone:
- DMZ (Demilitarized Zone) per consentirci l'accesso ai servizi online al quale abbiamo connesso due server. Tali server sono un server web HTTP (Hypertext Transfer Protocol) su porta 80 e un server di posta SMTP (Simple Mail Transfer Protocol) su pora 443;
- Intranet: una rete interna con in genere un livello di sicurezza intermedio con in questo caso l'aggiunta di un semplice server.

Al cloud abbiamo collegato un router per l'instradamento dei pacchetti ai due switch che inoltreranno i dati al PC collegati ad esso. La connessione é protetta e gestita da un firewall in modo che la DMZ e la Intranet non comunichino tra loro. Inoltre usando un server web http e non https (quindi senza aggiunta di protocolli di crittografia SSL/TSL) é buona norma aggiungere e configurare quel firewall.

Il firewall é un sistema per proteggere una rete da minacce esterne, controllando il traffico in entrata e uscita. Puó essere sia software che hardware ma in questo caso abbiamo inserito quello software. Un altro modo per proteggere questa rete sarebbe stato quello di inserire due firewall: uno software per la DMZ e uno hardware per l'Intranet.
Una volta controllato il traffico il firewall a seconda di come é stato configurato decide se far passare o no quei determinati dati seguendo le "action":

- Allow per far lasciare il pacchetto;
- Drop per scartarlo senza informare la sorengte;
- Deny pee non farlo passare avvisando la soregente.