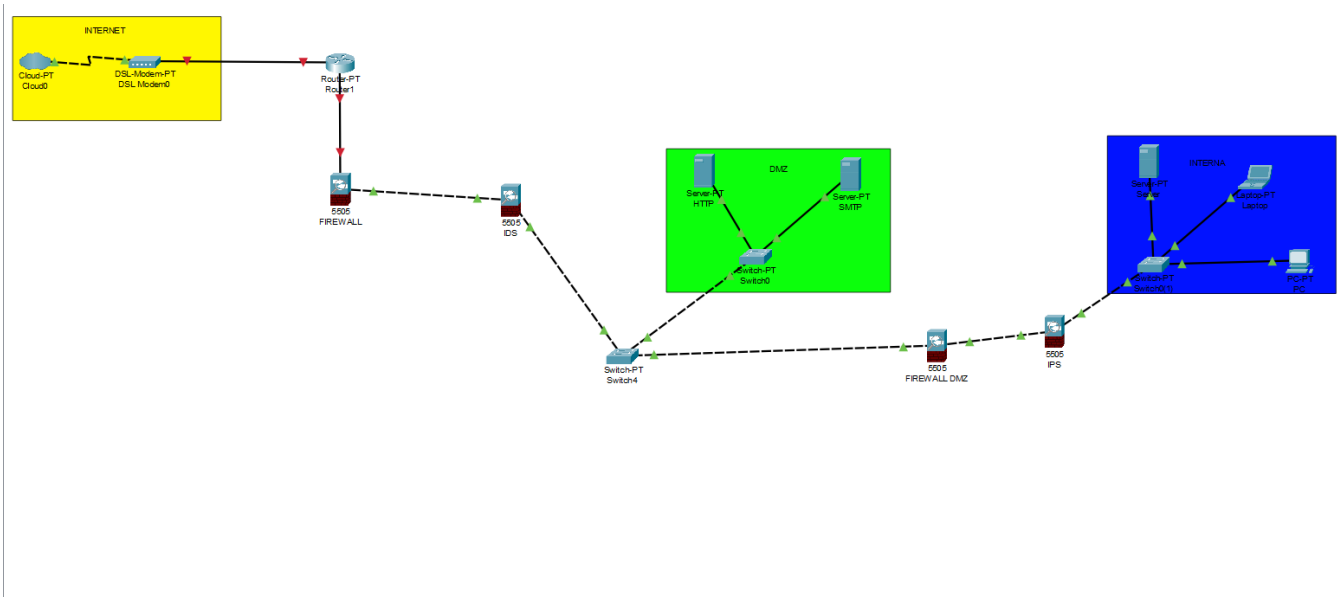
ESERCIZIO S3L4



La configurazione proposta è quella di un FIREWALL generale all'estremo, prima della connessione ad internet e di un IDS successivo per il monitoraggio del traffico della rete e l'identificazione di anomalie che potrebbero essere indicative di una minaccia alla sicurezza della rete.

Tra la rete DMZ e quella INTERNA ho inserito un ulteriore firewall e un IPS, che a differenza di un IDS, interviene in maniera attiva sulla minaccia, interrompendo l'attività dannosa, bloccando il traffico sospetto e notificando il tutto. Si è preferito inserito due FIREWALL in quanto come soluzione risulta più sicura; un eventuale attacco alla rete dovrebbe compromettere tutti e due i FIREWALL per accedere alla rete interna.

La configurazione si potrebbe semplificare utilizzando dei FIREWALL di nuova generazione, che includono IDS e IPS.