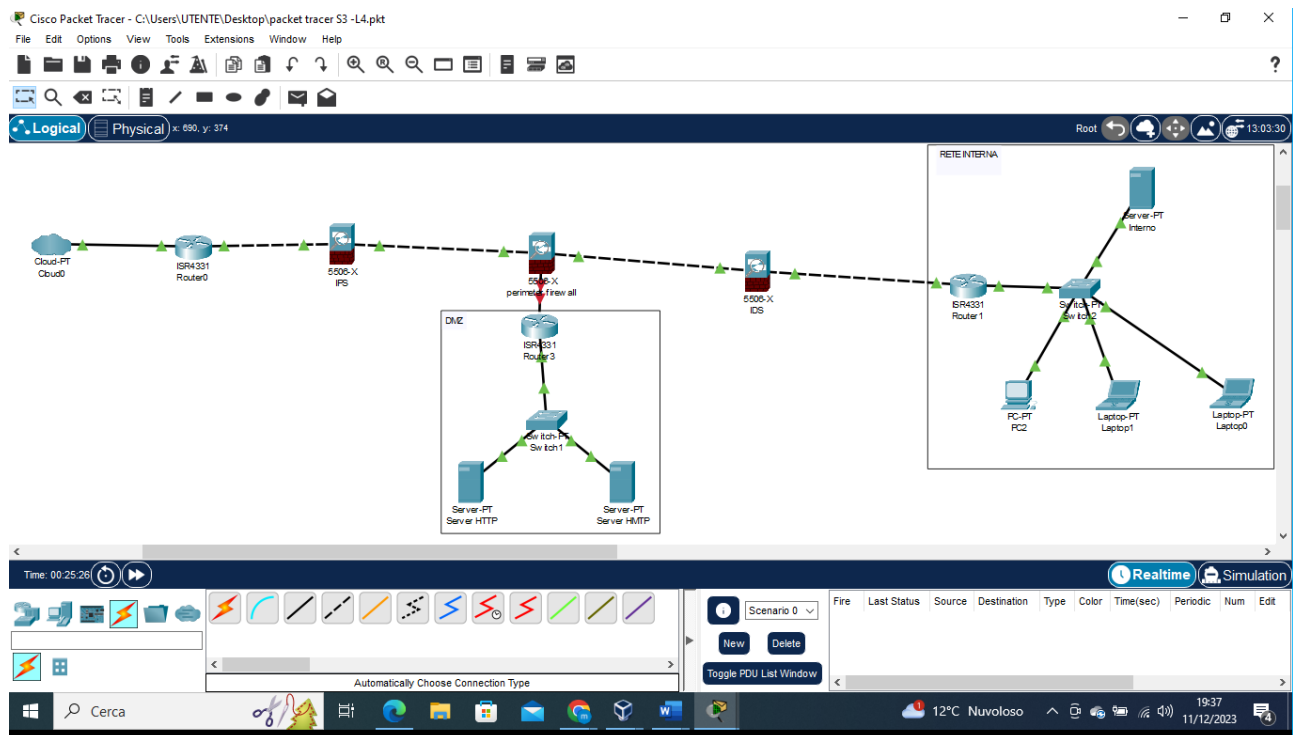


ESERCIZIO S3-L4

COMPITO: DISEGNARE UNA RETE CON I SEGUENTI COMPONENTI:

- 1)UNA ZONA INTERNET (RAPPRESENTATA DA UN CLOUD O SIMBOLO DI INTERNET)
- 2)UNA ZONA DMZ CON ALMENO UN SERVER WEB (HTTP) E UN SERVER DI POSTA ELETTRONICA(SMTP)
- 3)UNA RETE INTERNA, CON ALMENO UN SERVER O NAS
- 4)UN FIREWALL PERIMETRALE POSIZIONATO TRA LE TRE ZONE
- 5)UN SISTEMA DI RILEVAMENTO DELLE INTRUSIONI (IDS) POSIZIONATO STRATEGICAMENTE NELLA RETE
- 6)UN SISTEMA DI PREVENZIONE DELLE INTRUSIONI (IPS) POSIZIONATO STRATEGICAMENTE NELLA RETE.



Nella mia configurazione di rete ho scelto di suddividere le tre zone, a sinistra il **cloud** (internet, cioè rete esterna), al centro il firewall perimetrale, sotto la **DMZ** e a destra la **LAN** più interna. Le misure di sicurezza sono state poste nel seguente modo: Il **sistema di rilevazione IPS**, poco dopo il router provider, come primo strumento di sicurezza della rete perché non solo invia notifica di allarme agli amministratori della sicurezza ma agisce proattivamente bloccando il traffico sospetto/minaccioso o disconnettendo gli account degli utenti. Il **firewall perimetrale** è posto al centro, in modo da proteggere la DMZ da attacchi esterni e “isolare” il nodo dei dipendenti dalla DMZ. Quest’ultima infatti, esponendo i servizi della rete all’esterno (Internet) ed essendo perciò vulnerabile ad attacchi esterni, si trova su una rete diversa rispetto alla rete interna, sorvegliata dal firewall perimetrale. L’**IDS** invece è l’ultimo strumento di sicurezza che, in caso di fallimento dell’ IPS e del Firewall perimetrale, invia notifica di allarme agli amministratori di sicurezza affinché intervengano per bloccare l’attacco.