S3 L4

Svolgimento esercizio del 07/12/23

Giulia Salani

Consegna

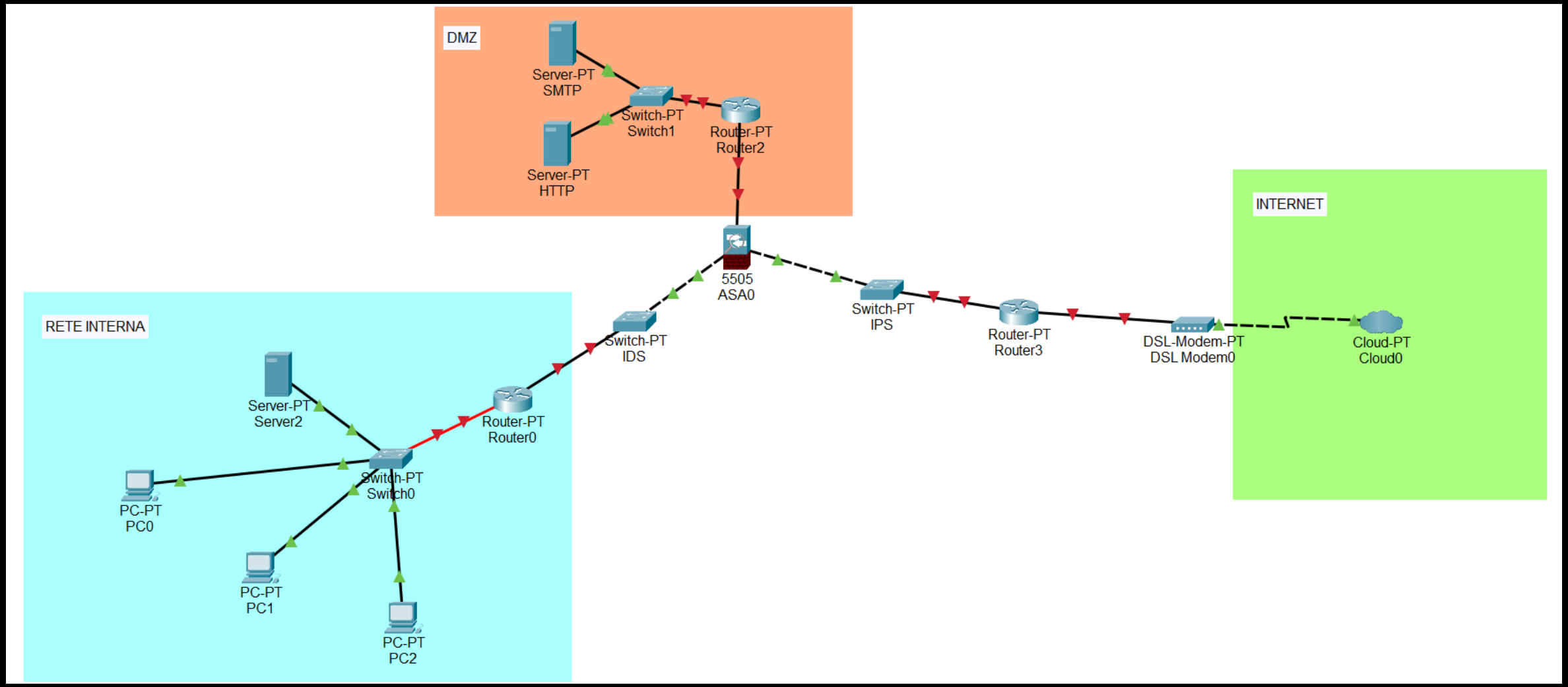
Traccia:

Compito di oggi 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
- Un Sistema di Rilevamento delle Intrusioni (IDS) posizionato strategicamente nella rete
- Un Sistema di Prevenzione delle Intrusioni (IPS) posizionato strategicamente nella rete

Spiegare le scelte.

Svolgimento



Svolgimento

- Avendo a disposizione solamente un dispositivo IDS e un dispositivo IPS, ho deciso di posizionarli come indicato nel progetto per le seguenti ragioni.

- Il dispositivo IPS è collocato vicino alla Zona internet affinché possa non solo identificare ma anche attivamente bloccare traffico malevolo o sospetto. Quindi la scelta di posizionarlo fra la zona internet e il firewall ha il fine di prevenire e limitare l'impatto delle minacce PRIMA che raggiungano le aree più sensibili della rete.

- Il dispositivo IDS invece, che monitora il traffico per rilevare eventuali attività sospette ma non interviene, l'ho posizionato all'ingresso della Zona interna per fornire ulteriore controllo alla rete dopo IPS e Firewall (che a quel punto saranno già intervenuti sulle principali minacce). Questo perché l'IDS identificherà processi sospetti senza bloccarli attivamente, quindi senza bloccare processi che potrebbero non essere malevoli e che anzi potrebbe essere dannoso bloccare. Saranno gli amministratori / le amministratrici di sistema, una volta ricevuta la segnalazione, a verificare e decidere se sia il caso di intervenire.