Esercizio sulla Progettazione di una rete con firewall,IDS e IPS

Data 09/12/23

Guglielmo Carratello

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).

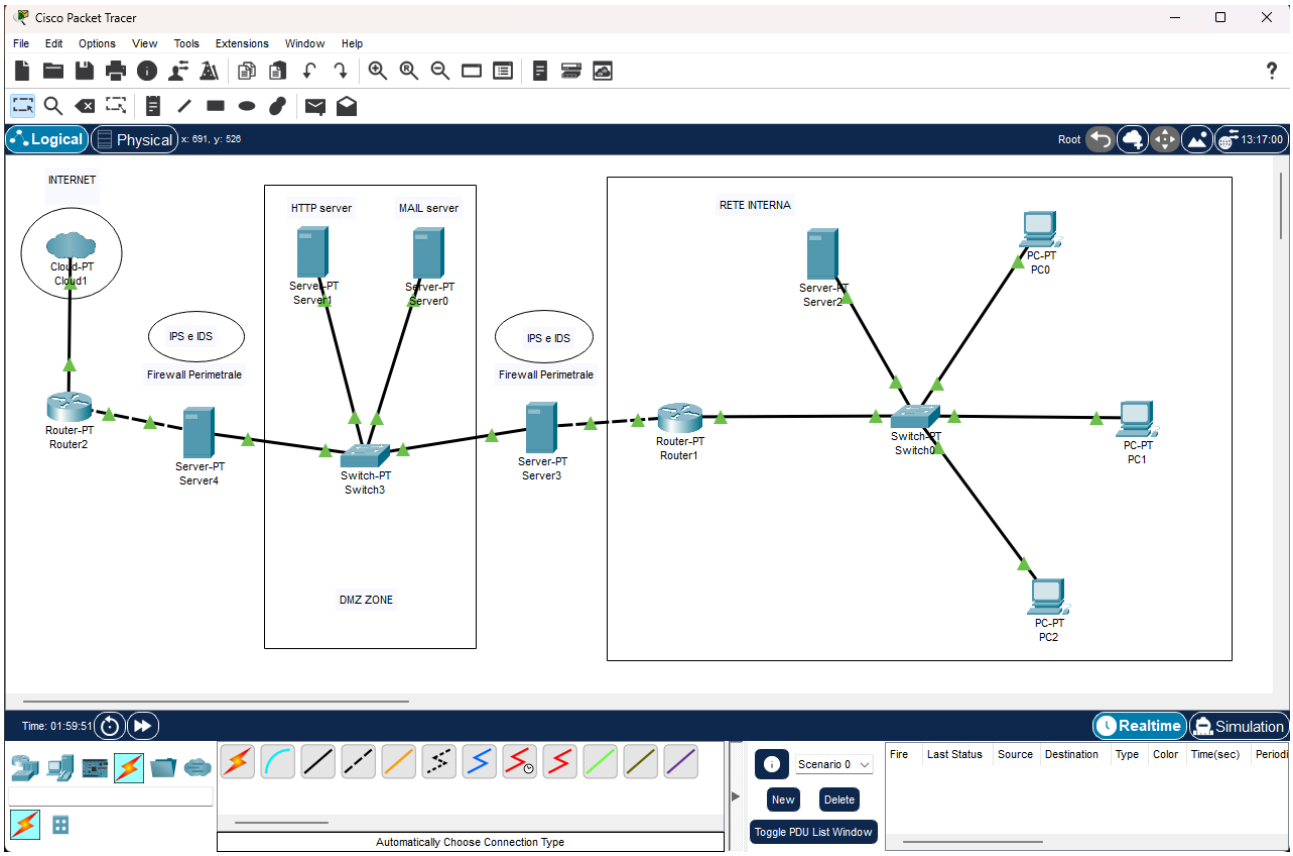
- Una rete interna con almeno un server o nas ● Un firewall perimetrale posizionato tra le tre zone.

- 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



Mettere un firewall, un sistema di rilevamento delle intrusioni (IDS) e un sistema di prevenzione delle intrusioni (IPS) tra la rete interna e la zona demilitarizzata (DMZ), e poi tra la DMZ e Internet,

è stata la mia scelta per migliorare la sicurezza di una rete. I motivi principali dietro questa configurazione sono:

Protezione della rete interna:

Firewall: Il firewall agisce come una barriera tra la rete interna e la DMZ, controllando e filtrando il traffico in base a regole predefinite. Ciò impedisce a eventuali minacce provenienti dalla DMZ di raggiungere la rete interna, riducendo il rischio di attacchi e compromissioni.

IDS e IPS: Un sistema di rilevamento delle intrusioni (IDS) monitora il traffico di rete per identificare comportamenti sospetti o potenziali minacce. Un sistema di prevenzione delle intrusioni (IPS) va un passo oltre, bloccando attivamente il traffico che è stato identificato come pericoloso.

Protezione verso Internet:

Firewall: Il firewall tra la DMZ e Internet svolge un ruolo cruciale nel proteggere la DMZ da attacchi provenienti dall'esterno. Filtra il traffico in entrata e in uscita, limitando l'esposizione dei servizi nella DMZ a potenziali minacce esterne.

IDS e IPS: monitorano il traffico tra la DMZ e Internet ed è essenziale per identificare e bloccare attacchi provenienti dall'esterno. L'IDS può individuare comportamenti sospetti, mentre l'IPS può prevenire attivamente attacchi noti o emergenti.

Conclusioni:

In sintesi, l'implementazione di firewall, IDS e IPS tra la rete interna, la DMZ e Internet crea un sistema di difesa stratificato che riduce il rischio di compromissione della sicurezza e protegge i dati sensibili e i servizi critici all'interno di un'organizzazione.