CS0424IT — ESERCITAZIONE S2 L1

Simone La Porta

GitHub

TRACCIA

Disegnare una rete con i seguenti componenti: una zona 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. Spiegare le scelte.

SVOLGIMENTO

La rete progettata è rappresentata schematicamente in Figura 1, secondo i seguenti accorgimenti:

- **FIREWALL PERIMETRALE**: un dispositivo di sicurezza di rete che si trova al confine tra la rete esterna (WAN) e la rete interna (LAN). Viene posizionato tra Internet e le diverse zone della rete aziendale, regolando il traffico in entrata e in uscita per proteggere la rete interna da minacce esterne. Il firewall perimetrale analizza i dati in transito e decide di bloccare o consentire il passaggio delle informazioni in base a un insieme di regole predefinite.

  Oltre a filtrare il traffico, un firewall perimetrale può offrire altre funzionalità avanzate, come la prevenzione delle intrusioni (IPS), la protezione contro i malware, la gestione delle VPN (Virtual Private Network) per connessioni sicure da remoto e il monitoraggio del traffico per rilevare comportamenti sospetti. In questo modo, il firewall perimetrale

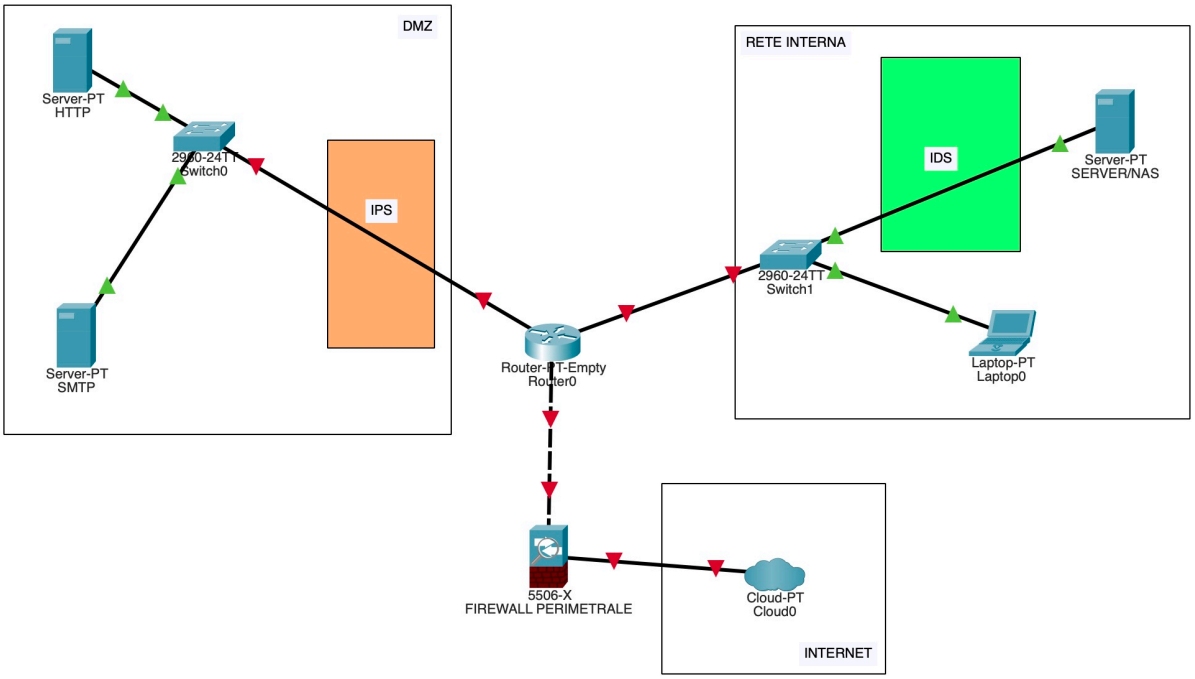

Figura 1: Schema della rete.

costituisce una linea di difesa fondamentale per prevenire accessi non autorizzati e garantire la sicurezza della rete aziendale;

- **DMZ (De-Militarization Zone)**: un'area di rete in cui vengono posizionati i server accessibili dall'esterno, come quelli per il traffico web (HTTPS) e la posta elettronica (SMTP). Questa zona funge da cuscinetto tra la rete interna sicura dell'azienda e l'internet pubblico, proteggendo i dati sensibili e le risorse interne da potenziali minacce esterne. I server nella DMZ sono configurati per fornire servizi agli utenti esterni, riducendo il rischio di accessi non autorizzati alla rete interna. In altre parole, la DMZ rappresenta una zona di sicurezza intermedia dove vengono collocati i server web e di posta elettronica per garantire un livello di protezione aggiuntivo alla rete aziendale interna;

- **NAS (Network-Attached Storage)**: un dispositivo in cui inserire della memoria di storage, un sistema di archiviazione totalmente condiviso. Viene usato per archiviare tutti i documenti importanti dell'azienda, a cui tutti gli host locali possono accedere. È quindi posto all'interno della rete locale;

- **IPS (Intrusion Prevention System) e IDS (Intrusion Detection System)**: software instal-

lati per proteggere le reti informatiche da attacchi esterni. La differenza principale tra i due risiede nelle loro funzionalità di risposta agli attacchi.

Un IDS si limita a monitorare il traffico di rete e segnalare i tentativi di intrusione attraverso messaggi di allarme. Questo consente agli amministratori di rete di essere avvisati tempestivamente degli attacchi, ma non interviene direttamente per bloccarli.

L'IPS, oltre a rilevare i tentativi di intrusione, agisce attivamente per impedirli. Quando rileva un potenziale attacco, non solo emette un allarme, ma blocca anche il pacchetto in entrata e l'indirizzo IP del mittente, prevenendo così l'intrusione.

Per questa ragione, l'IPS viene generalmente collocato presso i server web, dove può efficacemente bloccare le richieste sospette senza interferire con l'accesso legittimo ai file del NAS. Al contrario, l'IDS è tipicamente utilizzato a livello LAN e viene posizionato tra lo switch e il server locale o il NAS, monitorando il traffico interno senza bloccare direttamente alcuna comunicazione.

L'implementazione di IPS e IDS consente alle organizzazioni di migliorare significativamente la sicurezza della loro rete, offrendo sia una capacità di rilevamento tempestivo che una difesa attiva contro le minacce.