Pratica S2/L1 MARTA ARAMU

Consegna: 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. ● Spiegare le scelte.

Svolgimento: il cloud con la scritta WAN rappresenta internet e sta per Wide Area Network. Tutto il grafico è circondato è circondato da una rete LAN in cui troviamo in primis il Firewall, cioè un dispositivo o un software progettato per proteggere una rete informatica o un sistema da minacce esterne, regolando il traffico di rete in entrata e in uscita. Abbiamo un server web (server 1) e un server di posta elettronica (server 2). I server sono collegati ad una zona DMZ, detta anche «demilitarized zone», è un segmento di rete che espone servizi raggiungibili da internet o il servizio webmail.
Nella rete interna ho posizionato un NAS (Network-attached Storage) cioè un dispositivo di archiviazione dei dati dove è possibile conservare file digitali come foto, video, musica e documenti. Il NAS consente di accedere ai file tramite Wi-Fi o reti cablate in base ai casi di utilizzo. All'interno del NAS ho posizionato un IDS, cioè un sistema di sicurezza informatica progettato per rilevare e segnalare attività sospette o intrusioni nella rete o nei sistemi informatici. Quando rileva una potenziale minaccia, genera avvisi o notifiche per gli amministratori di sicurezza in modo che possano prendere provvedimenti. Un IDS non interviene direttamente per fermare l'attacco, ma fornisce solo una segnalazione. L'ho scelto al posto dell'IPS perché quest'ultimo, se non configurato correttamente, può generare dei falsi positivi e quindi bloccare del traffico legittimo. Ho scelto di usare l'IPS per la DMZ perché l''IPS opera in tempo reale per interrompere immediatamente l'attività dannosa o indesiderata: può agire in modo proattivo per fermare un attacco.
Il pacchetto, prima di arrivare ai server, incontra un primo muro chiamato WAF (Web Application Firewall) che è un componente di sicurezza informatica progettato specificamente per proteggere le applicazioni web da una varietà di minacce e attacchi online. Questo strumento si concentra sul livello delle applicazioni, analizzando il traffico Web in entrata e in uscita per identificare e bloccare attività sospette o pericolose.