# Esercizio S3-L4 Epicode

## Studente: Simone Mininni

## Traccia:

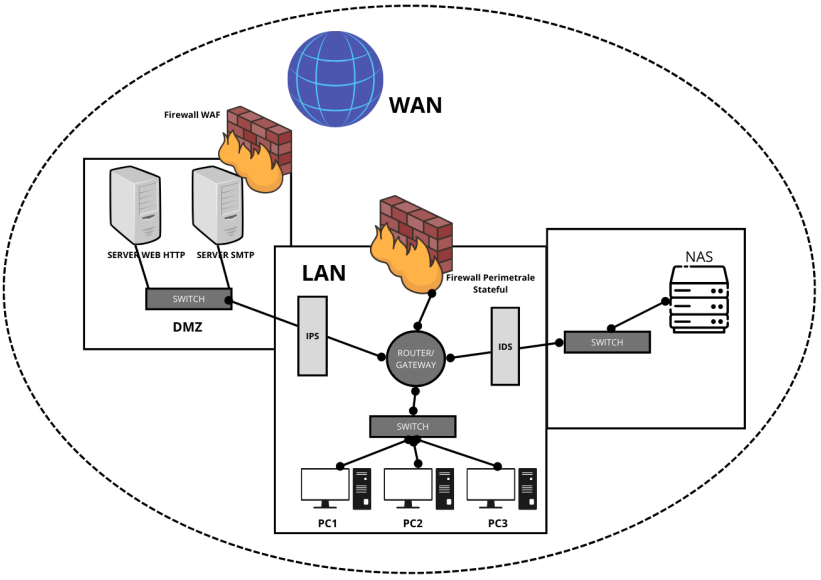
EPICODE — Cyber Security & Ethical Hacking
Compito

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.

## Disegno Rete:



# Relazione:

Supponiamo di essere in presenza di una rete aziendale.
Vado a determinare lo zoning, quindi ho tre aree in questa specifica situazione:DMZ, Area Pc, Area Server/NAS.
La LAN è protetta da un Firewall perimetrale per difendersi da minacce provenienti dall' esterno e utilizza uno steteful filtering o filtraggio di stato.
La particolarità di questo firewall è che tiene traccia dello stato delle connessioni, consentendo generalmente di far passare solo le connessioni iniziate dall'interno verso l'esterno.
Quindi dopo che si è stabilita una connessione tra la rete interna e quella esterna, il firewall tiene traccia degli indirizzi ip, porte del mittente e destinatario in modo che potrà consentire di far passare il pacchetto di response dalla rete esterna.
Ovviamente qualora sia una rete esterna a voler iniziare una connessione con la rete interna verrà bloccata, per questo si crea una DMZ, una zona demilitarizzata dove sono presenti i server accettano connessioni esterne e si interfacciano direttamente con il mondo, con la WAN.
Ovviamente anche i dispositivi presenti in questa zona dovranno essere protetti, ed utilizziamo una WAF, web application firewall.Questo si distingue per un tipo di filtering differente, in quanto va a controllare il contenuto del pacchetto proveniente dall' esterno e qualora viene rilevata una minaccia, un malware, viene bloccato.
Poi utilizziamo altri due dispositivi efficaci contro eventuali minacce:
IDS, Intrusion detection system e IPS, Intrusion prevention system.
IDS è un sistema di sicurezza che monitora costantemente il traffico della rete e qualora dovesse rilevare una minaccia lancia un segnale, un allarme che attenziona gli amministratori della sicurezza.
Mentre l' IPS ,oltre a lanciare un allarme, interviene automaticamente e blocca la minaccia.
Andando a posizionare un IDS e un IPS strategicamente, è preferibile posizionare il sistema IPS tra la DMZ e il resto della rete poiché qualora dovesse bloccare un falso positivo nella connessione con l' esterno non sarebbe un problema maggiore se invece bloccasse una connessione interna con i sistemi di archiviazione.Inoltre potrebbe creare maggiore latenza rispetto al sistema IDS rallentando le connessioni interne con il nas o i server.Inoltre ci si aspetta che la maggior parte degli attacchi o delle minacce arrivi proprio dal DMZ, dove ci sono i server web che comunicano direttamente con il mondo esterno, quindi l' IPS garantisce maggiore sicurezza.