•S3.E5

Traccia per il progetto Esercizio Segmentazione di rete 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

Esecuzione:

Il firewall è uno dei componenti principali della sicurezza informatica poichè protegge una rete informatica da minacce esterne.

Il firewall può essere sia software che hardware.

Il firewall software è un software che può essere scaricato e messe sui dispositivi, questo firewall utilizzerà le risorse del dispositivo stesso (se il dispositivo dispone di risorse limitate, minore sarà l'efficacia del firewall);

Al contrario il firewall hardware essendo un dispositivo a se, ha delle prestazioni migliori, ma allo stesso tempo ha un costo elevato.

Esistono diversi tipi di firewall e tra questi troviamo:

-Il firewall perimetrale, che come si intuisce dal nome si trova a perimetro tra la rete LAN (privata) e la rete WAN (pubblica)

-Il firewall non perimetrale, ovvero un firewall che si trova all'interno della rete:

- Firewall host (protegge solo il dispositivo)
- Firewall network (protegge tutti i dispositivi connessi a una bretella)

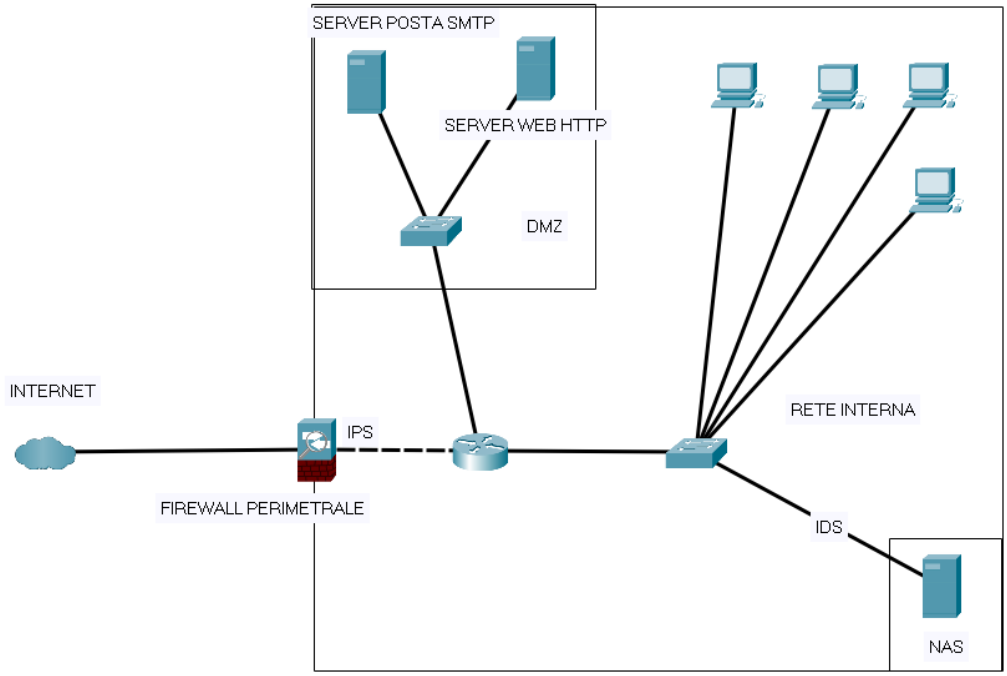
Di norma per grandi aziende è consigliabile il firewall hardware.

I firewall hanno quattro diversi tipi di filtraggio del traffico di rete, e sono:

- Filtraggio statico: valuta i pacchetti secondo dei criteri come l'indirizzo IP. Questi criteri vengo impostati manualmente, quindi il firewall controlla della sua tabella (ACL) quali indirizzi IP possono inviare pacchetti e quali invece deve bloccare, in più è importante ricordare che la lista verrà letta sempre dall'alto verso il basso, e verrà preso in considerazione il primo comando utile. Ad oggi questo filtraggio non viene più usato, sia perché vulnerabile al camuffamento dell'indirizzo IP, sia perché inserire manualmente ogni indirizzo IP esistente richiederebbe una quantità di tempo spropositata.

- Filtraggio dinamico: questa tipologia di filtraggio permette lo scambio di pacchetti solo se la connessione ha origine dall'interno verso l'esterno, e blocca ogni connessione se questa ha origine dall'esterno.
- Filtraggio a livello a livello di Applicazione (WAF): è un tipo di filtraggio che apre e legge il pacchetto in entrata alla ricerca di codice malevolo, per capire se si tratti o meno di codice malevolo confronta il codice del pacchetto con i codici presenti della sua tabella (può ricercare i codici anche su database esterni, che sono sempre aggiornati.
- Firewall Proxy: fungono tra intermediari tra rete interna ed esterna e camuffano l'indirizzo IP. Il firewall proxy a sua sua volta si divide in:
  1. Proxy forward
  2. Proxy reverse

L'esercizio ci chiedeva di realizzare la seguente rete:



Il filtraggio dinamico impedisce l'ingresso dei pacchetti provenienti dall'esterno; per risolvere questo problema è stata introdotta la DMZ, ovvero la zona demilitarizzata, che consente l'accesso dei pacchetti esterni. In questa zona si collocano i server che vogliamo rendere accessibili, come ad esempio il server di posta elettronica e il server HTTP, utilizzato per servizi come ad esempio pagine di e-commerce.

Ci viene anche chiesto di inserire dei sistemi di rilevamento delle intrusioni: IDS/IPS

L’IDS è uno strumento che ci aiuta nel rilevamento delle intrusioni, questo apre il pacchetto, verifica la presenza di codice malevolo e controlla se il pacchetto ha il permesso di entrare, nel caso in cui c’è qualcosa di anomalo l’IDS manda un allert e lascia a noi la decisione di come intervenire al riguardo.

L’IPS invece oltre a svolgere le stesse funzioni dell’IDS, blocca in maniera automatica il mittente del pacchetto.

Nell’esercizio ho deciso di posizionare l’IDS a "protezione" del NAS (dispositivo di archiviazione) e di utilizzare l’IPS per controllare i pacchetti provenienti dall’esterno.

Ho scelto questa configurazione perché sia l’IDS che l’IPS possono generare falsi positivi, ossia identificare come minacce utenti autorizzati ad accedere.

Ipotizziamo che il direttore, autorizzato ad accedere al NAS, venga erroneamente identificato come minaccia dall’IPS. In questo caso, l'IPS lo bloccherebbe immediatamente, impedendogli l'accesso ai dati necessari. Al contrario, l'IDS richiederebbe l'intervento di un operatore, il quale, riconoscendo che si tratta del direttore, autorizzerebbe l’accesso.