Esercizio S2-L2

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.

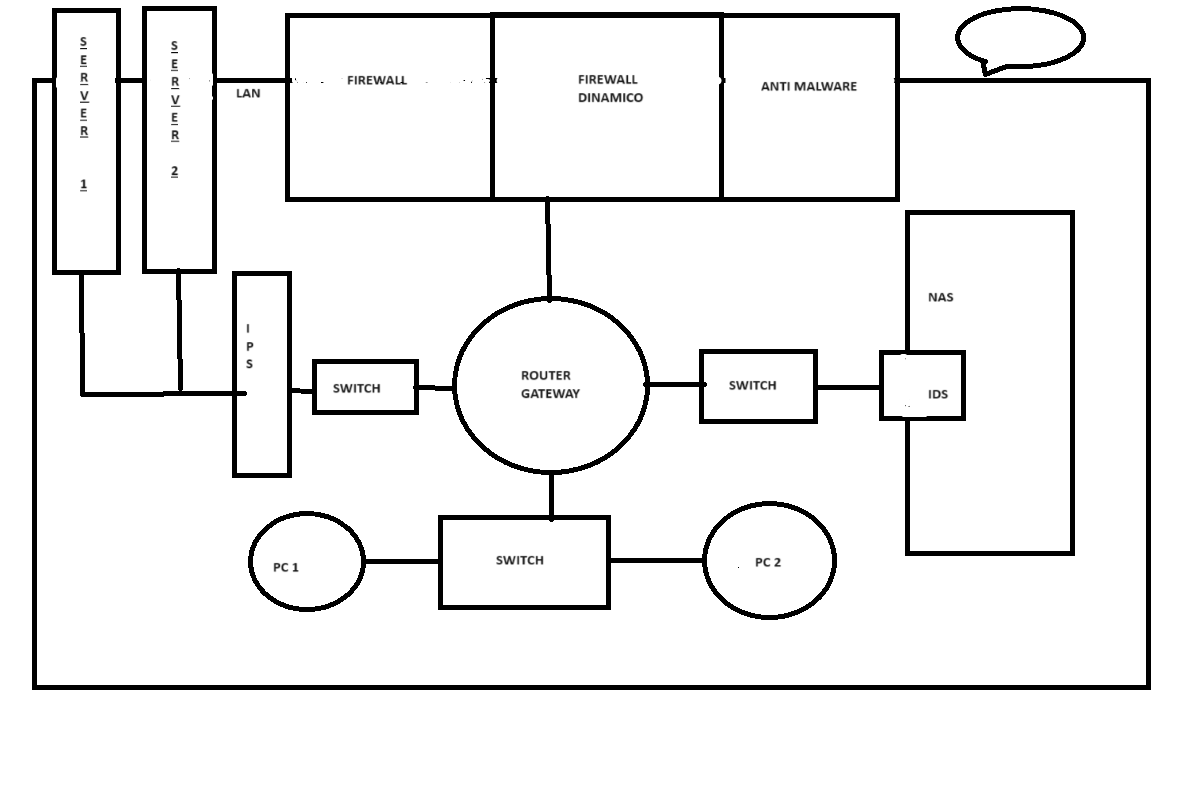
● Un firewall perimetrale posizionato tra le tre zone.

● Spiegare le scelte.

SERVER 1= APPLICAZIONE

SERVER 2= EMAIL

waf WAN



In questa Rete Lan possiamo trovare un Nas (dispositivo di archiviazione file collegato a una rete costituito da uno o più hard disk), un NGFW un dispositivo di sicurezza informatica moderno che opera dal livello 7 al livello 1 del modello ISO/OSI. Un firewall perimetrale tra LAN e WAN che difende il la rete da agenti esterni e consente il passaggio di dati solo verso l’esterno e si necessita di inserire un sistema DMZ. La DMZ o demilitarized zone, è un sistema informatico (sottorete fisica o logica) che consente il passaggio di informazioni sia dal client verso server che viceversa. La presenza di un firewall di tipo dinamico necessita obbligatoriamente di un DMZ per avere la possibilità di ricevere informazioni dall’esterno della rete privata. Gli IDS è un sistema di rilevamento dell’intrusione che funziona da allarme mentre gli IPS è un sistema di prevenzione dell’intrusione che ha sia modo di allertare in caso di un tentativo di accesso esterno.Andiamo quindi a collocare l’IDS in corrispondenza del NAS in modo che tutti riescano ad accedervi senza essere bloccati, mentre andremo a inserire l’IPS in corrispondenza dei due server, luogo in cui vi è più probabilità di ricevere un attacco. Abbiamo anche due Server uno dedicato al web (HTTP) e uno dedicato alla posta elettronica (SMTP). La WAF o Web Application Firewall è un firewall dinamico, opera a livello dei contenuti quindi legge l’indirizzo IP, porta e contenuto del pacchetto e bloccando quest’ultimo nel caso in cui il contenuto sia malevolo o sospetto. Possiede una tabella di riferimento dove vi confronta i contenuti del pacchetto controllando che tutto risulti benevolo. Contenuti come malware.exe vengono bloccati. Questo sistema difende al livello applicativo del sistema ISO/OSI.