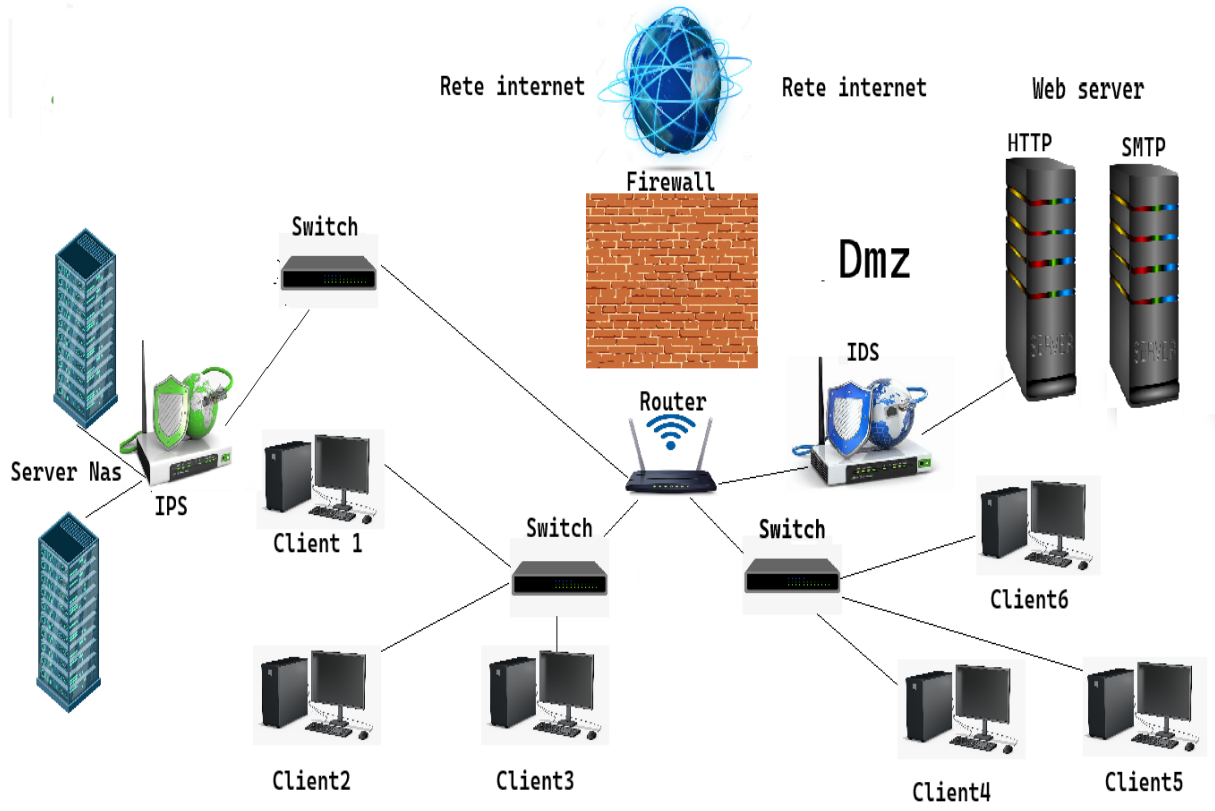
Progetto S3/L5

-Relazione di una rete aziendale e i suoi componenti

-"Prima di iniziare con la descrizione del progetto, vorrei precisare, che investire nella sicurezza in Internet non è solo una questione di proteggere i dati, ma è un aspetto cruciale per la sostenibilità e il successo a lungo termine di un'azienda. Con le minacce informatiche in continua evoluzione le aziende devono rimanere vigili e adottare misure proattive per proteggere i propri asset e garantire la fiducia dei clienti."

In questo progetto è stata creata una ipotetica rete aziendale, con tutte le relative protezioni contro le intrusioni di Malware.



In ogni rete aziendale che si rispetti l' uso del Firewall è fondamentale per la sicurezza informatica, poiché funziona da sistema di filtraggio controllando il traffico in entrata e in uscita, proteggendo i dati aziendali da minacce esterne e garantendo la sicurezza delle informazioni.

Non esiste modo migliore di descrivere un Firewall come muro invalicabile che ci protegge da tutte le intrusioni esterne. In questa rappresentazione il nostro muro rappresenta un Firewall perimetrale.

Un firewall perimetrale è un dispositivo di sicurezza, progettato per monitorare e controllare il traffico di rete, in entrata e in uscita tra una rete interna e il mondo esterno, come Internet. Si trova all'esterno della rete aziendale, fungendo da barriera tra la rete interna e le potenziali minacce esterne.

Al firewall per aumentare la sicurezza di filtraggio possiamo implementare una Web Application di nome WAF (Web application Firewall).

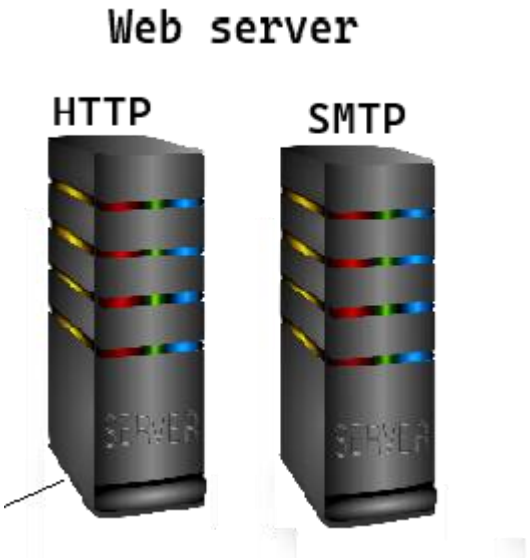
Cosa fa in più WAF?

Mentre negli altri Firewall erano fondamentali gli indirizzi IP ,poiché il sistema bloccava in maniera automatica gli indirizzi sconosciuti , considerati malevoli, con WAF avremo uno spacchettamento dei pacchetti e un controllo del contenuto, che se considerato malevolo lo bloccherà in automatico . Inoltre utilizza anche una tabella (ACL) esterna (oltre quella interna) per riconoscere con maggiore precisione i file malevoli.

Proseguiamo spiegando il motivo per cui abbiamo una DMZ (Demilitarized Zone) all'interno del nostro Firewall.

Prima di tutto la DMZ indica una sottorete che si trova tra la rete Internet pubblica e le reti private. Essa espone i servizi rivolti all'esterno alle reti non attendibili e aggiunge un ulteriore livello di sicurezza, per proteggere i dati sensibili archiviati su reti interne, utilizzando firewall per filtrare il traffico.

L’obiettivo finale di una DMZ è consentire a un’organizzazione di accedere a reti non attendibili, tra cui Internet, garantendo al contempo la sicurezza della propria rete privata o LAN. Le organizzazioni in genere archiviano nella DMZ servizi e risorse rivolti all'esterno, nonché server per il sistema dei nomi di dominio (DNS), FTP (File Transfer Protocol), posta, proxy, server Web.



Questi server e risorse sono isolati e dispongono di un accesso limitato alla rete LAN, per garantire che sia possibile accedervi tramite Internet, ma la LAN interna non può farlo. Di conseguenza, un approccio con la DMZ rende più difficile per un hacker ottenere l’accesso diretto ai dati e ai server interni di un’organizzazione tramite Internet.

Un ulteriore controllo per i nostri Server Web può essere l’utilizzo di un sistema di rilevamento intrusioni come l’IDS (Intrusion detection System).

L’IDS è un sistema che ha il compito di rilevare il traffico e monitorare attività insolite, che potrebbero indicare un attacco o una violazione della sicurezza.

Il suo funzionamento è molto semplice, arriva un pacchetto, lo apre, lo confronta con la sua tabella e se malevolo manda subito un allert, cosi da poter intervenire, bloccando il pacchetto.

Se per la protezione dei nostri Server Web utilizziamo un IDS, per proteggere dati sensibili contenuti nei Nas o Server all’interno della nostra rete, andremo ad implementare un altro sistema di rilevamento, l’IPS (Intrution prevention system). In questo caso l’IPS a differenza dell’ IDS ci apporterà una protezione maggiore, rilevando se presente un pacchetto malevolo, soltanto che in questo caso andrà a bloccarlo senza dover mandare nessun allert.

Ricordo inoltre che non basta soltanto l’utilizzo di Firewall per proteggere una rete aziendale, bisogna tenere sempre i nostri dispositivi e tutte le risorse presenti sempre in continuo aggiornamento e tenersi sempre pronti per far fronte a nuovi attacchi provenienti dall’ esterno, solo cosi potremo considerare una rete protetta.