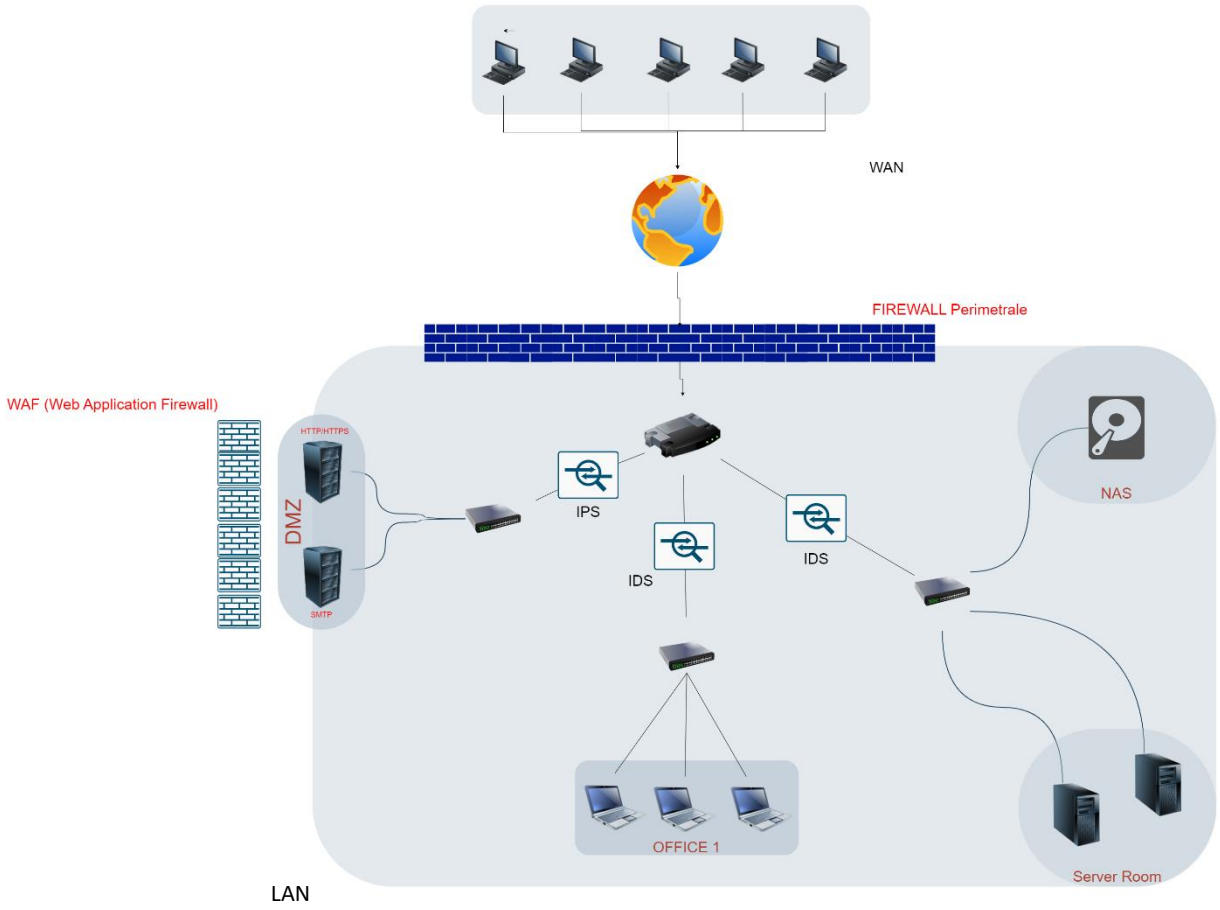
Settimana 3 Esercizio 4

Disegno di rete

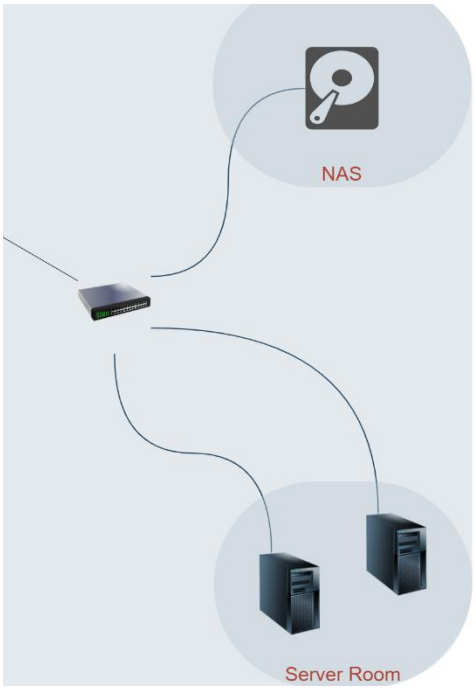
L'immagine che segue mostra un'ipotetica struttura di una rete aziendale:



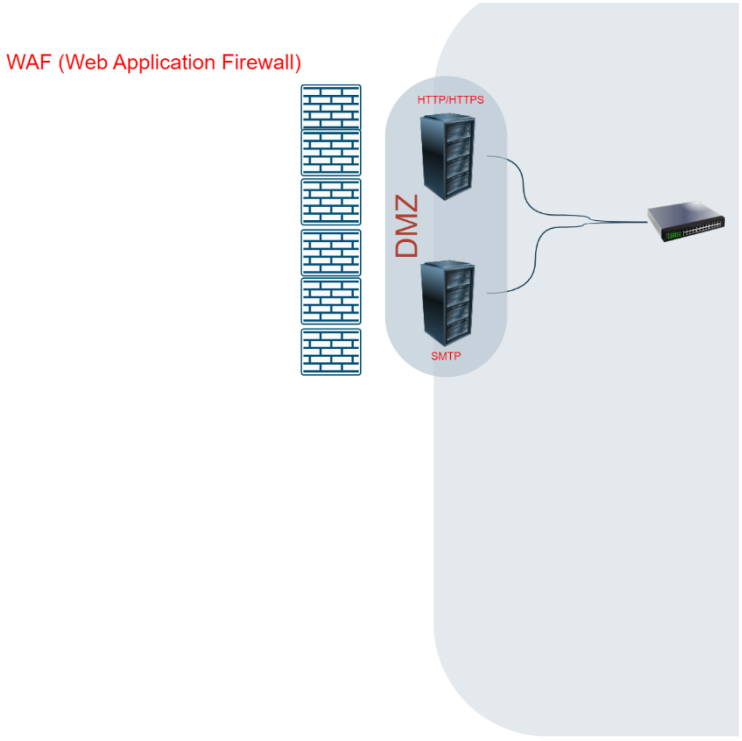
Vediamo più nello specifico come è stata pensata:

A. Abbiamo creato la nostra rete LAN interna;
B. Per prima cosa usiamo un firewall perimetrale per poter tenere al sicuro la rete. In questo caso lo andiamo ad utilizzare dinamico o Stateful Firewall che permetterà il traffico dall'interno della LAN all'esterno tenendo traccia delle connessioni. Anch'esso utilizza una tabella di registro per gli indirizzi IP che vogliamo raggiungere e, non appena finisce il collegamento, essa si cancella (memoria cache) bloccando quindi ogni richiesta di accesso da IP esterni ad eccezione di quelli inseriti in una ipotetica whitelist;
C. All'interno della rete abbiamo creato una zona dedicata ai server e alla NAS (Network Attached Storage), un dispositivo di archiviazione dati che li rende condivisibili agli utenti dell'azienda,

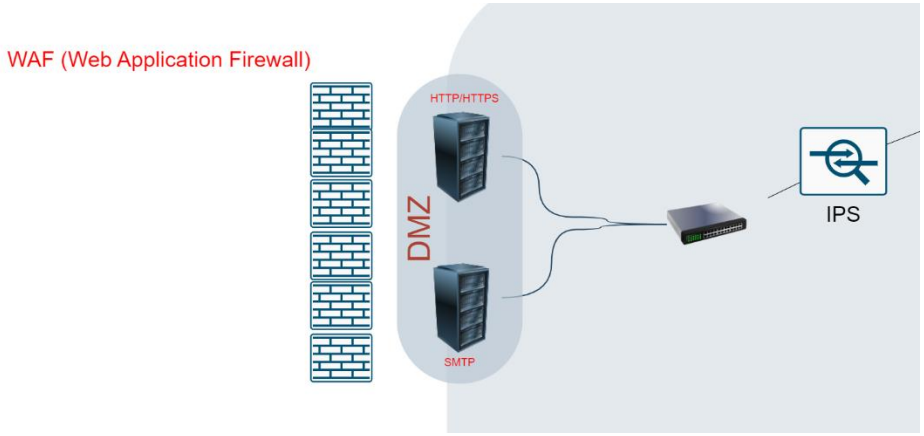
dispositivo **molto importante**. Spesso qui si archiviano dati molto importanti e sensibili, bisogno tenerlo bene al sicuro da attacchi malevoli;



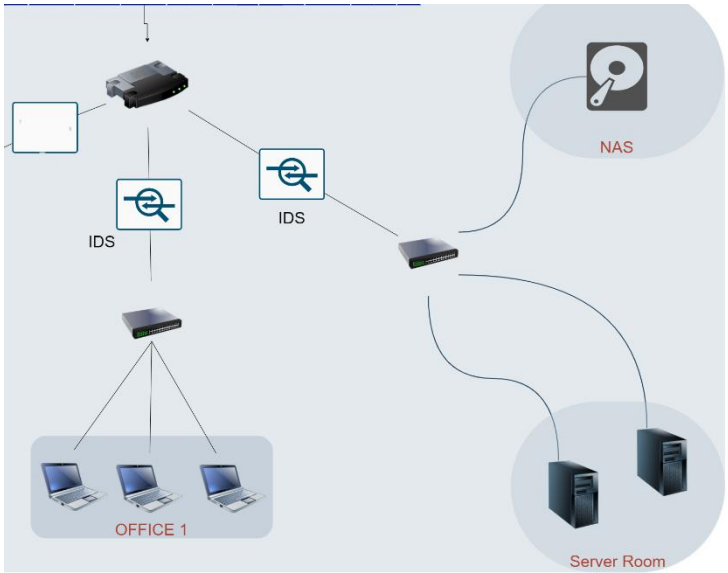
D. Creiamo anche una zona DMZ (Demilitarized Zone), molto importante se voglio fare sì che gli utenti possano accedere ai miei servizi (e-commerce, streaming etc). Questa sezione la si crea appositamente per poter rendere possibile l'accesso ai servizi offerti o ai servizi mailing (server http/https e SMTP). Di conseguenza si utilizza un WAF (Web Application Firewall) che utilizza il sistema OWASP di confronto (contiene tabelle dedicate per migliorare la sicurezza delle applicazioni) per proteggere adeguatamente la "porta d'accesso": esso infatti agisce sul traffico in entrata e in uscita e scansiona i pacchetti di dati rigettando quelli ritenuti malevoli e garantendo una protezione per tutti e 7 i livelli ISO/OSI;



E. A questo punto dobbiamo rendere la nostra rete interna ancora più sicura nel caso ci fosse una vulnerabilità da sfruttare. Utilizziamo un sistema di rilevamento delle intrusioni IDS o IPS: il rilevamento IPS è programmato per mandare un allert all'amministratore non appena trova un pacchetto malevolo e agisce attivamente alla minaccia rigettando i dati in automatico. Esso presenta una latenza maggiore rispetto all'IDS e crea qualche problematica nel caso in cui si dovesse imbattere in un tipo di dato non malevolo, ma ritenuto tale ("falso positivo"). Essendo più sicuro, ma più "lento", lo posizioniamo a cavallo tra la DMZ e il nostro router/gateway;



F. il rilevamento IDS è programmato per mandare un allert all'amministratore non appena trova un pacchetto malevolo, agendo passivamente facendo passare il dato. Esso possiamo andarlo a mettere a cavallo tra il router/gateway e le macchine dell'azienda e tra router/gateway e il sistema NAS–server. Anche se meno sicuro rispetto all'IPS, rende il tutto più veloce per attingere ai dati importanti dall'interno della LAN.



Questo è un esempio di una rete protetta con Firewall, WAF, IDS e IPS.