In questa rete abbiamo una lan composta da un router-gateway che collega 3 switch e si collega al firewall per la wan. Uno switch è collegato a 3 host, il secondo switch è collegato ad un IPS che fa da sistema di protezione dato che è collegato alla DMZ composta da due server (server email e server web) che per aver accesso ad internet i dati passano attraverso un WAF. Il terzo e ultimo switch si collega ad un IDS che fa pure lui da sistema di protezione per il NAS o sistema di archiviazione.
Il Firewall può essere un hardware o software ed è fondamentale per la protezione della rete interna, proteggendola da minacce analizzando il traffico di rete in entrata e uscita.
Il WAF (Web Application Firewall) è un sistema di sicurezza che si applica a livello applicativo, per proteggere il web analizzando il traffico dati in entrata ed uscita per bloccare i pericoli.
Viene messo come ‘’secondo switch’’ per i server web, perchè sarebbe impossibile fare continuamente accessi tramite un firewall normale che è molto più selettivo.
L’IDS monitora il traffico di rete e segnala solamente un’attività per lui pericolosa per la rete. Viene messo tra lo switch e il nas perchè può succedere che un attività può essere rilevata come minaccia mentre non lo è, quindi non c’è bisogno di bloccare la minaccia.
L’IPS fa lo stesso lavoro dell’IDS però allo stesso tempo blocca in tempo reale le minacce trovate.
Viene messo tra lo switch e la DMZ perchè la DMZ è accessibile a tutti quindi l’IPS se trova una minaccia la deve anche bloccare perchè troppo esposti a pericoli esterni.
La DMZ (Demilitarized zone) è una parte della rete accessibile da internet per esempio un sito web, è bisogno che venga protetta in modo efficace.
Nel disegno infatti ho messo la DMZ che contiene i due server esposti a internet.