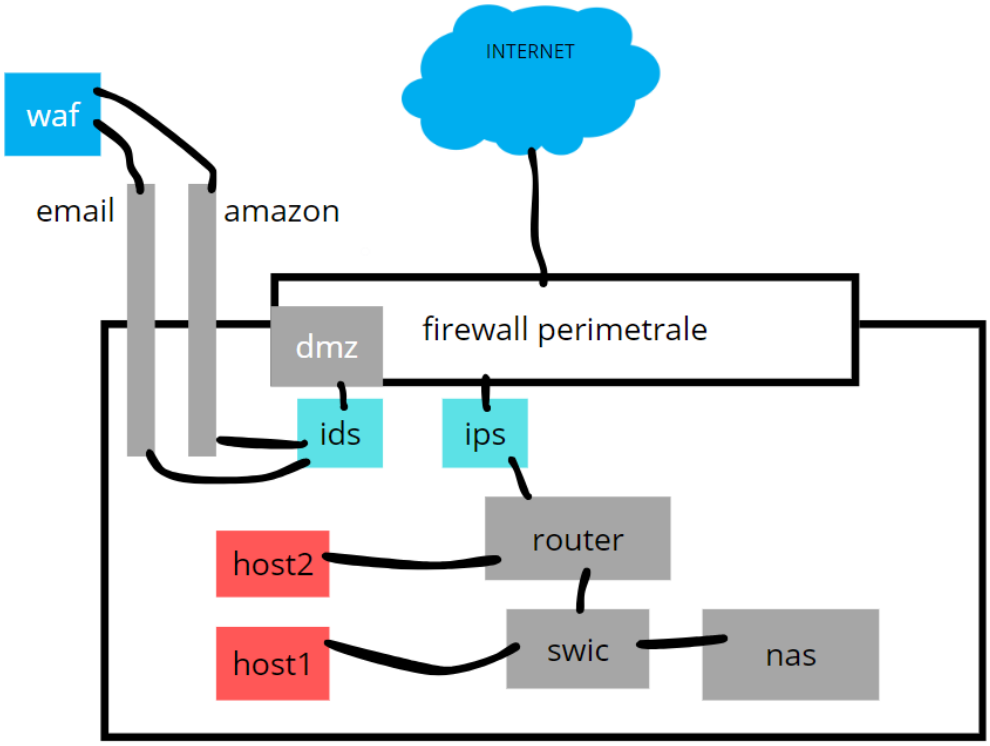
S3L5



Nello schema che segue vediamo esempio di rete. Il firewall presente è di tipo perimetrale, ovvero un firewall che protegge tutta la rete e si trova fra la rete locale e la rete wan (internet), possiamo vedere che nel firewall è presente anche la dmw(area demilitarizzata), la dmz permette l'invio di pacchetti dall'esterno della rete privata. Possiamo vedere che un pacchetto prima di arrivare alla dmz dovrà passare per la waf(web application firewall), che esamina il contenuto del file e se è malevolo lo blocca, subito dopo abbiamo un altro sistema di sicurezza che è l'ids, questo sistema controlla nuovamente i file in ingresso e nel caso sono dannosi invia notifiche all'amministratore di rete. Se il file è pulito passera i due sistemi di sicurezza e arriverà al dmz. Il

firewall permette l’accesso alle richieste in uscita dalla rete locale. Possiamo vedere che dopo il firewall è presente l’ips che è un altro sistema di sicurezza che a differenza del ids rileva e cancella il file malevolo. Lo abbiamo inserito dopo del firewall (che fa da prima difesa) cosi che possa analizzare il traffico e insieme la sicurezza della rete è maggiore. Il nas ci permette di condividere e immagazzinare dati, al suo interno è presente un sistema operativo che gestisce l’archiviazione dei dati.

RICERCA SUL FIREWALL

Il firewall è un sistema di sicurezza che controlla i pacchetti in entrata e in uscita da una rete. Viene spesso definito come un guardiano che controlla l'ingresso in una citta. Ci sono vari tipi di firewall ovvero quello hardware e quello software, le differenze sono:

- Quello **software** è un firewall che si installa su un pc è la sua potenza di calcolo sarà limitata alla potenza di calcolo del pc dov’è installato. Questo tipo di firewall è molto usato per via del suo costo.
- Quello **hardware** ha una struttura fisica indipendente da quella del pc. Quindi dispone di una potenza di calcolo maggiore del firewall software. Il lato negativo è che questo tipo di firewall è molto costoso.

Queste differenze non vogliono dire che uno è meglio di un altro, un'azienda deve valutare l’uso di questi firewall in base: alle dimensioni dell'azienda, alla disponibilità economica e al numero

di connessioni. Ad esempio un'azienda con 30 dipendenti avrà meno connessioni rispetto ad un'azienda con 500 dipendenti, quindi nell'azienda piccola si può usare il firewall software mentre in quella grande si deve usare quello hardware.

I firewall possono essere posizionati:

- su un solo dispositivo e in questo caso si chiama firewall host ovvero che protegge il singolo dispositivo.
- tra i dispositivi e la rete, in questo caso si chiama firewall perimetrale. Questo sistema è progettato per proteggere l'intera rete.

Il firewall ha 4 tipi di filtraggio che sono:

- Filtraggio statico, ovvero le decisioni sui file che entrano nella rete vengono scritti dall'amministratore di rete, quest'ultimo imposterà quali file entrano tramite: indirizzi ip, porte d'entrata e uscita e se il protocollo è consentito. Ad esempio se blocchiamo l'IP 192.168.1.2 alla porta 80 (http) e al firewall arriva una richiesta da questo indirizzo con questa porta lui lo blocca.
- Filtraggio dinamico, è quello più usato e accetta le richieste in uscita e non quelle in entrata, ovvero se io mi connetto al server di YouTube lui lascia passare i pacchetti e memorizza i dati su una memoria cash che si cancella una volta chiusa la connessione. Se dopo la chiusura l'indirizzo privato di YouTube cerca di stabilire una connessione con noi, il firewall lo blocca.

- Filtraggio per contenuto (Waf), il waf(web application firewall) ispeziona il contenuto del file e se sono dannosi li blocca mentre se non sono dannosi li fa passare.
- Il proxy è un server che si mette fra due indirizzi IP, fa da intermediario che controlla il contenuto dei file. Il suo vantaggio è la sicurezza mentre lo svantaggio è che può risultare un po' lento. I proxy server invece agiscono tra utente e server.

La zona dmz(zona demilitarizzata) è una zona di accessibilità che permette le connessioni in entrata dall'esterno, questo sistema espone il dispositivo a dei rischi. Per risolvere i problemi di sicurezza nella dmz inseriamo il waf.