DMZ/FIREWALL

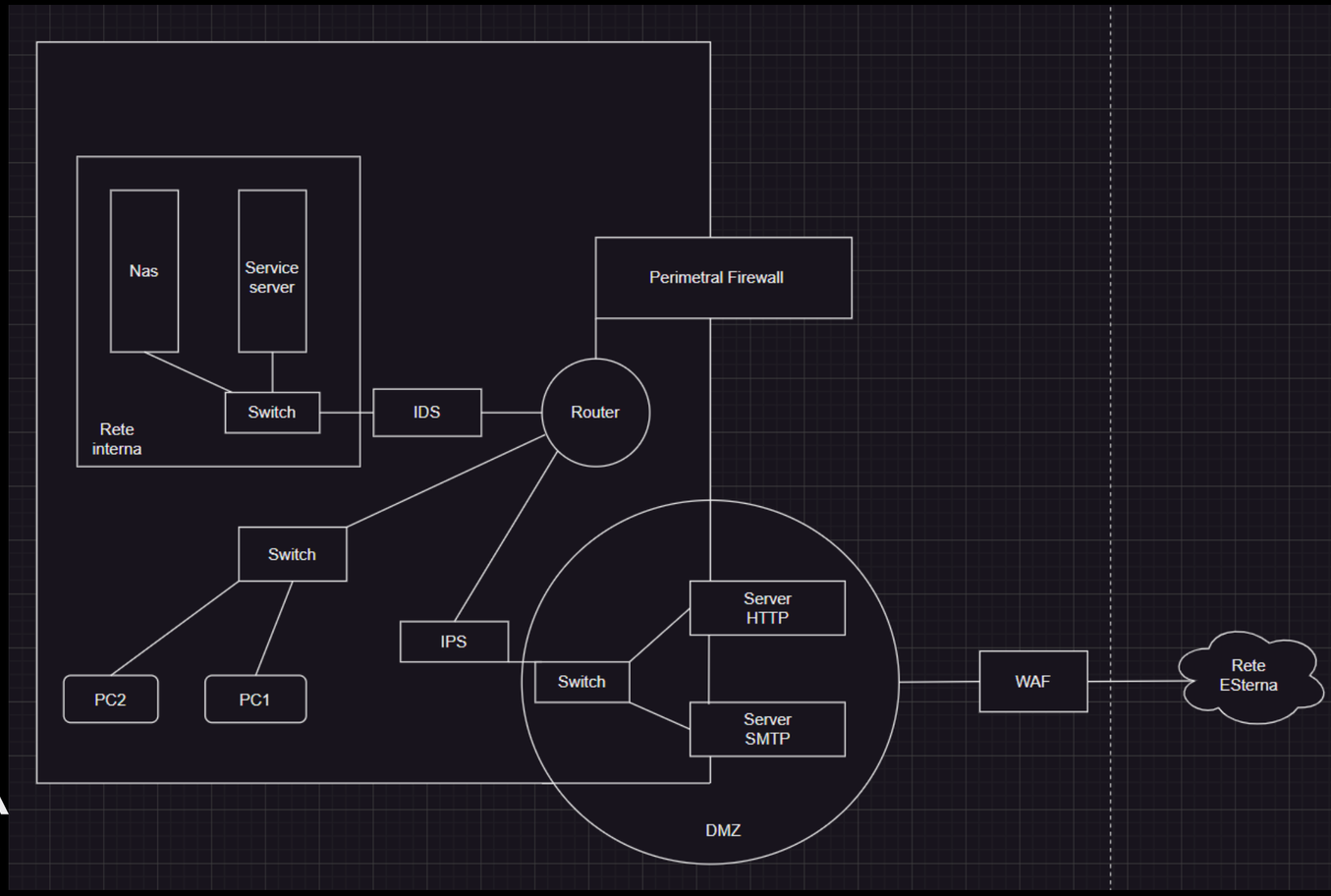
Ernesto Robles

DMZ/FIREWALL

LO SCHEMA ILLUSTRA UNA RETE AZIENDALE COMPOSTA DA UNA DMZ E UNA RETE INTERNA.

CON IL WAF OCCUPA TUTTO IL TRAFFICO DESTINATO AI SERVER WEB NELLA DMZ DEVE PASSARE ATTRAVERSO SE STESSO PRIMA DI RAGGIUNGERE I SERVER STESSI, QUANDO IL WAF RILEVA UN COMPORTAMENTO SOSPETTO O UNA POTENZIALE MINACCIA, BLOCCA LA RICHIESTA O INTRAPRENDE AZIONI COME L'INVIO DI UNA NOTIFICA ALL'AMMINISTRATORE DI SISTEMA

IL FIREWALL PERIMETRALE SI OCCUPA DI AGIRE COME UNA BARRIERA TRA LA RETE INTERNA E LA DMZ.
IL FIREWALL IMPEDISCE AL TRAFFICO DANNOSO O NON AUTORIZZATO CHE VIENE DALL'ESTERNO DI PENETRARE NELLA RETE INTERNA E CONTROLLA IL TRAFFICO CHE ENTRA E ESCE NELLA DMZ, GARANTENDO CHE SOLO IL TRAFFICO AUTORIZZATO RAGGIUNGA I SERVER AL SUO INTERNO



DMZ/FIREWALL

IDS IN QUESTA POSIZIONE MONITORA IL TRAFFICO IN ARRIVO E PERMETTE DI RILEVARE POTENZIALI MINACCE O ATTIVITÀ SOSPETTE IN TEMPO REALE. L'USO DI IDS MI PERMETTE DI NON ANDARE INCONTRO A FALSI POSITIVI COME POTREBBE SUCCEDERE CON L'IPS IN OGNI CASO L'IDS SEGNALA IL POTENZIALE FALSO POSITIVO MA NON LO BLOCCA.

IPS IN QUESTA POSIZIONE ESAMINA IL TRAFFICO PRIMA CHE RAGGIUNGA I SERVER NELLA DMZ, QUESTO PERMETTE ALL'IPS DI PRENDERE AZIONI IMMEDIATE PER BLOCCARE EVENTUALI ATTACCHI O ATTIVITÀ SOSPETTE.