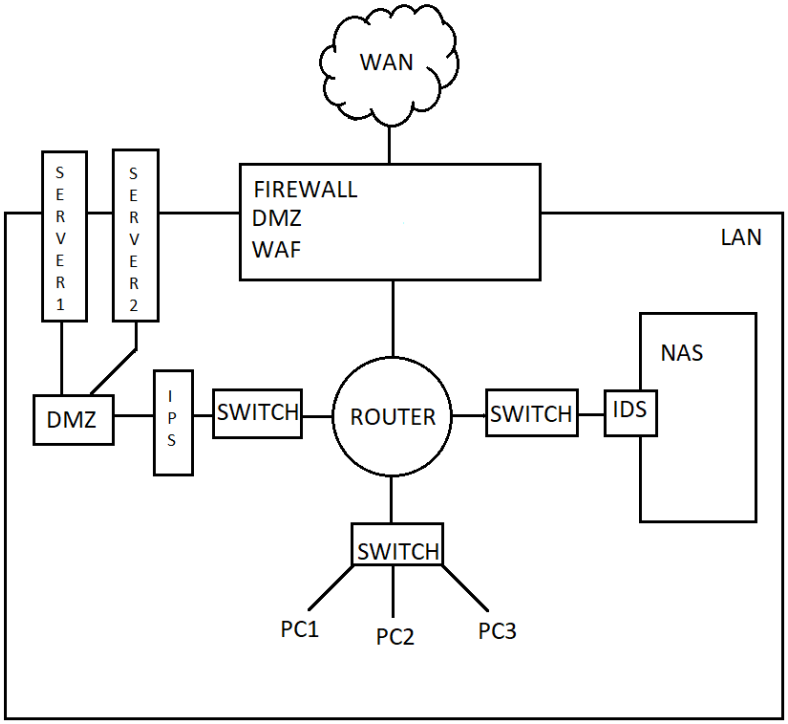
Compito S2/L1



Nella rappresentazione sopra, le linee rappresentano il flusso del traffico tra le diverse zone, e il firewall perimetrale controlla e filtra il traffico tra Internet, la DMZ e la rete interna.
La DMZ contiene almeno un server web (HTTP) e un server di posta elettronica (SMTP), mentre la rete interna ha almeno un server o un Network Attached Storage (NAS).
Il WAF (web application firewall) protegge le applicazioni web da attacchi malevoli o vulnerabilità di sicurezza, utilizzando soluzioni esterne come OWASP.
Questa configurazione è progettata per fornire una sicurezza a strati, con il firewall perimetrale che controlla il traffico tra le diverse zone per impedire accessi non autorizzati e proteggere le risorse più sensibili nella rete interna.
Questo approccio è comune nelle infrastrutture di rete aziendali per migliorare la sicurezza e limitare l'accesso non autorizzato alle risorse interne.
IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) sono entrambi strumenti utilizzati per la sicurezza delle reti, ma hanno scopi leggermente diversi.
IDS- Rileva le attività sospette o intrusioni nella rete o nei sistemi.
IPS- Previene gli attacchi bloccando il traffico sospetto.
In breve la differenza principale tra IDS e IPS è che IDS è più orientata alla rivelazione e agli avvisi, mentre un IPS oltre ad avvisare va a fermare un attacco, per questo non mettiamo IPS per non avere un falso positivo.