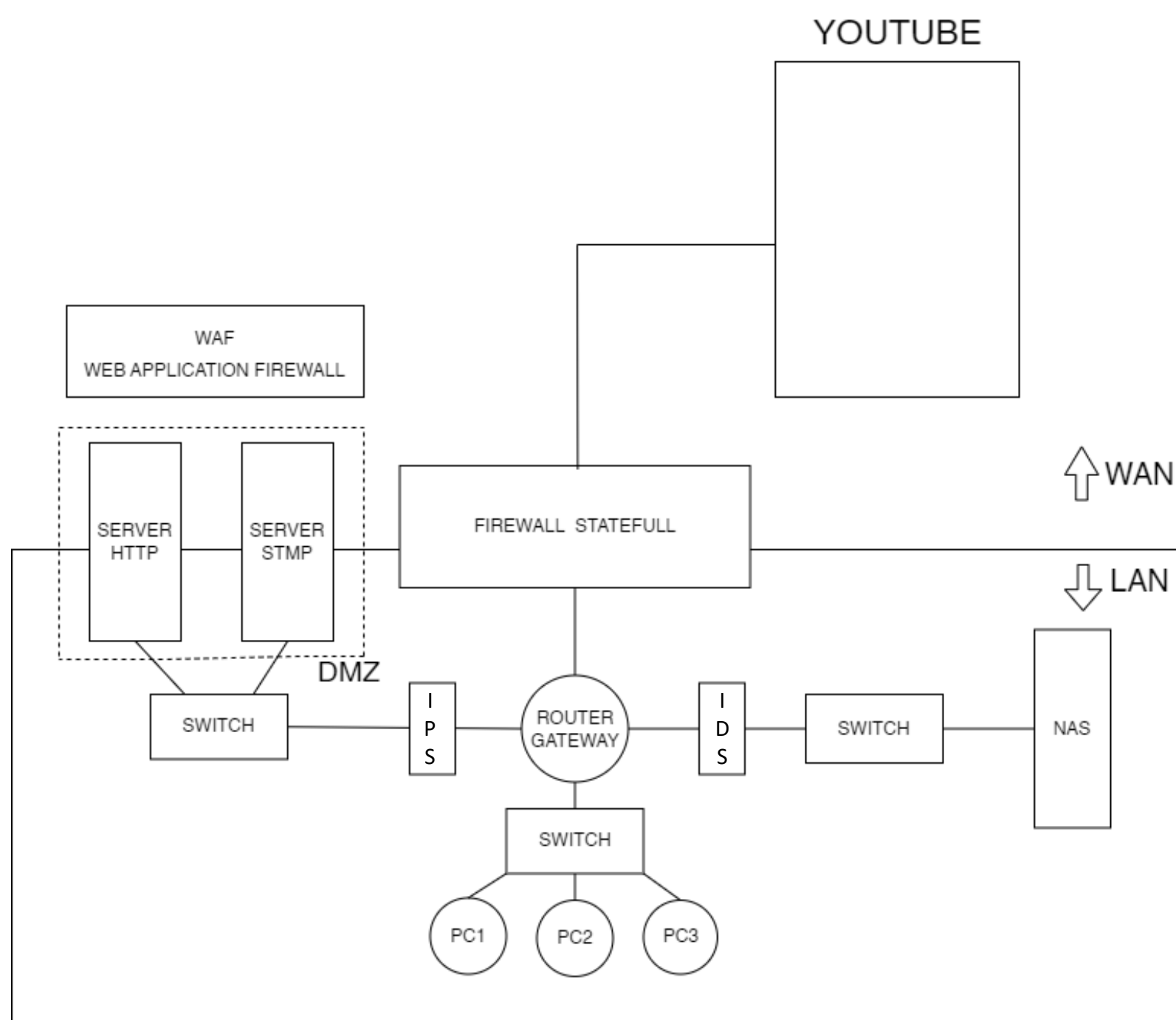


EPICODE esercizio 12.10.2023

Illustrare una rete LAN che comunica con una rete WAN e indicare i passaggi.



Il server di youtube nella rete WAN comunica con la nostra rete LAN (PC1,2,3).

PC1 cercherà di connettersi al server di YT nella rete WAN passando i pacchetti attraverso questi 3 dispositivi: Switch, Router Gateway e Firewall Statefull.

Quando i pacchetti passeranno per il Firewall, esso salverà questi dati in un compartimento dedicato della propria lista ([con questo tipo di Firewall possiamo solo inviare pacchetti in uscita da un client con indirizzi IP e porte autorizzate](#)). Questi dati saranno pacchetti in uscita e in entrata tra PC1 e Youtube che continueranno in sequenza finché PC1 non terminerà la connessione.

Il problema di questo Firewall con filtraggio dinamico è che le reti esterne non possono entrare nella nostra, perciò abbiamo bisogno di una «porta aperta». Questa «porta» prende il nome di DMZ, dove all'interno metteremo due Server, uno per il protocollo HTTP ([siti web](#)) e l'altro per il protocollo SMTP ([email](#)). Dato che la DMZ è vulnerabile ad attacchi esterni, ci sarà una WAF che farà da filtro ai pacchetti in entrata nei server([la WAF legge/analizza direttamente il contenuto del pacchetto, nel caso fosse malevolo non lo accetta](#)).

Per un check di sicurezza in più metteremo un dispositivo IPS([intrusion prevention system](#)) dalla parte della DMZ nel caso il WAF facesse passare dei pacchetti indesiderati.

Dall'altra parte della rete, avremo una NAS con affianco allo switch un dispositivo IDS ([intrusion detection system](#)), per un semplice check dei client che vorranno accedervi. Non abbiamo il bisogno di fare un controllo approfondito perché poi potremmo avere un importante ritardo sul passaggio di dati tra NAS e client.