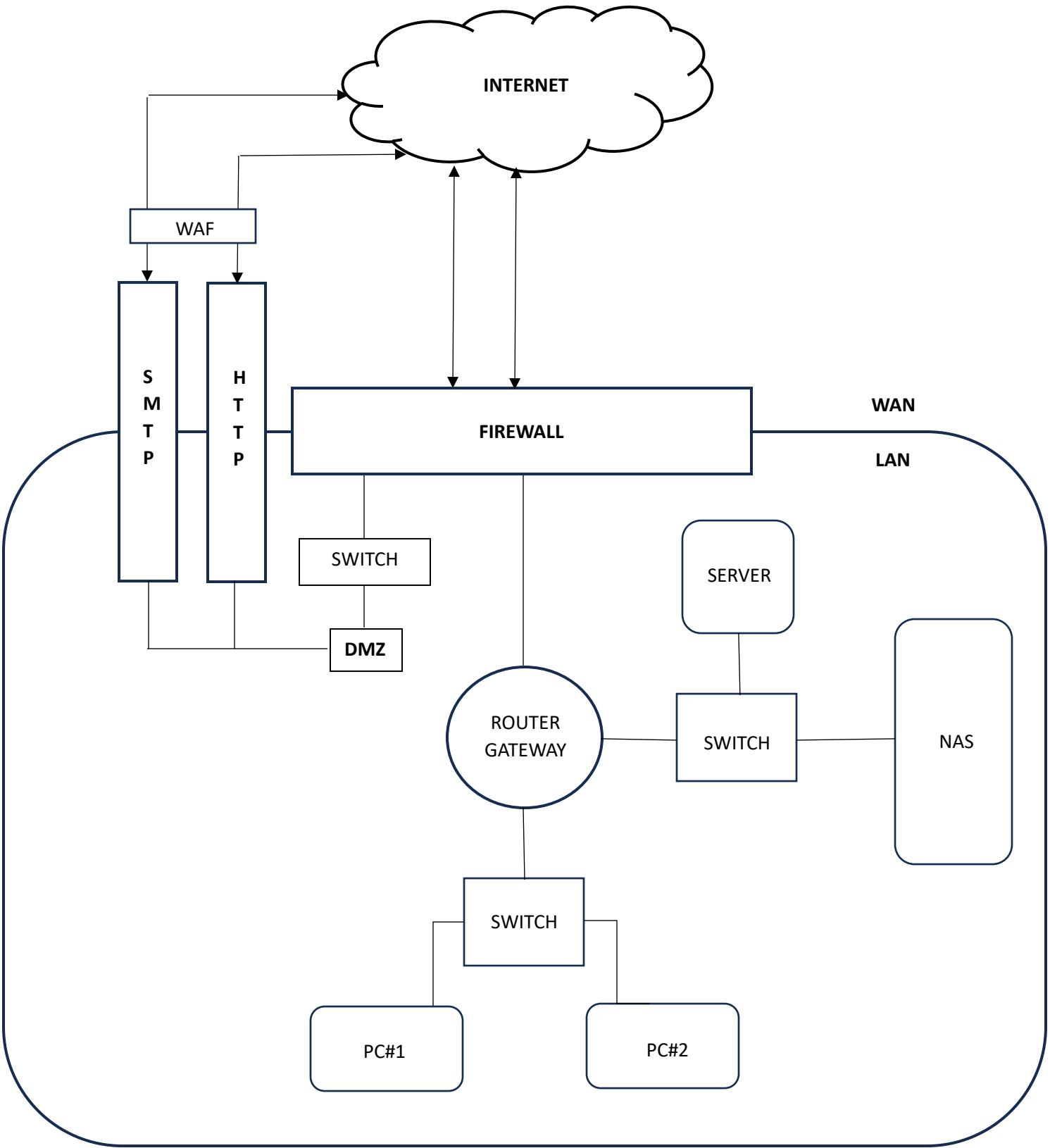


CONSEGNA [SETTIMANA 2 LEZIONE 1]



Nella rappresentazione soprastante è raffigurata graficamente una rete LAN, con i seguenti dispositivi/software di rete:

- **1 router-gateway**
- **3 switch**
- **1 server**
- **1 firewall**
- **1 waf**

In questa rete ho inserito un firewall di tipo dinamico, in quanto necessario per la sicurezza delle connessioni in ingresso/uscita. Questo tipo di firewall non impone una tabella ACL fissa, ma bensì costruita dinamicamente quando un host all interno della rete si connette ad un server esterno, consentendo così lo scambio di pacchetti.

Questa configurazione quindi, ipotizzando la necessità di servizi http e smtp, necessita di una zona detta dmz, ovvero dove è consentito l accesso ad indirizzi IP esterni solo in tale sezione, senza la necessità di un controllo tramite la tabella ACL.

Per rendere ulteriormente sicura la nostra rete, è consigliabile usufruire di uno strumento detto WAF ( web application firewall ), che ha la capacità di analizzare il contenuto dei pacchetti in ingresso e in uscita per bloccare eventuali file malevoli. Questo componente è inserito, nel nostro caso graficamente, prima dell accesso ad eventuali pagine web della rete o server di posta. Per funzionare, il WAF necessita di una lista, spesso reperibile sui database di organizzazioni specifiche, comprendente i nomi e le relative estensioni dei file malevoli conosciuti.

Infine, in caso volessimo una ulteriore protezione da eventuali minacce informatiche, sarebbe possibile inserire due sistemi di sicurezza chiamati IDS e IPS.

L'IDS ha come scopo principale quello di rilevare e segnalare attività sospette o intrusioni, controllando costantemente il traffico della rete in ingresso. L'IPS invece, si occupa della rilevazione/segnalazione ma anche dell'annientamento di tali minacce.