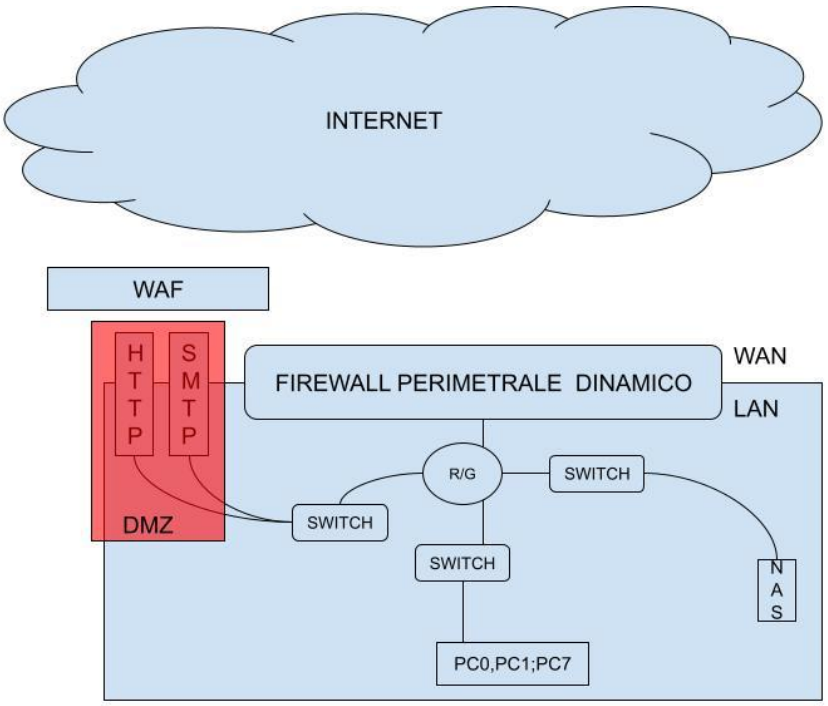

Nell’esercizio di oggi abbiamo realizzato una rete LAN con firewall perimetrale dinamico.
Il firewall perimetrale consente di creare una protezione tra la rete interna e le minacce che potrebbero provenire dall’esterno
A differenza del firewall statico che ha delle regole (ALLOW,DENY) basate su indirizzi ip e porte, il firewall dinamico consente di tenere traccia delle connessioni che partono dall’interno della rete e quindi permettere uno scambio di pacchetti .

Nello schema precedentemente realizzato ci sono esattamente tre zone:

- Rete internet (wan)
- Rete intranet (o rete interna, o lan)
- Rete DMZ
    - La rete DMZ (Demilitarized Zone) è un’area intermedia tra la zona interna (lan) e la’ zona esterna (internet) e serve per delimitare la zona di intranet che può essere accessibile pubblicamente senza incorrere in blocchi da parte del firewall dei pacchetti provenienti da client esterni. *Ad esempio se utente A che è al di fuori della rete di Google vuole raggiungere YouTube e i server di quest’ultimo non si troverebbero in una zona DMZ non riuscirebbe a raggiungerlo.*

Nel caso specifico si rende accessibile a tutti lo scambio di pacchetti con i due server HTTP e SMTP.
Troveremo a monte della zona demilitarizzata un WAF che permette un livello aggiuntivo di sicurezza, essa analizza i pacchetti provenienti dai diversi client e decide se bloccare la richiesta o meno in base anche ai propri database (interni o esterni), permettendo una protezione maggiore della zona