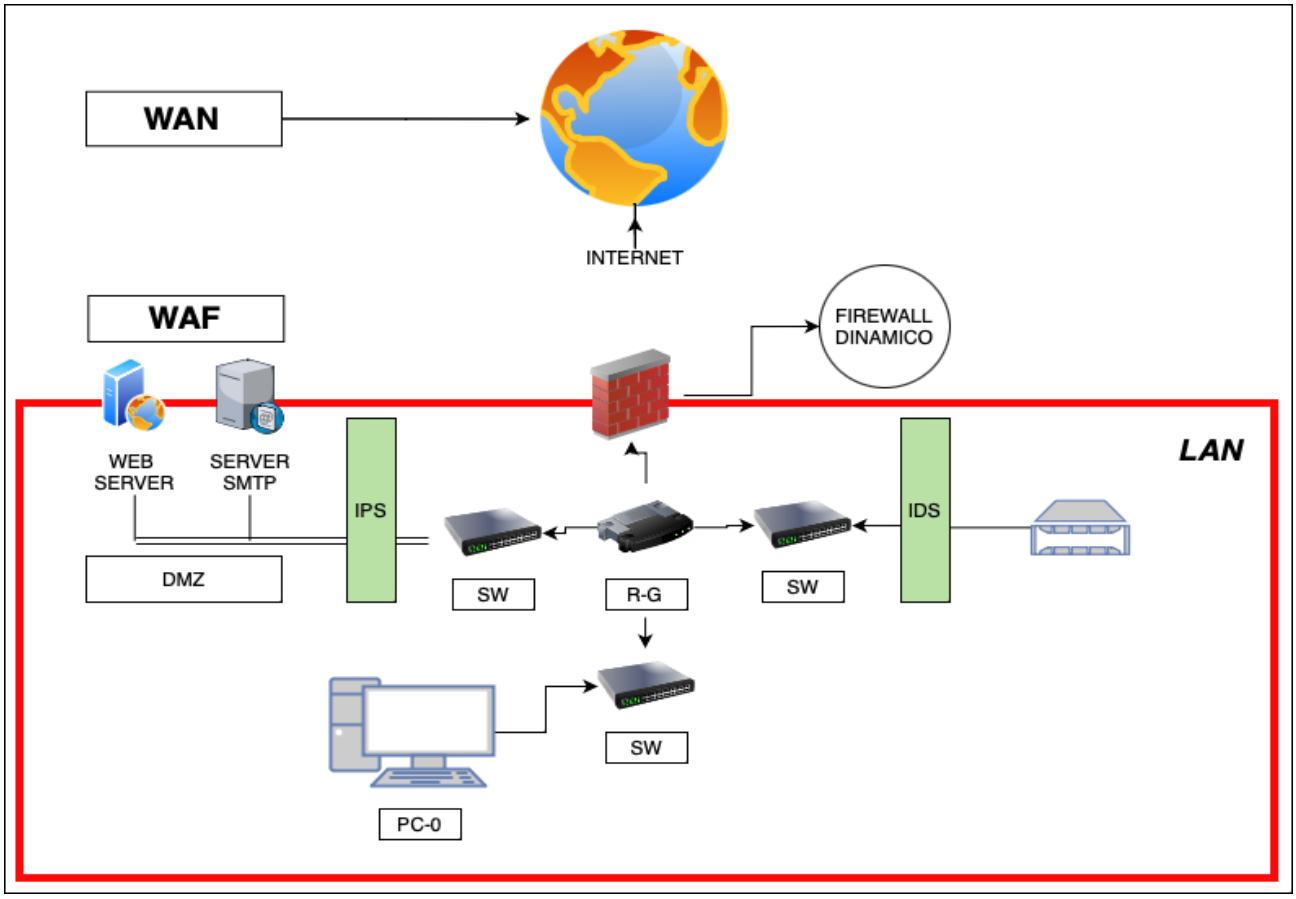

Compito di oggi: disegnare una rete con i seguenti componenti:

- Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).
- Una zona DMZ con almeno un server web (HTTP) e un server di posta elettronica

  (SMTP).

- Una rete interna con almeno un server o NAS.
- Un firewall perimetrale posizionato tra le tre zone.
- Spiegare le scelte.

  Firewall dinamico: firewall perimetrale (standard odierno)
  Permette connessioni di tipo interno verso esterno.
  Esempio: PC-0 tenta di accedere a un server web esterno alla sua LAN.

  Come funziona: presenta due tabelle.

- La prima tabella contiene tutti gli indirizzi IP della rete LAN dove è presente.
- La seconda tabella (ACL) con memoria volatile salva l'indirizzo IP esterno con il

  quale si comunica.

  Una volta che i vari host della rete chiudono la connessione con gli host esterni alla rete, l'IP inserito nella cache della seconda tabella viene resettato.

Poiché all'interno del firewall dinamico la connessione deve partire dall'interno, i server WEB (esterni) sono predisposti in una zona demilitarizzata (DMZ).

Poiché la DMZ è accessibile a tutti (quindi vulnerabile), viene introdotto un altro tipo di firewall, il WAF (Web Application Firewall).

Il WAF, a differenza degli altri tipi di firewall, "scannerizza" anche il contenuto del pacchetto, leggendolo e confrontando il suo contenuto con una tabella alla ricerca di contenuti malevoli.

Per rendere questa rete più sicura, vengono introdotti sistemi IDS e IPS.

- IDS - IPS: sono lo stesso dispositivo/software.

  - IDS => Intrusion Detection System
  - IPS => Intrusion Protection System

L'IDS prende il pacchetto, lo spacchetta, lo confronta con una sua lista/tabella alla ricerca di possibili elementi malevoli; se trova elementi malevoli, invia un alert/notifica (IDS passivo). Al contrario, l'IPS, oltre a inviare l'alert, blocca anche l'indirizzo IP del mittente (IPS attivo). Nonostante sembrino uguali, anzi, l'IPS è più utile; viene utilizzato anche l'IDS per una questione di falsi positivi. Al fine di evitare il blocco di un IP che potrebbe sembrare malevolo a causa di un falso positivo, viene solo inviato un alert al security.