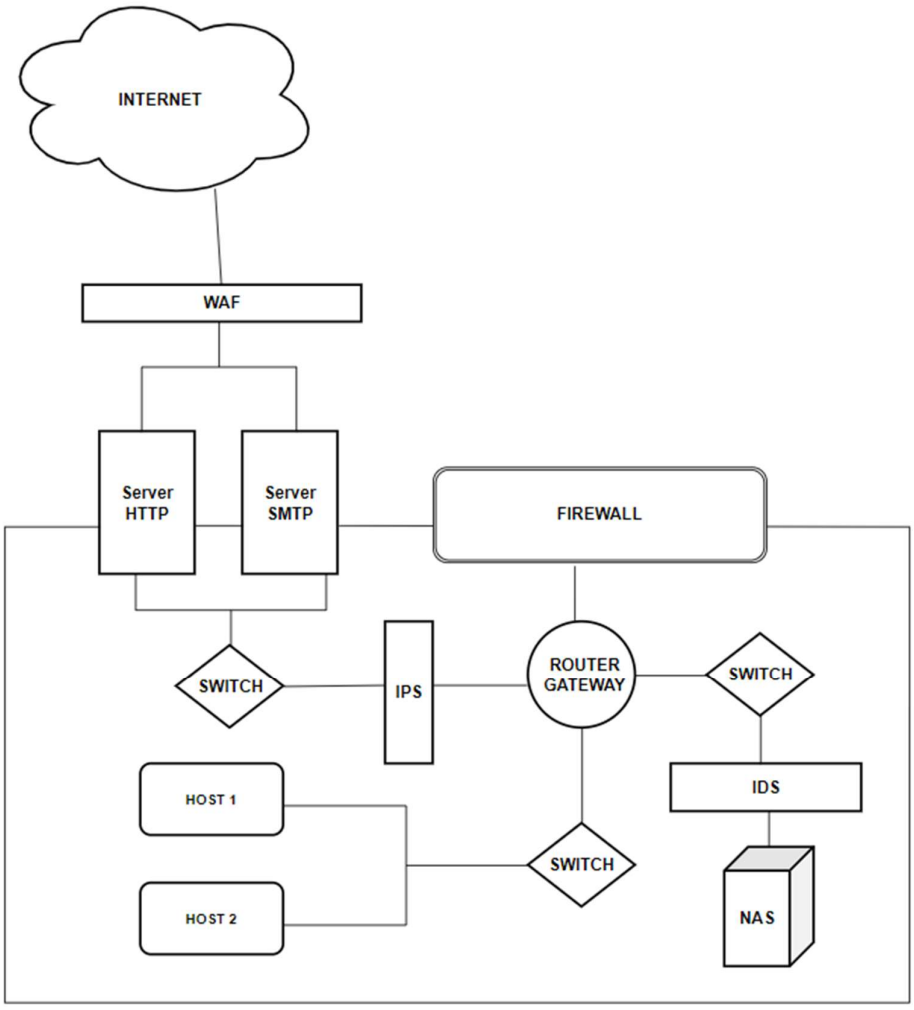
Compito di oggi disegnare una rete con i seguenti componenti:

- 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.
- Un Sistema di Rilevamento delle Intrusioni (IDS) posizionato strategicamente nella rete.
- Un Sistema di Prevenzione delle Intrusioni (IPS) posizionato strategicamente nella rete.

Spiegare le scelte.



Nel grafico precedente possiamo constatare la DMZ (Demilitarized Zone), ovvero quella parte della rete aziendale che contiene ed espone determinati servizi alla rete esterna.

Possiamo notare in questo esempio che i servizi facente parte della DMZ sono il server HTTP e il server SMTP; tra loro e la rete Internet si interpone la WAF (Web application firewall) un componente di sicurezza informatica con lo scopo di proteggere le applicazioni web dalle minacce esterne.

Successivamente vi è il Firewall perimetrale utilizzato per proteggere la rete interna dalle minacce esterne, è consigliato che si tratti di un firewall con tipologia di filtraggio "Stateful Filtering".

Vi sono poi 2 ulteriori strumenti informatici che aiutano nella protezione della rete: sono l'IDS e l'IPS detti anche IDS passivo e attivo.

Entrambi svolgono una funzione di analisi del traffico di rete inviando una notifica agli amministratori di security qualvolta si rilevi una potenziale minaccia. L'IPS oltre che a notificare, può intraprendere anche azioni attive per bloccare gli attacchi, quali possono essere il blocco del traffico sospetto o la disconnessione degli utenti; purtroppo questa ulteriore funzionalità potrebbe causare del "lag" nel traffico di rete.