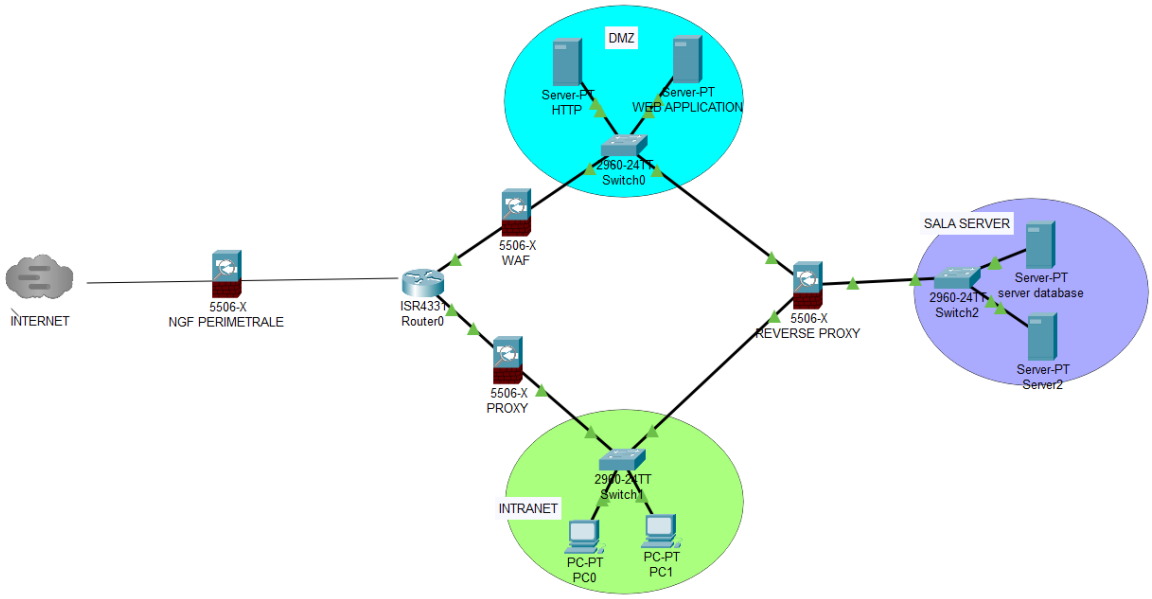


**Difese del sistema**

1. **NGF perimetrale**. Il next-generation firewall perimetrale è la prima linea di difesa del sistema che si interfaccia con internet controllando il traffico in entrata e in uscita.

2. **WAF**. Il web app firewall è specializzato della difesa delle web application andando a difendere i sistemi da attacchi diretti ai servizi web.

3. **PROXY server**. A differenza della DMZ la zona intranet non deve essere facilmente raggiungibile dall'esterno e per questo c'è bisogno di un ulteriore livello di controllo. Il proxy permette di nascondere l'Indirizzo IP, filtrare il traffico in base a determinate regole e fare caching, cioè possono memorizzare localmente le risposte alle richieste effettuate dai client così da consentire al proxy risposte senza dover contattare il server.

4. **REVERS PROXY**. Nella sala server ci sono i dati sensibili dell'azienda (ad esempio il mail server). Se pur ci sono già due livelli di difesa (firewall perimetrale e intranet) un ulteriore firewall è necessario perché un attacco potrebbe essere anche di natura interna. Ad esempio, un personale poco formato potrebbe mettere in pericolo i server scaricando o inserendo inavvertitamente software malevolo. Il revers proxy offre una protezione per i server, poiché gli utenti esterni interagiscono solo con il reverse proxy e non direttamente con i server interni. Inoltre, fornisce quello che viene chiamato bilanciamento del carico, ovvero può distribuire il carico tra diversi server di back-end. Questa funzione può migliorare le prestazioni, la disponibilità e l'affidabilità del sistema distribuendo le richieste tra più server.