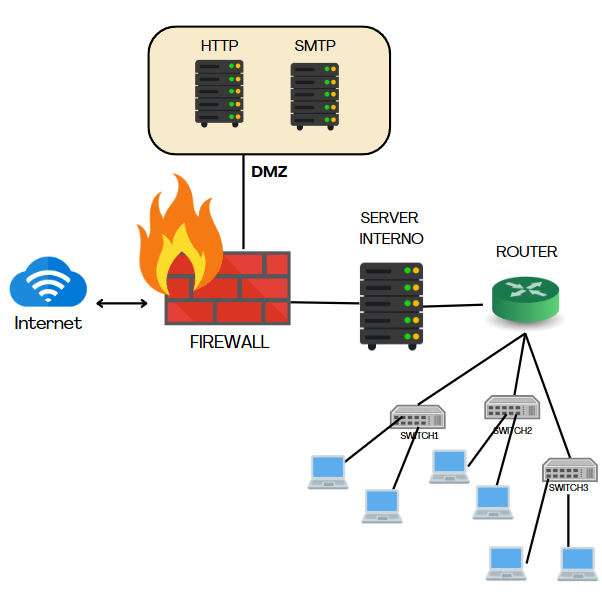
**Prova pratica 22-11-24 Valentina Rubina Tempesta**

**Segmentazione di una rete:**

****

Data una rete come quella rappresentata in immagine possiamo descrivere che:

La rete è collegata ad internet, di conseguenza è esposta a molte minacce e malintenzionati pronti ad approfittare e rubare dati e informazioni sensibili.

Tutto ciò viene ostacolato, se non fermato del tutto grazie alla presenza del Firewall.   
Il **Firewall** è letteralmente un muro che separa il traffico internet in entrata ed uscita, e che analizza il contenuto dei pacchetti per capire se possano essere delle minacce per la rete privata o l’utente finale. In questo caso il Firewall oltre ad essere collegato ad una rete interna è anche connesso ad una DMZ.   
La **DMZ** (Demilitarized Zone) è una zona semi-trusted, isolata ed indipendente che può agire o agisce senza l’utilizzo del Firewall. E’ formato da server che riescono a gestire molto più traffico rispetto al server Firewall, quindi più rapidi ed efficienti. Viene utilizzata come barriera tra la rete interna protetta ed internet, isolata dalle risorse del network interno. La DMZ in una grande azienda, o in ambienti protetti, è molto importante poiché garantisce un ulteriore livello di sicurezza oltre al Firewall. In questo caso la DMZ ha al suo interno due server:

* **HTTP** che gestisce le richieste web esterne
* **SMTP** gestisce il traffico email sia in entrata che uscita.

Per quanto riguarda il network interno esso è composto dal server per la gestione di dati e risorse aziendali, un router e vari switch ai quali sono collegati a loro volta tutti gli host della rete. Questa è la parte più sicura ed isolata da minacce dove dati sensibili vengono scambiati e custoditi. Grazie a tutte le misure di sicurezza apportate da Firewall e DMZ, entrare con intenzioni malevole in una rete interna del genere è abbastanza difficile, anche se si è sempre esposti a molte minacce provenienti specialmente dall’interno dell’azienda.