# Esercizio 22 - 11 - 2024

La rete è stata progettata con lo scopo di garantire la sicurezza, l’affidabilità e la gestione ottimale dei servizi.

La rete è stata suddivisa in due diverse zone.

* **Rete Interna**: Questa sezione della rete è destinata ai dipendenti dell’azienda. Questa zona contiene i pc aziendali e dispositivi critici come il server NAS. I dispositivi di questa rete non sono direttamente accessibili da internet ma posso accedere alla zona DMZ tramite il firewall
* DMZ: Questa è una zona isolata separata dalla rete interna, questa zona ospita il server web (HTTP), il server di posta (SMTP) e un reverse proxy. Questa zona è accessibile dalla rete interna e da internet ma le comunicazioni sono controllate dal firewall. Il proxy è stato inserito per aumentare la sicurezza da potenziali attacchi esterni ai due server.

La separazione tra queste due reti è fondamentale per isolare le utenze dell’azienda da attacchi provenienti da internet. I due server della DMZ sono sì esposti ad internet ma protetti dal firewall perimetrale e dal proxy e inoltre vedono il loro traffico verso la rete interna filtrato dal firewall in questo modo tutti i dati sensibili non vengono esposti.

## Firewall Perimetrale

Il firewall perimetrale è posto tra la rete esterna (Internet) e la DMZ e tra la DMZ e la rete interna.  
Questo firewall si occupa di filtrare il traffico in entrata e in uscita.

* Permette solo il traffico autorizzato verso i server HTTP E SMTP nella DMS.
* Il firewall impedisce attacchi bloccando il traffico sospetto e monitorando il flusso di dati.
* Impedisce la comunicazione diretta tra la rete interna e internet, costringendo il traffico a passare attraverso la DMZ e il server di reverse proxy.

## Reverse Proxy

In questa configurazione c’è un reverse proxy, questo è posizionato nella DMZ con i server HTTP e SMTP. Questo componente ha il ruolo di gestione del traffico in ingresso oltre ad aiutare la sicurezza.

* Gestione del traffico: Il reverse proxy gestisce tutte le richieste web indirizzandole al server appropriato.
* Bilancia il carico: Se i server sono molto richiesti il reverse proxy può bilanciare il traffico tra più server (Nel caso dell’aggiunta di un server)
* Aumento della sicurezza: Nascondendo l’indirizzo IP dei server il reverse proxy dà ancora più protezione non mostrando dove si trovano i server effettivi.