# Relazione Esercizio 02-03-2024

1) Zona Internet: Questa zona (rappresentata da una nuovola) è il punto di ingresso nella rete e rappresenta l'area pubblica e non protetta.

2) Firewall Perimetrale: È posizionato tra la zona di Internet e le altre zone della rete. Controlla il traffico che entra e esce dalla rete filtrando quello indesiderato, impedendo l'accesso non autorizzato e proteggendo la rete interna. Può essere configurato in diversi modi, per esempio per bloccare l'ingresso di pacchetti provenienti da alcuni indirizzi IP, oppure per evitare la scansione non autorizzata delle porte interne.

3) Zona DMZ: Quest'area, tra il firewall perimetrale e il firewall interno, è chiamata zona demilitarizzata (DMZ). È progettata per ospitare servizi accessibili dall'esterno come server web e server di posta elettronica. Questi server sono esposti al traffico esterno, quindi devono essere protetti in modo appropriato. Il server web risponderà alle richieste HTTP provenienti da Internet, mentre il server di posta elettronica gestirà le email in entrata e in uscita.

4) Rete Interna: Quest'area è protetta dal firewall interno e contiene le risorse interne della rete, come server aziendali, NAS (Network Attached Storage), computer degli utenti, e altri dispositivi di rete. Questa zona è considerata più sicura rispetto alla DMZ in quanto non è direttamente esposta a Internet.

Le scelte di progettazione sono state fatte per garantire una sicurezza adeguata alla rete. La posizione del firewall perimetrale tra la zona di Internet e le altre zone della rete limita l'accesso non autorizzato e controlla il traffico in entrata e in uscita. La DMZ offre un luogo sicuro per ospitare i servizi pubblici, come il server web e il server di posta elettronica, mantenendo separati i servizi interni. Infine, la rete interna è protetta dal firewall interno per garantire che le risorse interne siano accessibili solo agli utenti autorizzati all'interno dell'organizzazione.