Spiegazione delle scelte Internet: Rappresentato da un cloud, simbolizza la connessione alla rete globale esterna. Qualsiasi traffico che entra o esce dalla rete aziendale passa attraverso Internet.

Firewall Perimetrale: Posizionato tra Internet, la DMZ, e la rete interna, il firewall serve a proteggere la rete aziendale controllando e filtrando il traffico in entrata e in uscita. Il firewall è configurato per permettere solo il traffico necessario verso le diverse zone.

DMZ (Demilitarized Zone): Questa zona semi-sicura ospita servizi che devono essere accessibili sia da Internet sia dalla rete interna, ma che devono essere isolati dalla rete interna per motivi di sicurezza. Server Web (HTTP): Ospita siti web e altre applicazioni accessibili pubblicamente. Configurato per rispondere alle richieste HTTP da Internet. Server di Posta (SMTP): Gestisce l'invio e la ricezione di e-mail. Configurato per gestire il traffico SMTP da Internet.

Rete Interna: È la zona più sicura della rete, dove risiedono i sistemi e i dati più sensibili. Accessibile solo dai dispositivi e utenti autorizzati.

Server/NAS: Utilizzato per l'archiviazione dei dati e altre funzioni di rete interna. Il NAS (Network Attached Storage) permette una gestione centralizzata dei file e backup.

Configurazione del Firewall

Regole di Accesso: Solo il traffico HTTP e HTTPS (porte 80 e 443) dal cloud Internet è consentito verso il server web nella DMZ. Solo il traffico SMTP (porta 25) dal cloud Internet è consentito verso il server SMTP nella DMZ. Il traffico dalla rete interna verso la DMZ è limitato ai protocolli necessari (ad esempio, per gestione dei server o recupero della posta). Il traffico dalla DMZ verso la rete interna è bloccato per prevenire eventuali compromissioni. Il traffico dalla rete interna verso Internet è permesso solo per le destinazioni e i protocolli necessari (ad esempio, navigazione web, aggiornamenti software).

Motivi delle Scelte

Firewall: Protegge la rete filtrando il traffico non autorizzato, riducendo il rischio di attacchi.

DMZ: Isola i server pubblicamente accessibili dalla rete interna, migliorando la sicurezza. Rete Interna: Mantiene i dati e i sistemi sensibili protetti da accessi non autorizzati.

Selezione dei Server: I server web e di posta sono essenziali per molte operazioni aziendali e devono essere accessibili da Internet, ma con una configurazione sicura per minimizzare i rischi.