Immagine che contiene schermata, diagramma, design

Descrizione generata automaticamenteReport di Configurazione della Rete

Questo report descrive la progettazione di una rete aziendale che soddisfa specifici requisiti di sicurezza e operatività. La struttura comprende una zona internet, una zona DMZ e una rete interna protetta da un firewall perimetrale.

**Zona internet:**

La zona rappresentata dal simbolo del cloud simboleggia la connessione globale a internet.

Serve come punto di ingresso per il traffico esterno e come collegamento per i servizi online accessibili dall’azienda e dai suoi utenti.

**Firewall perimetrale:**

Il firewall perimetrale è un router configurato con regole di sicurezza per filtrare il traffico di rete.

È stato posizionato tra la zona internet, la DMZ e la rete interna per fornire una barriera di sicurezza che protegge la rete interna da attacchi e accessi non autorizzati.

**Zona DMZ:** la DMZ è una sottorete che funge da strato aggiuntivo di sicurezza, isolando i servizi accessibili dall’esterno dalla rete interna dell’organizzazione.

Contiene server web e di posta che necessitano di essere accessibili da internet ma che devono rimanere separati dalla rete interna per ragioni di sicurezza.

**Server Web (HTTPS) e server di Posta (SMTP)**

Sono server situati nella DMZ configurati per gestire rispettivamente il traffico web e di posta elettronica, permettono l’accesso ai servizi aziendali dai clienti e dai partner senza esporre direttamente l’azienda.

**Rete interna**

È la rete all’interno dell’organizzazione che contiene asset critici come i server NAS, questa rete va protetta in quanto contiene dati sensibili e risorse vitali che richiedono il livello massimo di sicurezza.

**Server NAS:**

è un dispositivo di archiviazione connesso alla rete che centralizza la memorizzazione e la condivisione dei file, memorizza dati critici e sensibili, che se compromessi, potrebbero causare danni significativi.

**IDS e IPS:**

L’IDS è un sistema di rilevamento delle intrusioni e L’IPS è un sistema di prevenzione delle intrusioni, il primo monitora il traffico per rilevare potenziali intrusioni senza interrompere l’attività della rete il secondo è attivamente coinvolto nel bloccare attacchi in transito tra la DMZ e la rete interna per prevenire danni.