Relazione sulla rete aziendale

Questa configurazione di rete è progettata con l'obiettivo di garantire sicurezza ed efficienza:

Sicurezza: La rete è segmentata e protetta su più livelli grazie ai firewall e alla DMZ, riducendo il rischio di attacchi e limitando l'accesso alla rete interna.

Efficienza: Gli switch migliorano la gestione del traffico di dati interno, mentre il router gestisce il traffico esterno senza impattare sulle comunicazioni interne.

Descrizione in dettaglio della rete

La rete in questione è segmentata principalmente in due zone:
LAN: Rete interna
DMZ: Demilitarized zone

La LAN è organizzata in modo tale che tutti i PC presenti, essendo collegati ad uno switch possano comunicare tra loro in modo efficiente e sfruttando al meglio la larghezza di banda. Questa LAN è configurata per essere sicura e segmentata, con l'obiettivo di ridurre il rischio di attacchi e mantenere il traffico interno ben gestito.

La zona DMZ ospita due server uno per la comunicazione web e uno per l'invio di mail. Viene isolata dalla rete interna, in modo tale da evitare compromissioni della stessa in caso di attacco ai server (questo è consentito anche grazie ai firewall).La DMZ funge da "zona cuscinetto" che permette di ospitare servizi rivolti al pubblico, mantenendo la rete interna isolata e protetta.

Descrizione dei dispositivi di gestione del traffico

Switch

Per gestire al meglio il traffico all'interno della LAN e sfruttare il più possibile la larghezza di banda è presente uno switch.
È presente un altro switch a gestire il traffico in entrata verso i server presenti nella DMZ.

Firewall

Un firewall è posizionato tra la LAN e la DMZ, isolando la rete interna dai server accessibili dall'esterno. Questo firewall filtra il traffico, consentendo alla LAN di comunicare con i server nella DMZ in modo sicuro.
Il firewall protegge i PC della LAN, bloccando qualsiasi accesso non autorizzato proveniente dai server pubblici nella DMZ o da eventuali connessioni indesiderate che potrebbero compromettere la sicurezza dei dispositivi e dei dati interni.
Questo firewall garantisce che, anche se un server nella DMZ venisse compromesso, gli attaccanti non avrebbero accesso diretto alla rete interna.

La LAN è separata dal resto di Internet tramite un secondo firewall. Il firewall aggiuntivo tra la LAN e Internet garantisce che solo il traffico autorizzato possa entrare o uscire dalla rete locale.
Questo secondo firewall serve anche a regolare il traffico in entrata e in uscita dalla DMZ. Questo firewall permette agli utenti esterni di accedere ai servizi nella DMZ (come il server HTTP o il server di posta) e blocca qualsiasi tentativo di accesso non autorizzato.

Router

Il router connette la LAN e la DMZ a Internet, permettendo ai dispositivi interni di accedere a risorse esterne in modo sicuro e controllato.