

Relazione sul Funzionamento della Rete e la sua Topologia

Introduzione

La rete è stata progettata per connettere in modo sicuro ed efficiente un edificio aziendale con diverse VLAN, fornendo accesso controllato a Internet, comunicazione interna tra VLAN e gestione centralizzata dei dispositivi. La topologia include:

6 VLAN di rete interna (una per ogni piano).

1 VLAN DMZ per il Web Server accessibile dall'esterno.

1 VLAN NAS per la condivisione centralizzata dei file.

1 VLAN di Management per l'accesso SSH e l'amministrazione remota dei dispositivi.

Topologia della Rete

La rete è organizzata in una struttura gerarchica con i seguenti componenti principali:

Switch di Accesso (Layer 2):

Ogni piano dispone di uno switch che collega i dispositivi locali tramite porte configurate in modalità access per la VLAN del piano.

Gli switch sono collegati al router tramite trunk per trasportare il traffico di tutte le VLAN.

Router Aziendale:

Configurato in modalità Router-on-a-Stick per gestire il routing inter-VLAN.

Fornisce accesso a Internet tramite una connessione WAN (seriale) e utilizza NAT per tradurre gli indirizzi privati in un indirizzo pubblico.

Cloud/Router ISP:

Simula la connessione Internet, consentendo ai dispositivi interni di accedere a risorse esterne come server web o DNS.

Server (DMZ e NAS):

Un server nella VLAN DMZ (Web Server) è accessibile sia internamente che dall'esterno.

Un server nella VLAN NAS è accessibile solo dai dispositivi interni per la condivisione dei dati.

Funzionamento della Rete

Separazione delle VLAN:

Ogni piano ha una VLAN dedicata, che isola il traffico per motivi di sicurezza e prestazioni.

Le VLAN sono configurate su tutti gli switch e vengono trasportate al router tramite trunk.

Routing Inter-VLAN:

Il router aziendale gestisce il routing tra le VLAN utilizzando sub-interfacce, ciascuna configurata con un indirizzo IP come gateway per la VLAN corrispondente.

Accesso a Internet:

Tutti i dispositivi interni accedono a Internet tramite NAT configurato sul router aziendale.

Il traffico in uscita viene tradotto utilizzando un singolo indirizzo IP pubblico (PAT).

Accesso alla DMZ e al NAS:

Il server DMZ è accessibile tramite HTTP/HTTPS per fornire servizi pubblici.

Il server NAS è accessibile solo dalle VLAN interne, garantendo la sicurezza dei dati.

Gestione Remota:

La VLAN di Management consente l'accesso SSH ai dispositivi di rete, permettendo agli amministratori di gestire la rete in modo sicuro.

Sicurezza base della Rete (senza firewall IPS/IDS)

Isolamento delle VLAN:

Le VLAN impediscono la comunicazione diretta tra piani senza passare dal router, riducendo il rischio di attacchi interni.

NAT e DMZ:

L'accesso a Internet è controllato tramite NAT, e il server DMZ è isolato per proteggere la rete interna.

Gestione Sicura:

L'accesso SSH è limitato alla VLAN di Management, impedendo l'accesso non autorizzato da altre VLAN.

Conclusione

La rete è progettata per essere scalabile, sicura e performante, soddisfacendo i requisiti aziendali di:

Connettività interna tra i piani.

Accesso controllato a Internet.

Condivisione sicura dei dati tramite il NAS.

Accesso remoto sicuro per l'amministrazione della rete.

Se necessario, la rete può essere facilmente estesa con nuove VLAN