Relazione sulla Rete Implementata

Obiettivo del Progetto

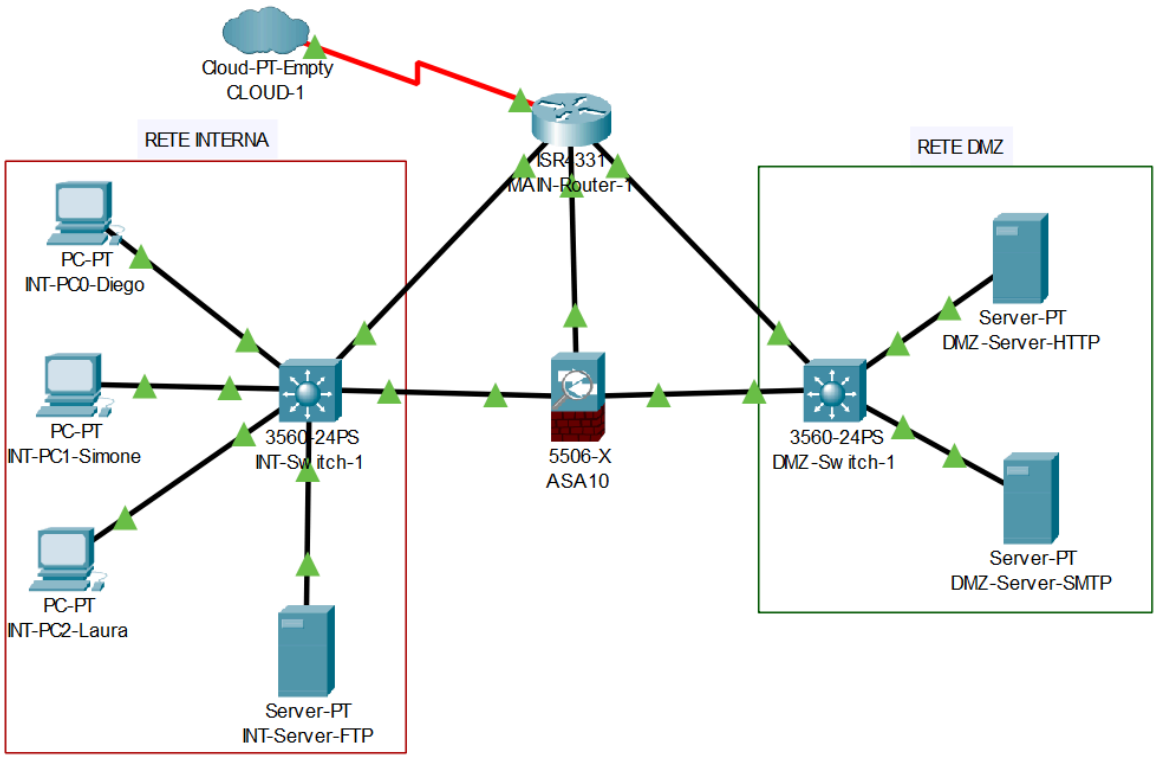
Realizzare una rete segmentata composta da tre zone principali controllate da firewall:

1. **Zona Internet (Outside):** Accesso esterno simulato con una connessione cloud.
2. **Zona DMZ:** Rete intermedia per i server pubblici HTTP e SMTP.
3. **Rete Interna (Inside):** Rete aziendale privata con dispositivi client e un server FTP.

Struttura della Rete Realizzata

Schema generale

1. **Router:** Connessione principale a Internet tramite **cloud**.
2. **Firewall:** Gestisce la separazione e la sicurezza tra le zone (Inside, DMZ e Outside).
3. **Switch DMZ e Interna:** Collegano i dispositivi locali rispettivamente alla rete DMZ e alla rete interna.



Collegamento degli Switch

Spiegazione scelta effettuata

Ho collegato gli switch sia al firewall che al router per i seguenti motivi:

1. **Separazione dei ruoli:**
    - Il **firewall** gestisce la sicurezza e il controllo del traffico tra le zone.
    - Il **router** è utilizzato per il routing tra la rete aziendale (Inside/DMZ) e Internet.
2. **Scalabilità e flessibilità:**
    - Collegando gli switch al router, possiamo aggiungere ulteriori connessioni o segmenti di rete in futuro senza modificare la configurazione del firewall.
    - Questo approccio consente di ridurre il carico sul firewall.
3. **Ridondanza e troubleshooting:**
    - In caso di malfunzionamenti del firewall, possiamo deviare il traffico direttamente al router per mantenere la connettività (anche se con meno sicurezza).
    - Permette di isolare rapidamente le problematiche, separando il livello di sicurezza (firewall) dal livello di connettività (router).

Descrizione delle ACL

Le ACL sono configurate sul firewall per controllare il traffico tra le zone, consentono solo il traffico necessario e bloccano tutto il resto.

ACL Configurate

1. **DMZ verso Internet:**
    - Permette ai server nella DMZ di inviare traffico HTTP (porta 80) e SMTP (porta 25) verso Internet.
    - Blocca tutto il traffico non necessario per garantire che i server non possano accedere a risorse interne o non autorizzate.
2. **interna verso DMZ:**
    - Permette ai dispositivi interni di accedere ai server HTTP e SMTP nella DMZ.
    - Blocca tutto il traffico non autorizzato per garantire che gli host interni possano accedere solo ai servizi pubblici.
3. **interna verso Internet:**
    - Consente agli host interni di navigare su Internet tramite HTTP (porta 80) e HTTPS (porta 443).
    - Blocca tutto il resto per evitare traffico non controllato verso l'esterno.
4. **server FTP nella rete interna:**
    - Consente connessioni FTP (porta 21) al server interno solo dalla rete interna e dalla DMZ.
    - Blocca tutto il traffico non autorizzato al server FTP.

Spiegazione scelta effettuata

1. Così ho limitato il traffico per prevenire attacchi e accessi non autorizzati.
2. Ogni zona della rete ha un accesso ben definito alle altre, riducendo la superficie di attacco.
3. Implementano il principio di **zero trust**, bloccando tutto il traffico non esplicitamente autorizzato.

Conclusione

La rete configurata presenta una segmentazione logica (e penso sicura) grazie al firewall.

Il collegamento degli switch sia al firewall che al router offre:

- **Flessibilità**, consentendo un'espansione futura della rete.
- **Sicurezza**, isolando le zone tramite ACL ben definite.
- **Ridondanza**, permettendo di risolvere eventuali problemi in maniera più rapida.

Le ACL implementate assicurano che il traffico tra le zone sia strettamente controllato, permettendo solo ciò che è strettamente necessario per il funzionamento dei servizi.