**TRACCIA PER IL PROGETTO**

Disegnare una rete con i seguenti componenti:

● Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).

● Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.

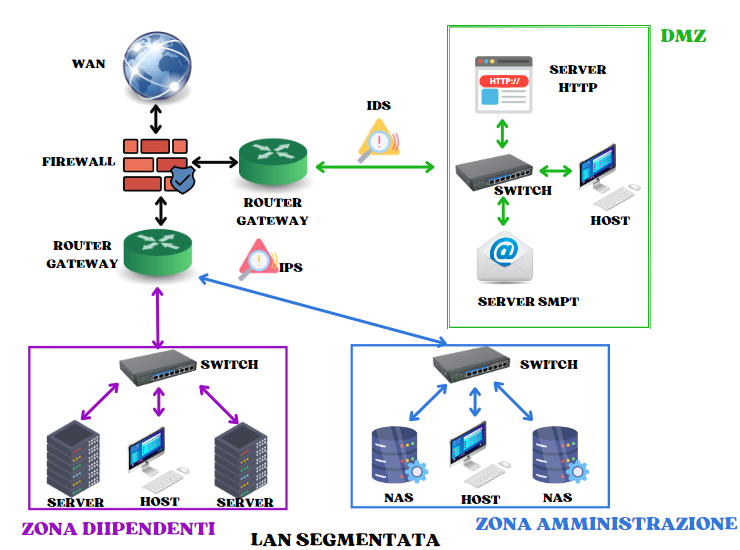
● Una rete interna con almeno un server o nas.

● Un firewall perimetrale posizionato tra le tre zone.

● Un IDS e un IPS

● Spiegare le scelte.

**TOPOLOGIA DELLA RETE**

****

1. **Zona Internet (WAN):** Rappresentata dal simbolo di internet (il globo). Permette agli utenti e ai dispositivi di accedere a contenuti e servizi disponibili su Internet, come siti web, applicazioni cloud, servizi di streaming e, più in generale, la comunicazione tra persone e/o organizzazioni.

2. **Firewall perimetrale:** si trova a cavallo tra la WAN e la LAN. Definisce il confine tra la rete privata e quella pubblica. Lavora a filtraggio dinamico, consulta i propri registri ACL e blocca tutte le connessioni che hanno origine dall’esterno della rete. Potenzialmente, avrei potuto inglobare il lavoro del router gateway all’interno del firewall ma ho scelto di non farlo per ragioni sia di sicurezza sia che di performance: se il firewall/router venisse compromesso o presentasse un malfunzionamento, l'intera rete può diventerebbe inaccessibile, causando interruzioni significative nelle operazioni aziendali; inoltre, il dispositivo andrebbe a sovraccaricarsi, rallentando instradamento e l’analisi dei pacchetti, soprattutto nel caso di grandi aziende.

3. **Router Gateway:** Dopo il firewall, il router gateway gestisce il traffico tra la zona DMZ e il resto dei segmenti di rete, oltre che permettere la comunicazione con la rete pubblica

4. **Rete interna (LAN) segmentata**: ho scelto di suddividere la rete sia per migliorare l’utilizzo delle risorse di rete sia per ragioni di sicurezza, cosicché, nel caso di un attacco, il malintenzionato non possa controllare a pieno la rete. Ogni segmento è gestito dallo switch che, grazie alla tabella MAC, invia i file al destinatario e instrada i pacchetti broadcast a tutta la rete. La rete interna è suddivisa in tre segmenti:

* DMZ: di cui parlo di seguito
* Zona dipendenti: qui sono presenti i server come quello di stampa e file locale per trasmettere i dati non critici tra i vari dipendenti; vi sono anche vari host
* Zona amministrazione: qui sono presenti i server NAS, dove solo gli amministratori di rete possono accedere per gestire facilmente backup, permessi, dati sensibili e la manutenzione

5. **Zona DMZ:** Se tutte le aziende utilizzassero il firewall perimetrale, non sarebbe possibile la comunicazione in quando i movimenti provenienti dall’esterno sarebbero bloccati. Per evitare questo problema è stata implementata la DMZ (zona demilitarizzata). La DMZ indica comunemente una sottorete che si trova tra la rete Internet pubblica e le reti private. Essa espone i servizi all'esterno alle reti non attendibili, offrendo e utilizzando servizi web. Oltre alla comunicazione con il mondo esterno, fornisce un’ulteriore protezione in quanto, essendo una zona isolata, è in grado di mantenere al sicuro i dati sensibili e privati dell’azienda. In questa zona sono presenti:

* Server HTTP: Utilizzato per ospitare applicazioni web e fornire contenuti agli utenti esterni.
* Server SMTP: Utilizzato per la gestione della posta elettronica, consentendo l'invio e la ricezione di e-mail.
* Host

6**. IDS (Intrusion Detenction System) e IPS (Intrusion Prevention System):** Questi sistemi sono integrati nella rete per monitorare il traffico, rilevare attività sospette e, nel caso dell'IPS, intervenire attivamente per prevenire intrusioni. L’IDS si trova nel braccio di rete della DMZ. L’IPS si trova nel braccio di rete del router gateway della zona amministrativa. Ho scelto di posizionarlo qui perché è in grado di bloccare le intrusioni nelle zone di dati sensibili e proteggere i backup

**CONSIDERAZIONI FINALI**

Il progetto di rete descritto offre una soluzione equilibrata tra sicurezza e funzionalità. La configurazione della DMZ, insieme alla gestione sicura della rete interna, rappresenta un approccio efficace per proteggere i dati e i servizi critici dell'organizzazione, garantendo al contempo un accesso facile e sicuro alle risorse esterne.

**-Sicurezza Rafforzata:** La presenza del firewall, insieme ai sistemi IDS e IPS, fornisce un elevato livello di protezione contro le minacce esterne.

**-Accessibilità dei Servizi:** La DMZ consente l'accesso pubblico ai servizi web e di posta elettronica senza compromettere la sicurezza della rete interna.

**-Isolamento delle Risorse:** La segmentazione della rete interna permette di isolare le risorse critiche, riducendo il rischio di compromissione in caso di attacco.