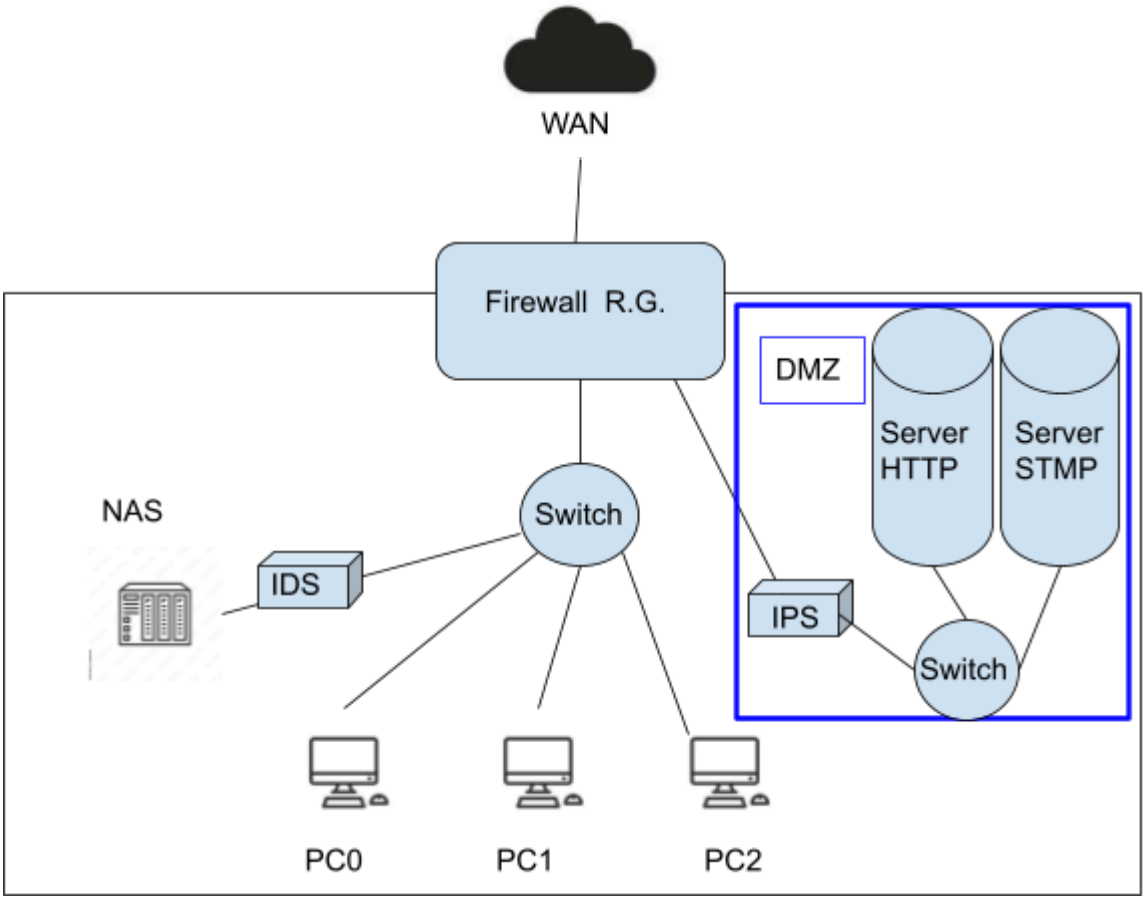
Ghassan Haouem

Traccia per il progetto Esercizio Segmentazione di rete

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.
- Integrare IDS e IPS
- Spiegare le scelte

Mappatura della rete.

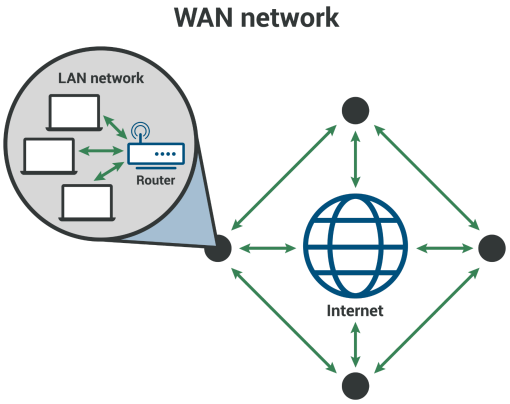


Ghassan Haouem

La rete :

1) WAN (Wide area Network)

Simboleggia il collegamento con il mondo esterno, ovvero l'accesso agli utenti esterni che vogliono raggiungere i servizi ospitati all'interno della rete, come un sito web o un server di posta. È importante separare la rete interna dal mondo esterno (Internet) per motivi di sicurezza, rendendo necessario l'uso di firewall e DMZ per proteggere i dati e i sistemi interni (Host , nas, archivi, utenze).



2) FIREWALL

Il firewall rappresenta una barriera di sicurezza che filtra tutto il traffico in entrata e uscita. Posizionato tra la zona Internet, la DMZ e la rete interna, il firewall gestisce quali connessioni possono passare e quali devono essere bloccate. Generalmente, è configurato per:

- **Permettere** solo il traffico HTTP e SMTP verso i server nella DMZ.
- **Bloccare** qualsiasi tentativo di accesso diretto dalla zona Internet alla rete interna.
- **Reject** blocca il tentativo di accesso (illegittimo)

Firewall Fisico SN-M-Series-720

3) DMZ (Zona Demilitarizzata)

La DMZ agisce come una "zona cuscinetto" tra Internet e la rete interna. Posizionando i server che devono essere accessibili dall'esterno nella DMZ, si limita il rischio di attacchi diretti alla rete interna. Se un server nella DMZ viene compromesso, gli attaccanti non avranno accesso diretto alla rete interna.

Server ospiti della DMZ in questa struttura :

- **Server Web HTTP**: Un server che gestisce le richieste di pagine web (porta 80 per HTTP o 443 per HTTPS).
- **Server di posta elettronica SMTP**: Un server che gestisce il traffico di posta elettronica in entrata e in uscita tramite il protocollo SMTP (porta 25 per il traffico in uscita o 587/465 per traffico sicuro).

4) IPS

L'IPS si trova in linea con il traffico che passa attraverso il firewall, tra la zona Internet e la DMZ. In questo modo, l'IPS può bloccare attivamente attacchi esterni diretti ai server pubblici, come quelli ospitati nella DMZ (server web, server di posta).

Vantaggi: L'IPS rileva e blocca le minacce prima che possano raggiungere i server della DMZ, proteggendo questi sistemi da exploit o attacchi di tipo DDoS (Distributed Denial of Service).

Cisco Secure IPS - Cisco

Svantaggi:

- **Falsi positivi**: Può bloccare traffico legittimo, interrompendo i servizi e creando disservizi.
- **Impatto sulle prestazioni**: L'analisi in tempo reale può causare rallentamenti nelle reti ad alta intensità di traffico creando cosi' il famoso collo di bottiglia.

5) Switch

Lo switch rappresentato nello schema ha il ruolo di distribuire il traffico tra i vari dispositivi all'interno della rete locale, come PC0, PC1, PC2, e il NAS. È responsabile del corretto instradamento del traffico interno , garantendo che i dati arrivino solo ai dispositivi corretti senza conflitti.

6) NAS (Network-Attached Storage)

Un NAS (Network Attached Storage) è un dispositivo di archiviazione di rete ideato per fornire accesso ai dati attraverso una rete (in questo caso il NAS comunica solo ed esclusivamente con la rete interna tramite i nostri host). I NAS sono utilizzati per centralizzare e gestire file, rendendo l'archiviazione e la condivisione di dati più efficienti e veloci.

Nas fisico

7) IDS

L'IDS collegato al NAS ha il compito di monitorare il traffico locale per rilevare eventuali minacce o comportamenti sospetti all'interno della rete. A differenza dell'IPS, l'IDS non blocca direttamente il traffico, ma avvisa l'amministratore se rileva anomalie. Questo è utile perché anche se il firewall blocca gli attacchi dall'esterno, potrebbero esserci minacce che provengono dall'interno della rete (ad esempio, un dispositivo compromesso).

Vantaggi:L'IDS monitora costantemente il traffico di rete e l'attività del sistema, consentendo di rilevare tempestivamente tentativi di intrusione o comportamenti sospetti. Questo permette di adottare misure correttive rapidamente, riducendo il rischio di danni.

Svantaggi: L'IDS come l'IPS può generare un numero elevato di falsi positivi, cioè avvisi su attività legittime che vengono erroneamente identificate come minacce. Questo può portare a una perdita di tempo nel verificare avvisi inutili e a una diminuzione della fiducia nel sistema di sicurezza.

8) HOST

Integrando i PC in una rete con switch e NAS, si ottiene una soluzione efficace per la condivisione di risorse, la collaborazione e la gestione dei dati. È importante configurare correttamente la rete per garantire la massima efficienza e sicurezza, adottando misure come firewall, autenticazione e crittografia quando necessario.