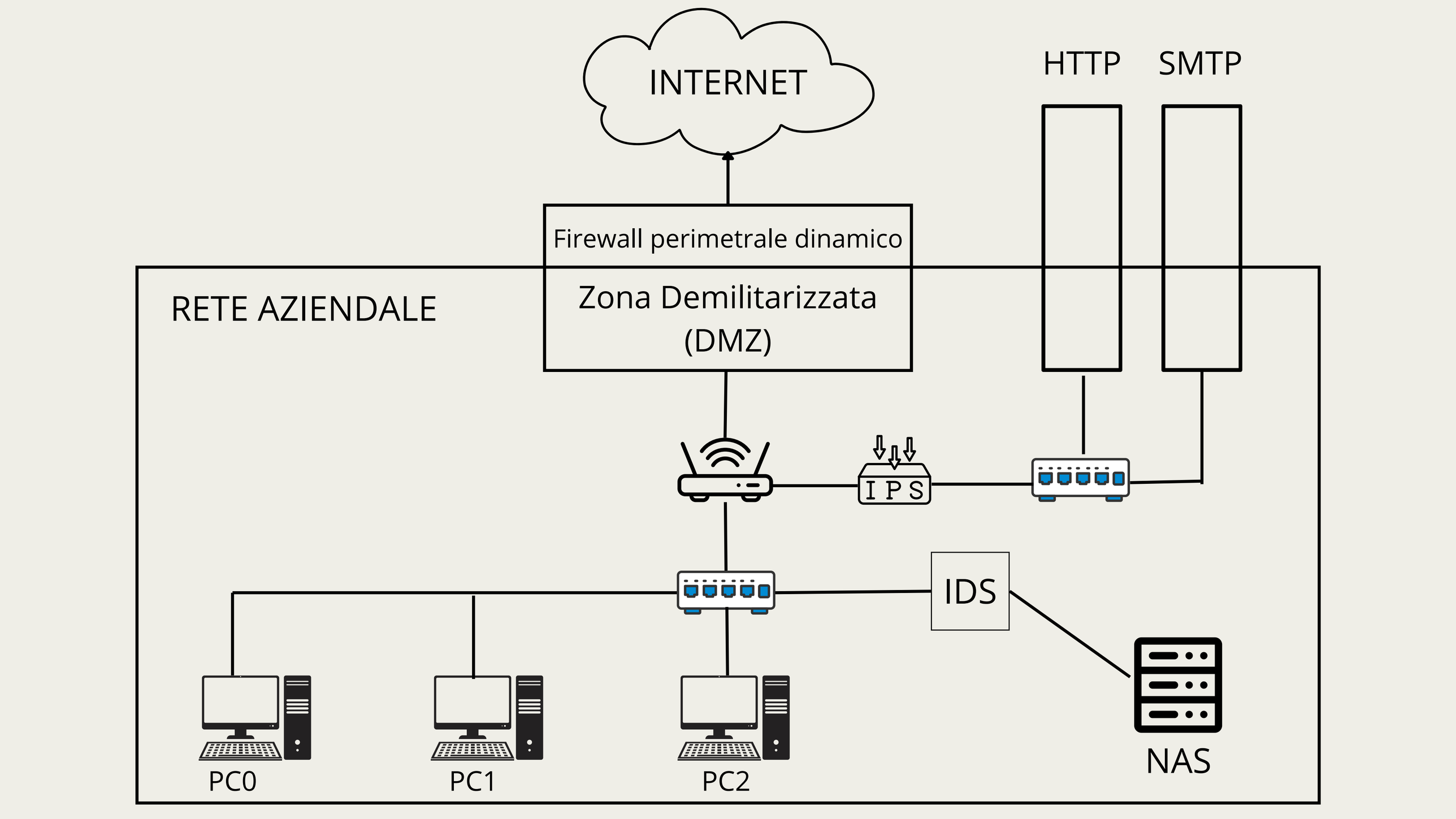
S3-L5

SEGMENTAZIONE DI UNA RETE

T R A C C I A

Disegnare una rete con i seguenti componenti:

- Una zona di internet rappresentata da un cloud.
- Una zona DMZ (Demilitarizzata) con un server web HTTP e un server SMTP di posta
- Una rete interna con almeno un server o NAS
- Un firewall perimetrale posizionato tra le tre zone
- Inserire un sistema di prevenzione IDS/IPS
- Spiegare le scelte


INTERNET
HTTP
SMTP
Firewall perimetrale dinamico
RETE AZIENDALE
Zona Demilitarizzata
(DMZ)
IPS
IDS
PC0
PC1
PC2
NAS

Firewall (cos'è e a cosa serve)

Un firewall è una componente fondamentale della sicurezza informatica, utilizzato per proteggere la rete da minacce esterne e per garantire che il traffico non autorizzato non raggiunga i sistemi interni. Potremmo definirlo come un router più prestante a livello di hardware. Prende il pacchetto, lo spacchetta, lo confronta con una tabella e tutto ciò che essa dice, lo esegue.

Possiamo distinguere due tipi di firewall:

- **Software**: è un programma che viene utilizzato su un computer o un dispositivo. Protegge un singolo dispositivo dove è installato. Facile da configurare ed installare. Ed è spesso utilizzato per proteggere piccole reti domestiche.
- **Hardware**: è un dispositivo fisico posizionato all'interno di una rete. Ha prestazioni elevate in quanto può gestire un'enorme traffico di rete. Ha un costo molto elevato pertanto viene utilizzato a livello aziendale.

Firewall perimetrale Dinamico

Per il progetto ho optato per l’utilizzo di un Firewall Perimetrale Dinamico.
Esso come dice il nome è un “Firewall Perimetrale” ovvero è situato a livello perimetrale tra la WAN e la LAN.
Questo tipo di Firewall Dinamico ha il compito di bloccare tutte le connessioni in ingresso provenienti dall’esterno verso l’interno della rete, permettendo solo l’invio di pacchetti da connessioni autorizzate.
Esso utilizza una tabella ACL (Access Control List) per confrontare gli indirizzi IP dei pacchetti in arrivo con una lista predefinita e, se l’indirizzo non è autorizzato, provvederà a bloccarlo.
Una volta che chiude una connessione tra indirizzo IP privato e indirizzo IP pubblico, il firewall svuota la cache e blocca eventuali pacchetti residui.
Questo Firewall opera fino al livello 4 del modello ISO-OSI, analizzando indirizzi IP e numeri di porta.

Zona Demilitarizzata (DMZ)

Nel mio progetto ho inserito una DMZ che si trova sulla parte destra. Essa è composta da due server web HTTP e SMTP, da uno switch e da un IPS (Intrusion Prevention System) il tutto collegato a un router gateway.

Questa zona delimitarizzata agisce come un cuscinetto tra internet e la rete interna. Se un'attaccante volesse compromettere un server nella DMZ, il firewall impedirebbe ad esso di raggiungere la rete interna minimizzando i danni. Questo garantisce che i dati sensibili restino protetti.

Per ulteriore difesa ho optato per aggiungere un IPS ovvero un sistema di sicurezza che monitora il traffico di rete per rilevare e prevenire minacce o attacchi informatici.

A differenza del Firewall, che si occupa di controllare chi può entrare nella rete, l'IPS analizza il traffico in arrivo in dettaglio, provvede quindi a ricevere il pacchetto, spacchettarlo e a bloccarlo attivamente se sono presenti all'interno potenziali malware. Ovviamente l'azione è preceduta dall'invio di un alert per avvisare di potenziali pericoli.

Protezione del NAS

Infine ho provveduto a dare protezione aggiuntiva al NAS inserendo un IDS (Intrusion Detection System) all'interno della mia rete aziendale.
Il NAS è uno dei dispositivi più importanti in ambito aziendale in quanto vengono utilizzati per archiviare dati anche sensibili pertanto vanno protetti da eventuali minacce a tutti i costi.
Aggiungendo un IDS al NAS ho garantito migliore protezione per il traffico interno di dati. Nel caso riuscisse ad entrare un'attaccante nella rete, l'IDS fornirebbe immediatamente un'alert subito dopo aver analizzato il pacchetto e quindi permetterebbe di agire subito sul problema cercando di mitigare il danno.

Grazie

MATTIA DI DONATO