COMPITO 18/10/2024 PAOLO TAVIAN

EPICODE

Esercizio
Segmentazione di rete

Traccia per il progetto

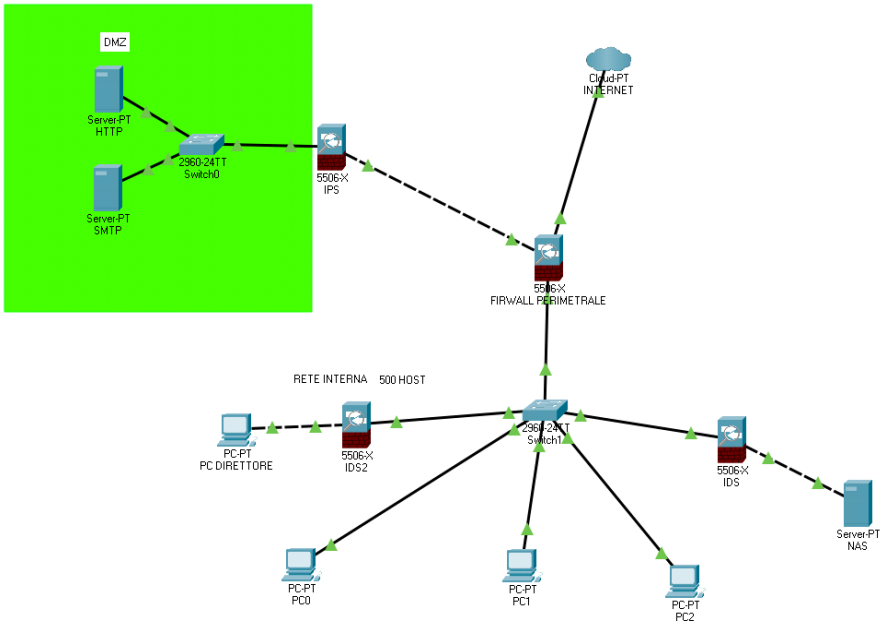
Disegnare una rete con i seguenti componenti:

- 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.
- Spiegare le scelte.

3

COSTRUZIONE DELLA RETE

Disegno tecnico



Componenti utilizzati:

Nuvola: rappresenta l'nternet

Firewall : dispositivo che, in questo caso sarà utilizzato come router,

Una zona demilitarizzata DMZ: E' una zona all'esterno della rete interna in cui permette la comunicazione con tutti sia dall'esterno che dall'interno.

Viene utilizzata per evitare che le persone esterne possano attacare la rete interna poichè la zona è collegata a firewall che filtrano il traffico

Nas: un server contente informazioni vitali per la azienda

IPS:Avvisa se ci sono minacce nei pacchetti ricevuti Manderà un alert al personale

IDS: Oltre a mandare un alert al personale l'IPS controlla le regole e se non vengono rispettate blocca il pacchetto

2 server HTTP e SMTP: server che permettono la comunicazione esterno,

essendo nella DMZ tutti si possono connettere

Perchè utilizziamo il FIREWALL?

Si utilizza il firewall per proteggere la nostra rete da venteuali minacce provenienti dall'esterno.

La maggior parte degli attacchi proviene da fuori.

Per proteggere la nostra rete:

1.Firewall a filtraggio dinamico (di stato): blocca tutte le connessione che hanno origine dall'esterno verso l'interno al contrario consente dall'interno verso l'esterno

2.IPS: software che avvisa se ci sono minacce nei pacchetti ricevuti Manderà un alert al personale

3.IDS: software che, Oltre a mandare un alert al personale, l'IPS controlla le regole e se non vengono rispettate blocca il pacchetto

Adesso facciamo un esempio:

Il firewall ha una tabella contenente delle regole, programmate da noi, che va a controllare quando un pacchetto entra nel firewall.

A seconda del contenuto del pacchetto (IP per il firewall dinamico , messaggio contenuto nel pacchetto per IPS e IDS) si va a compiere un'azione: Block, pass e reject

Block: blocca il pacchetto senza dire il perchè al mittente

pass: fa passare il pacchetto

reject:blocca il pacchetto e va a dire il perchè al mittente

IPS è posizionato tra la zona demilitarizzata ed il firewall perchè va a controllare i pacchetti in entrata (il contenuto) dalla DMZ e guarda le sue regole (tabella ACL), a seconda della regola (vedi sopra)

Il firewall è posizionato tra l'internet e la rete interna:

Il firewall può essere configurato anche come un router (è anche più performante)

Esso, come IPS, va a controllare i pacchetti (solo IP) in entrata e va a controllare nella sua tabella se il messaggio può passare o meno

IDS: è posizionato nella rete interna ed va ad analizzare il pacchetto (contenuto) ; se è malevolo va a segnalare al supervisore che il pacchetto è infetto.

Di IDS ce ne sono molti poichè hanno la funzione di avvisare l'autorità competente

Di IPS ce ne saranno meno perchè posso bloccare anche i pacchetti non pericolosi ostacolando la produttività della azienda.

Esempio:

Per proteggere il NAS (server con informazioni importanti per l'azienda)

aggiungerò un IDS tra lo switch e il nas perchè cosi analizzo i pacchetti e se sono infetti le autorità possono intervenie tempestivamente

Mettendoci un IPS potrebbe bloccare un dipendente che cerca di comunicare con il NAS.