S3E5

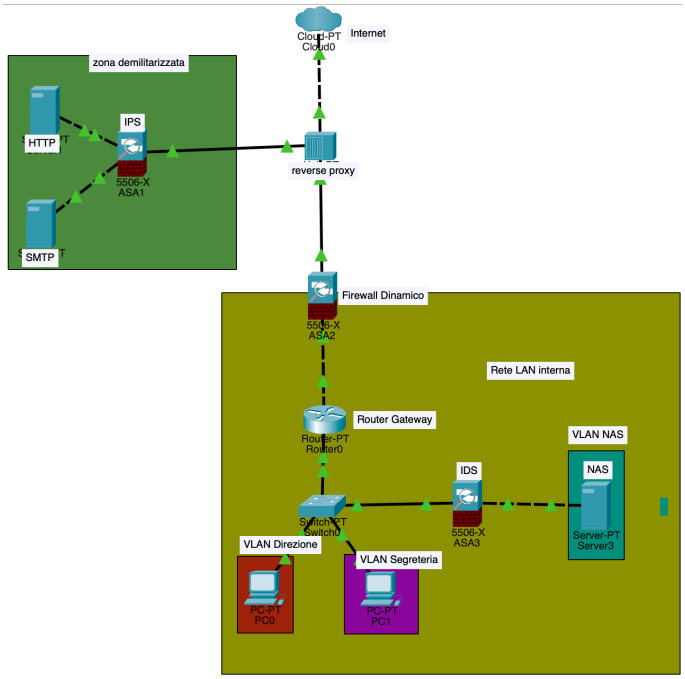
Segmentazione di una rete

L'esercizio di oggi consiste nel creare una rete il più segmentata e sicura possibile, utilizzando tutti gli strumenti imparati finora.
La rete deve contenere dei componenti precisi che sono:

- Una zona di internet
- Una zona demilitarizzata (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 zone
- Almeno un IDS e un IPS

Progettazione della rete

Nella figura sotto ci sarà una rappresentazione grafica della rete, in questo caso andrò a fare alcuni esempi di come questa rete funzioni e spiegherò man mano perché quel componente è stato messo in quel punto e qual è la sue funzione.



Come si può notare dal punto di vista grafico ho diviso le varie zone in più colori, la prima zona che andrò a spiegare sarà la zona gialla ovvero la rete LAN.

Rete Lan

In questo caso la rete LAN è composta di vari dispositivi, tra cui due PC, un NAS (ovvero un dispositivo di archiviazione che permette di avere i dati sempre disponibili tra i dipendenti), un IDS (Intrusion Detection System), uno Switch, un Router gateway e un Firewall Perimetrale (in questo caso è stato scelto un firewall dinamico).
Per cercare di far capire meglio come funziona una rete è meglio andare a spiegare alcuni componenti in maniera più specifica.

Che cos'è un Firewall Perimetrale?

Un Firewall Perimetrale è un dispositivo che si va a posizionare tra la rete LAN e la rete WAN, questo firewall andrà a spacchettare e analizzare tutti i pacchetti in uscita ed in entrata, ed in base a delle regole pre-impostate andrà a compiere delle azioni. Il modello di firewall da me scelto è un modello di Firewall a filtraggio dinamico. Il firewall dinamico blocca tutte le connessioni che partono dall'esterno della rete e puntano ad arrivare all'interno. Una comunicazione può arrivare dall'esterno della rete solo se prima un dispositivo dall'interno ha avviato una sessione con il dispositivo esterno. Ho preso la scelta di posizionare quel Firewall in quella posizione per cercare di avere la mia LAN il più blindata possibile dall'esterno.

Che cos'è un IDS? Un IDS è un software che spacchetta il messaggio e lo esamina, ha anche lui una tabella di regole da seguire, se il messaggio fa attivare una di queste regole allora manderà un alert e l'operatore che visionerà il messaggio potrà scegliere se far passare il messaggio o bloccarlo. Ho deciso di metterlo a protezione del NAS, perché essendo la parte più delicata della rete ho bisogno che resti il più integra possibile e ho deciso di utilizzare il software IDS per non rischiare che vengano bloccate anche richieste legittime.
Nella LAN come ulteriore forma di difesa ho utilizzato anche le VLAN. Una VLAN è una tecnica informatica, e tramite lo switch, mi permette di segmentare ulteriormente la rete, in questo caso ho segmentato ogni singolo host con la propria VLAN così che se l'attaccante riuscisse a raggiungere il PC1 (ovvero il pc segreteria) non potrà raggiungere facilmente né il PC0 (pc direttore) né il NAS.

Ora passiamo all'esterno della rete LAN dove troviamo reverse proxy e zona demilitarizzata.
Che cos'è un reverse proxy? Il proxy è un server che si mette tra due indirizzi IP, questi indirizzi possono essere sia pubblici che privati. Normalmente si utilizza per andare a camuffare gli indirizzi IP. In questo caso ho utilizzato un reverse proxy appena prima di entrare nella rete WAN. Questo proxy andrà a nascondere gli indirizzi IP pubblici dei miei server. Inoltre al proxy posso aggiungere una serie di protocolli. In particolare questo proxy farà da router gateway per la zona demilitarizzata e farà da filtro WAF (Web Application Firewall). **Che cos'è il filtro WAF?** Il filtro WAF è un firewall che protegge a tutti e sette i livelli del modello ISO/OSI. In questo caso il WAF andrà a spacchettare il pacchetto e andrà a visionare il codice del pacchetto. Se all'interno del pacchetto troverà codice malevolo allora significa che dovrà rigettare i dati, altrimenti farà passare la richiesta ai server. Il Filtro WAF è perfetto per proteggere e-commerce e servizi mail, per questo lo scelto come protezione della zona demilitarizzata.
Che cos'è la zona demilitarizzata? La zona demilitarizzata (DMZ) è una zona appena fuori al mio firewall perimetrale. In questa zona ho posizionato i server HTTP e SMTP perché ho bisogno che questi server riescano a comunicare con richieste dall'esterno (cosa che non potrebbero fare stando nella rete LAN). A protezione della zona ho piazzato un altro software chiamato **IPS (Intrusion Prevention System).**
Questo software funziona come il già citato IDS con la differenza che quando andrà a spacchettare il messaggio se ci troverà qualcosa di malevolo andrà direttamente a bloccare il pacchetto in automatico. Ho scelto di andare ad utilizzare il software IPS perché in questo caso se anche una richiesta fosse legittima ma bloccata per un falso negativo non recherò gravi danni all'azienda, basterà fare semplicemente un'altra richiesta.

Conclusioni

Segmentando la rete in questo modo se dall'esterno arriverà una richiesta HTTP o SMTP, il codice verrà esaminato più volte e poi passato ai server che comunicheranno con l'esterno. Avendo un'accessibilità più alta i server sono più a rischio di attacchi. Invece la mia rete interna avendo un Firewall dinamico avrà un'accessibilità dall'esterno notevolmente più bassa, inoltre l'attaccante troverà una rete segmentata dalle VLAN quindi non si potrà neanche muovere facilmente. Un pericolo per la rete LAN potrebbe essere il generare connessioni malevoli dall'interno verso l'esterno, in quel caso si creerebbe un canale di comunicazione che potrebbe far passare tutti i malware. Il consiglio è di andare su siti certificati e sicuri per cercare di ridurre al minimo la possibilità che dei malware possano entrare nella rete.