Yuliya Suvorova, 22/11/2024

Cyber Security & Ethical Hacking

ESERCIZIO: SEGMENTAZIONE DI RETE

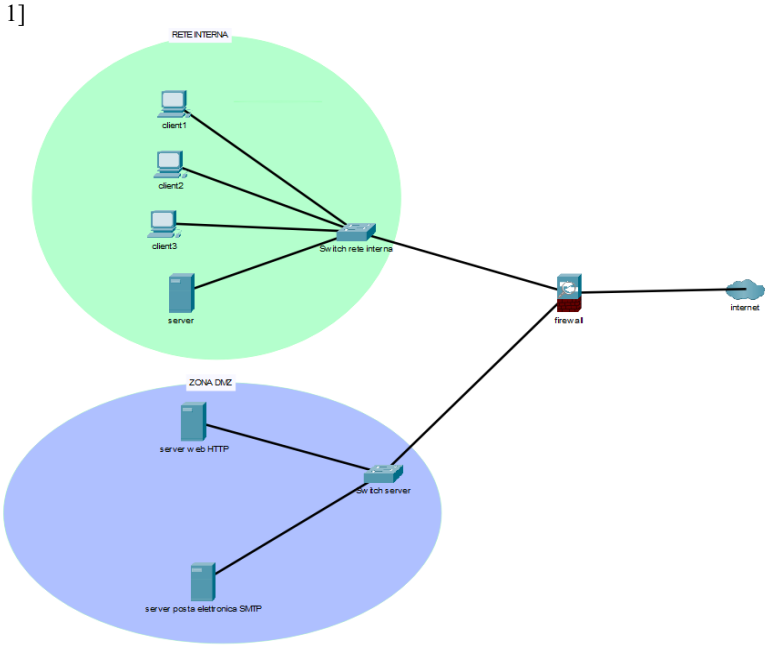
Traccia per il progetto

Disegnare una rete con i seguenti componenti:

1. Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).
2. Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.
3. Una rete interna con almeno un server o nas.
4. Un firewall perimetrale posizionato tra le tre zone.
5. Spiegare le scelte.

La traccia, quindi, richiedeva di rappresentare una rete segmentata (figura 1).

[figura 1]



Prima di spiegare le scelte fatte nello schema di rete, bisogna specificare cosa significhi e a cosa serva la segmentazione di una rete.

La segmentazione della rete è una tecnica utilizzata per dividere la rete in zone (principio di "zoning") in cui ogni area è dedicata ad una funzione diversa, con un diverso livello di sicurezza/protezione. Lo scopo è quello di aumentare la sicurezza della rete.

Per quanto riguarda la spiegazione, nello schema si possono individuare i componenti principali:

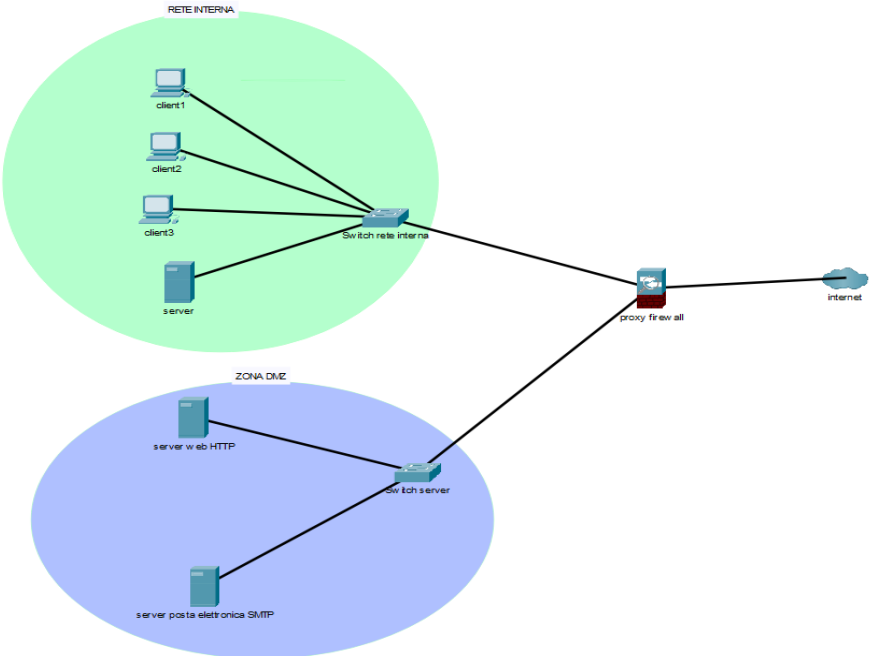
- Una rete interna, cioè una zona dedicata alla rete interna che ospita i computer e un server.
- Una zona demilitarizzata, una DMZ, che ospita i server web e i server di posta elettronica e quindi deve essere protetta efficacemente. I server devono essere configurati per consentire solo il traffico specifico sulle porte HTTP(80) e SMTP(25).
- Un firewall perimetrale, che ha la funzione di filtrare il traffico di rete in entrata ed in uscita. In questo caso ha tre interfacce di rete: per la connessione internet, per la intranet e per la DMZ. Permette il traffico solo verso i server bloccando il traffico non autorizzato. Il suo funzionamento nelle architetture di rete è determinato da regole configurate di sicurezza e filtraggio. Ispeziona i pacchetti, ne monitora lo stato e ne analizza il contenuto, basando la sua funzione decisionale sul confronto dei dati nei pacchetti con le informazioni contenute nella tabella di stato delle connessioni attive per verificare che appartengano a connessioni esistenti. Monitora il traffico in tempo reale, generando non solo notifiche per avvisi di sicurezza ma anche report sulle proprie attività.
- Una zona internet che invece rappresenta la rete esterna alla quale si accede con internet.

In questo scenario il firewall filtrerà tutti i pacchetti provenienti da internet e permetterà il passaggio solo a quelli autorizzati, rafforzando così la sicurezza dell'intera rete. Protegge sia la intranet che la DMZ e ne gestisce il traffico, limitandolo, per esempio, solo all'invio o la ricezione di e-mail dal server SMTP nella DMZ.
Infatti, la intranet e la DMZ non possono essere direttamente collegate per una questione di controllo e sicurezza, in quanto il firewall monitora i log, riuscendo così a rilevare tempestivamente eventuali minacce, cosa che potrebbe non avvenire se le due aree fossero direttamente collegate.
Ovviamente per quanto riguarda la rete interna, oltre al firewall, bisogna avere anche un certo di grado di attenzione perché ci sono minacce che sono in grado di aggirare la protezione offerta dal firewall attaccando altri punti di accesso alla rete come scanner o stampanti.

CONSIDERAZIONI

Inoltre, nel firewall potrebbe essere integrato un sistema IDS (intrusion detective system) o un sistema IPS (intrusion prevention system) per aumentare il livello di sicurezza, in quanto, da definizione, IDS funziona analizzando il traffico di rete o i log di sistema alla ricerca di firme o modelli noti di attacchi informatici, comportamenti anomali o violazioni nelle policy di sicurezza, generando avvisi in caso di rilevamento minacce, senza però intervenire attivamente per fermarle; mentre IPS ha le stesse funzioni, con la differenza che è in grado di intervenire per fermare eventuali attacchi.

Un'altra implementazione potrebbe essere quella di un proxy firewall interposto tra internet e le aree della rete, cioè di un dispositivo intermediario che analizza il traffico di pacchetti a livello applicativo, rilevando eventuali contenuti dannosi nascosti (figura 2). Può nascondere gli indirizzi IP ed eseguire una cache dei contenuti, riducendo così il carico sulla connessione internet; permette, inoltre, l'accesso remoto alle risorse interne di una rete senza compromettere la sicurezza della stessa.
[figura 2]



Un dispositivo alternativo a quello sopra citato potrebbe essere il proxy-reverse collegato ai server nella DMZ. Questa implementazione fornirebbe un controllo più avanzato del traffico e una sicurezza aggiuntiva tra i server nella DMZ e internet, insieme al firewall. Infatti, il proxy reverse, in questo scenario, gestirebbe e filtrerebbe ulteriormente le richieste pervenute dal firewall, bilanciando il carico dei server e proteggendo la visualizzazione dei loro indirizzi IP.