PROGETTO S3-L5

Disegnare una rete con i seguenti componenti:

● Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).

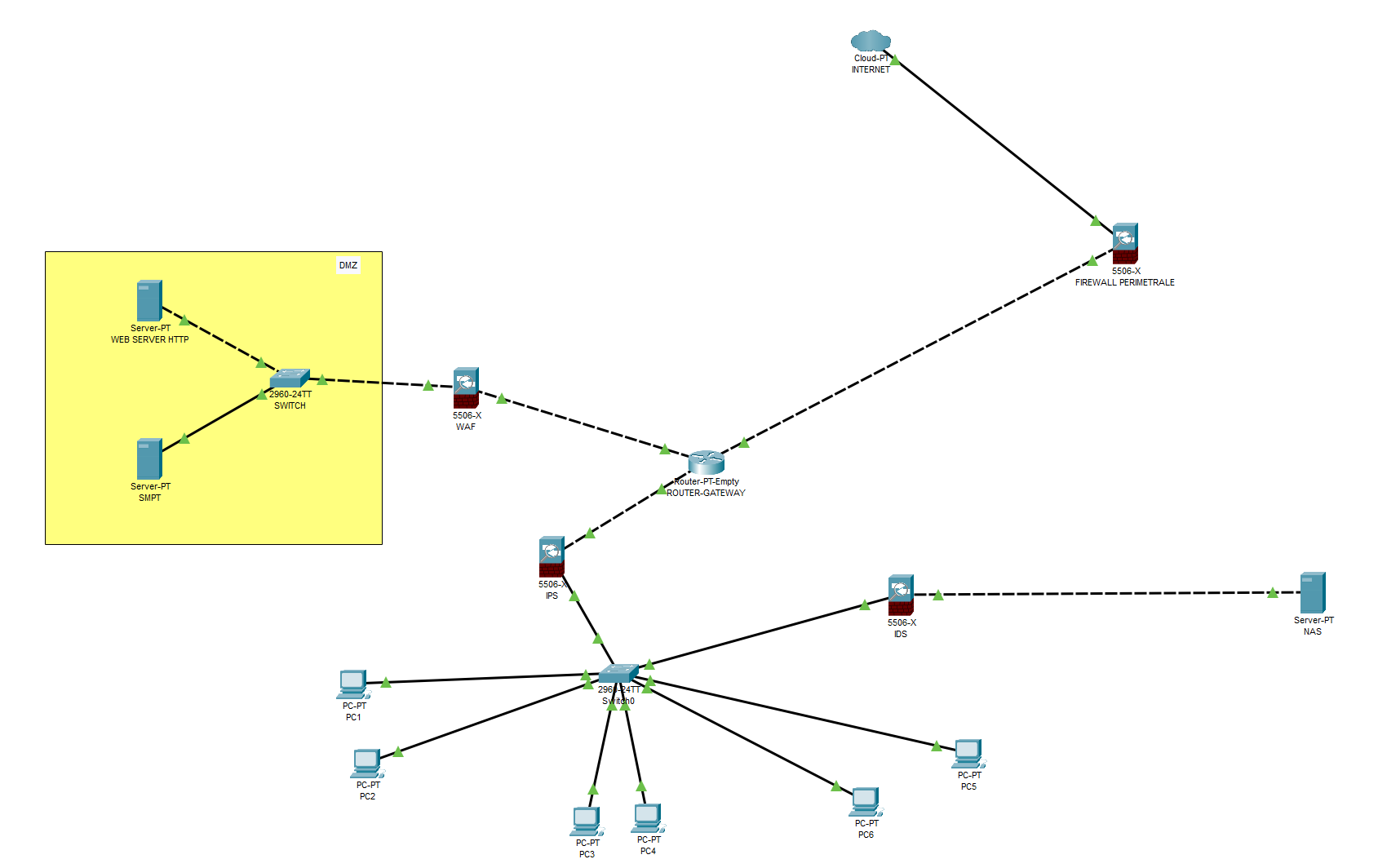
● Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.

● Una rete interna con almeno un server o nas.

● Un firewall perimetrale posizionato tra le tre zone.

● Spiegare le scelte.

Svolgimento



Componenti utilizzati nella rete creata:  
Internet  
Firewall Perimetrale  
Router-Gateway  
WAF  
SWITCH

WEB SERVER HTTP

Server posta elettronica SMTP

IPS e IDS  
NAS  
Client

In questo progetto andremo a descrivere il perché questa rete è stata creata in questo modo:

In questa ipotetica rete sono presenti vari componenti che hanno bisogno di essere protetti. Il primo passo, dopo aver creato la rete, e aver controllato la funzionalità, sarà creare un Firewall. Ma cos’è nello specifico?   
  
Per Firewall si intende un dispositivo di sicurezza che monitora i movimenti in entrata e in uscita tra reti. Esistono due tipi di firewall:  
il perimetrale e il non perimetrale.  
Il firewall perimetrale viene montato a cavallo tra la rete WAN e la rete LAN, il non perimetrale può esistere soltanto all’interno di una delle due.   
Il Firewall non perimetrale si suddivide ulteriormente in altri due tipi:  
Il Firewall host, che viene installato sui PC e il Firewall Network che viene montato nella bretella di rete. Due dei Firewall più comunemente usati sono il Watchguard e il PFSense.

Questi Firewall possono essere implementati in due modi. In modalità hardware o software, in base al numero di connessioni presenti nella rete.  
A livello di sicurezza, tra i due, non c’è alcuna differenza. La sostanziale differenza sta nelle prestazioni. Il costo di un Firewall hardware, infatti, può raggiungere cifre astronomiche (500.000€ ad esempio) a causa delle specifiche tecniche di altissimo profilo (1TB RAM, 24 processori, 4 schede madre). Il Firewall software verrà invece limitato dalla componentistica del PC sul quale verrà montato.

In questo caso andremo ad utilizzare un Firewall perimetrale hardware.

Adesso c’è da decidere il tipo di filtraggio da utilizzare:

Il filtraggio dinamico è il più utilizzato a livello perimetrale, bloccando automaticamente l’accesso a tutte le connessioni che provengono dall’esterno e permettendo, invece, l’uscita di tutte le connessioni che partono dall’interno.

In questo modo il nostro firewall, grazie alla ACL (Lista di controllo accessi) ci proteggerà da qualsiasi tentativo di connessione esterna da parte di un indirizzo IP Pubblico e permetterà ai nostri host di poter raggiungere la rete internet. Grazie a questa lista, il Firewall registrerà l’indirizzo IP Pubblico del server che stiamo cercando di raggiungere, creando dunque una connessione sicura e permettendo al suddetto di server di inviarci pacchetti. Una volta che la connessione verrà interrotta, la lista verrà ripulita dato che fa affidamento ad una memoria volatile (memoria cache in questo caso).

Tutto sembra perfetto, ma pensandoci attentamente sorge un problema. Se il filtraggio dinamico blocca qualsiasi indirizzo IP pubblico, come faremo a contattare con terzi dato che anche noi verremo identificati come rete esterna?  
  
Ecco che viene creata la DMZ (Zona Demilitarizzata). In questa zona, tutte le connessioni, sia in entrata che in uscita, hanno il permesso di accedere, permettendo dunque le comunicazioni. Principalmente nelle aziende la DMZ viene utilizzata per permettere ai server web HTTP e ai server web di posta elettronica di comunicare con la rete internet, ma qui nasce un ulteriore problema. Come blocchiamo il contenuto malevolo adesso che abbiamo libero accesso ad Internet?

Lo faremo tramite il filtraggio a livello di contenuto. Tramite questo filtraggio utilizzeremo il WAF (Web Application Firewall) che andrà a spacchettare i pacchetti ricevuti cercando contenuto malevolo da bloccare. Per farlo, il WAF farà riferimento alla sua ACL che potrà essere di due tipi:   
Tabella Interna, dove tutti i dati dovranno essere inseriti manualmente, oppure Tabella Esterna, dove l’ACL si collegherà ad un dizionario malware esterno (il più famoso è OWASP).

Fatto ciò, potremmo dire di aver finito, ma dato che non si è mai troppo al sicuro, andremo ad implementare un altro sistema di sicurezza.  
  
L’IDS/IPS:

Questo software si divide in due modalità. Modalità passiva (IDS) e modalità attiva (IPS). L’IDS riceve i pacchetti, li spacchetta per il controllo e avvisa nel caso in cui ci fosse del contenuto malevolo.  
L’IPS fa la stessa cosa, ma in più blocca la minaccia.

In questo esempio di rete, l’IDS verrà posizionato a difesa del NAS e l’IPS verrà montato a difesa dei web server posizionati in DMZ.  
Qual è la motivazione dietro questa scelta?  
  
L’IPS può soffrire di falsi positivi/negativi, questo potrebbe causare problematiche d’accesso ad un host che andrebbe ad accedere al NAS, se montato a sua difesa, bloccandogli l’entrata. Per evitare questo “problema”, l’IDS è lo strumento migliore da utilizzare, lasciando in questo modo la decisione finale al giudizio umano.

Dunque, l’IPS va utilizzato per controllare principalmente il flusso di pacchetti proveniente dall’esterno, ecco perché viene a messo vicino alla nostra DMZ, in questo caso.

In conclusione, qualsiasi azienda dovrebbe salvaguardare i propri interessi difendendo al meglio la propria rete. Il modo migliore per farlo sarà sicuramente investendo sul backup dei proprio dati e su un firewall grande abbastanza da proteggere la propria rete.