ESERCIZIO S3-L3

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.

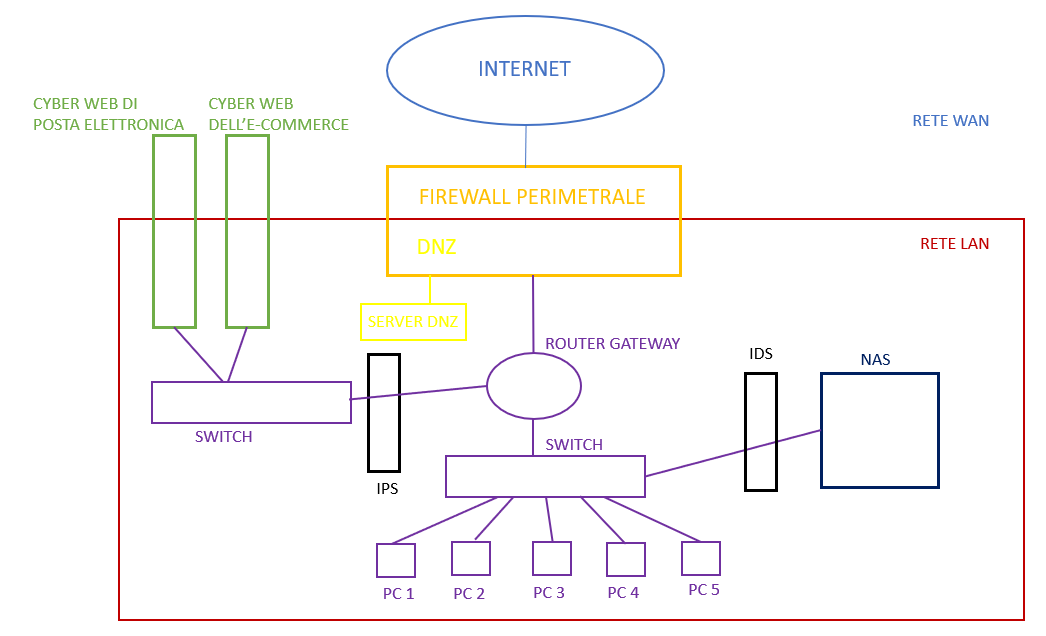
● Una rete interna con almeno un server o nas.

● Un firewall perimetrale posizionato tra le tre zone.

● Sistema IDS/IPS.

● Spiegare le scelte.

PER PRIMA COSA DI SEGUITO DISEGNAMO UNO SCHEMA DELLA RETE CON I COMPONENTI RICHIESTI:



FIREWALL PERIMETRALE

Iniziamo col parlare e definire cosa è un FIREWALL:

E’ un dispositivo di sicurezza informatica progettato per controllare il traffico di rete in entrata ed in uscita, in base ad un insieme di regole di sicurezza predefinite. La sua funzione principale è quella di proteggere la rete o un sistema da accessi non autorizzati e da potenziali minacce ( come malware, attacchi informatici, intrusioni ).

TIPI DI FIREWALL:

1. PERIMETRALE .

Si trova nel perimetro ( cavallo) tra la rete lan e wan.

1. NON PERIMETRALE.

Non sta tra la wan e la lan ma generalmente si trova nella lan e ce ne sono di 2 tipi:

* FIREWALL DI HOST: protegge l’host (esempio un pc )
* FIREWALL DI RETE: si trovano in un braccio di rete ( esempio vicino uno switch) e protegge più host associati alla rete dello switch.

Ci possono essere inoltre 2 tipo di firewall:

1. FIREWALL HARDWERE

È un dispositivo fisico di firewall con dentro già l’iso, il suo costo può variare tra i 3k euro e può arrivare a costare anche milioni. Il suo prezzo dipende dalle prestazioni dal dispositivo; in base a quante più connessioni dovrà sostenere e più dovrà avere componenti interni costosi in grado di sostenerli.

1. FIREWARE SOFTWERE

È un iso del firewall che posso scaricare direttamente sul mio pc

QUANDO INSTALLARE IL FIREWARE SOFTWERE E QUANDO QUELLO HARDWERE?

Dipende esclusivamente dal numero di connessioni.

Facciamo un esempio in base al numero di persone ( ma nella maniera standard dovremmo andare a vedere il numero di connessioni no delle persone )

* Azienda con meno di 30 persone – va bene un firewall softwere
* Azienda superiore a 30 persone – bisogna comprare un firewall hardwere: fino a 100 persone va bene un dispositivo da 4/5k euro. Sopra le 100 persone bisogna spendere molto di più.

TIPI DI FILTRAGGIO

* STATICO
* DINAMICO
* PER CONTENUTO
* PROXY

FILTRAGGIO STATICO

Usato fino agli anni 90, quando non c’era ancora molti dispositivi in circolazione.

E’ una tecnica di sicurezza che analizza i pacchetti di dati che attraversano la rete e decide di bloccarli o consentirgli il passaggio in base a regole predefinite.

Per configurarlo bisogna prima di accendere il firewall entrare nell’ACL (access control list ) e si vanno a scrivere gli indirizzi ip che si vogliono far passare da quelli che vogliamo bloccare.

Quando qualcuno passera per il firewall, questo cercherà una corrispondenza dall’alto verso il basso tra gli indirizzi nella lista e quando lo troverà vedrà se farlo passare o bloccarlo.

E’ importante scrivere bene perché alla prima corrispondenza non continuerà a scorrere, quindi se dopo abbiamo rimesso lo stesso indirizzo ip ma cambiato ( esempio da permit a block) non lo vedrà e fara affidamento solo alla prima corrispondenza.

Col passare del tempo e del crescente numero di indirizzi ip non era più fattibilie scrivere tutti gli indirizzi manualmente. Quindi si passò al filtraggio dinamico.

FILTRAGGIO DINAMICO

Blocca tutte le connessioni che hanno origine dall’esterno della rete ( dalla wan ) verso l’interno.

Consente invece la connessione dall’interno verso l’esterno.

COME FA A CAPIRE DA DOVE PARTE IL SEGNALE?

Dipenderà dal tipo di ip utilizzato, se arriverà con un indirizzo pubblico vorrà dire che viene dall’esterno e lo bloccherà, se arriva con indirizzo privato lo farà entarre.

Anche questo filtraggio avrà una tabella ma questa volta sarà una memoria volatile, vuol dire che una volta che io inizierò la comunicazione da dentro a fuori, andrà in memoria l’ip esterno, cosi che per la successiva comunicazione il filtraggio farà passare l’ip esterno perché noi per primi ci siamo connessi con lui o lo riconoscerà.

Ogni volta che chiuderemo la sessione questa memoria si cancella cosi da non riceve più dall’esterno.

Quale è il problema di questo filtraggio? Se tutti avessimo questo sistema non ci potrebbe essere comunicazione tra nessuno perché saremo sempre bloccati secondo il principio visto prima.

Qui di è stata creata per ovviare a questo una zona demilitarizzata.

LA ZONA DEMILITARIZZATA ( DNZ ) è una zona che permette l’accesso a chiunque. È progettata per isolare i servizi esposti al pubblico ( come un server web, di posta elettronica ( come nel nostro disegno) dalla rete interna.

Ora però non si ha più sicurezza facendo passare tutti e siamo troppo accessibili, quindi useremo un altro dispositivo di filtraggio, cioè il filtraggio per contenuto.

FILTRAGGIO PER CONTENUTO ( WAF )

Funziona in modo che quando arriverà un pacchetto esterno, questo filtro lo aprirà e leggerà il contenuto a livello di codice per assicurarsi che non sia malevolo, in quel caso lo blocca.

Per capire se un pacchetto è malevolo usa 2 soluzioni:

* INTERNO – utilizzando codice gia a sua disposizione
* IN ESTERNO – chiederà a siti terzi se il codice è malevolo. Confronterà con l’organizzazione OWASP il codice letto se corrisponde con la loro lista di codici malevoli. ( la loro organizzazione è in continuo aggiornamento di codici malevoli)

PROXY

E’ un server che si mette tra 2 indirizzi ip ( sia privati che pubblici che mischiati ) con lo scopo di camuffare l’ip pubblico.

Utilizzati per gestire il traffico di rete tra un client un server.

Si divide in :

* PROXY FORWARD – E’ un intermediario tra il client e un server, lo scopo è di nascondere l’ip del client
* PROXY REVERS – è un intermediario tra il client e uno o più servizi, gestendo le richieste provenienti dall’esterno verso l’interno. Questa è la soluzione migliore perché posso nascondere l’ip pubblico dei miei server ed in più posso mettere altre funzionalità come il waf, aspa, nat, ids,ips

SEGMENTAZIONE DI RETE

Sono dei dispositivi per proteggere la rete, sono lo stesso software.

IDS, INTRUSION DETECTION SYSTEM, è un Sistema che monitora il traffico di rete per rilevare potenziali minacce generando degli avvisi ( allert ) per gli amministratori di rete.

IPS, INTRUSION PREVENTION SYSTEM, oltre a rilevare le minacce mandando un avviso all’amministratore, in più la bloccherà il traffico sospetto.

Nella segmentazione di una rete non sempre è meglio l’ips che ha più funzionalità perché potrebbe dare falsi positivi ( quindi può sbagliarsi e riconoscere un ip di un collega come malevolo ).

Per questo motivo useremo l’IPS più esterno alla rete dalla parte web, e useremo l’IDS internamente per un discorso di accessibilità usando per proteggere i dati sensibili ( perché se dovesse arrivare un avviso all’amministratore sapendo che ci possono essere falsi positivi lui potrà subito intervenire e lascir passare, se avessimo messo l’IPS ogni volta blocca un ip non malevolo e farebbe rallentare tutto il processo dell’azienda )

SPIEGAZIONE DISEGNO:

Tracceremo come prima cosa il perimetro del nostro firewall perimetrale tra la nostra LAN e la WAN esterna cosi da proteggere la nostra rete.

Successivamente inseriremo una DNZ che proteggerà i servizi esposti al pubblico come la posta elettronica o il nostro e-commerce.

Internamente poi inseriremo un dispositivo IDS a proteggere i nostri dati sensibili nel NAS, mentre useremo un IPS per proteggere i servizi esterni.