Nel progetto odierno è stata ideata la rete di una possibile attività di e-commerce.

Nella progettazione della rete sono stati inserite diverse componenti indispensabili volte alla creazione di una rete sicura e molto difficile da attaccare. Primo tra tutti, di importante considerazione è senza dubbio l'inserimento di un firewall hardware, ma cos'è un firewall?

Un firewall è un dispositivo o software di sicurezza che monitora e controlla il traffico di rete in entrata e in uscita sulla base di regole di sicurezza predefinite, modificabili a seconda delle necessità. La prima differenza da citare è quindi senza dubbio la presenza di due tipologie di firewall, il firewall hardware, e il firewall software. Il primo è un dispositivo configurabile volto alla gestione di un gran numero di connessioni, utilizzato principalmente da aziende medio grandi, con caratteristiche e prezzi differenti in base alle varie necessità dell'azienda. Il secondo, software, si può reperire anche in modo gratuito, ma a differenza dell'hardware esso può essere installato direttamente su un dispositivo; la grande limitazione di ciò deriva però dal fatto che indipendentemente da quanto potente sia la macchina esso avrà dei limiti perché non sarebbe in grado di gestire un gran numero di connessioni. Infatti questa potrebbe essere una soluzione ideale solamente nel caso di piccole aziende in cui il numero di connessioni si aggiri intorno alle 30, superato questo limite è altamente consigliabile l'utilizzo di un firewall hardware.

Una seconda differenza importante è senz'altro tra il firewall perimetrale ed il firewall non perimetrale. Il non perimetrale si colloca all'interno della rete LAN, e la sua funzione di difesa è volta a proteggere quindi la rete interna, o in maniera più precisa, delle porzioni specifiche della rete interna, soprattutto nel momento in cui si parla di reti segmentate, non solo per proteggersi dalle minacce ma anche pere limitare rischi ed acceso a diverse sezioni della rete.

Il perimetrale invece, è situato a cavallo tra la rete WAN (Wide Area Network) e la rete LAN (Local Area Network), e svolge due funzioni, la prima è quella di bloccare tutti i tentativi di connessione tra l'esterno verso l'interno, la seconda è quella di permettere il passaggio di pacchetti tra l'interno e l'esterno. Esistono 3 tipi in particolare di firewall, il firewall a filtraggio statico, dinamico e con filtro WAF (Web Application Firewall). La prima tipologia di firewall, statico, è stata la prima ad essere utilizzata, e consisteva in una lista, o tabella, nella quale si potevano inserire gli indirizzi IP da bloccare, e a quali invece permettere la comunicazione. questo sistema lasciava però molto a desiderare, poiché visto che non erano molti gli indirizzi IP all'inizio era facilmente aggirabile camuffando il proprio indirizzo IP. Intorno alla fine degli anni 90 a causa del boom di Internet, si verificò inoltre un alto grande problema, ovvero gli indirizzi IP diventarono troppi ed impostarli all'interno di un firewall statico sarebbe stato pressoché impossibile, ragion per cui si passò ad un altro tipo di filtraggio.

Si passò dunque alla seconda tipologia di firewall, a filtraggio dinamico, il quale bloccava automaticamente le connessioni provenienti dall'esterno, e permetteva solo quelle da interno ad esterno, il quale presenta una memoria cache che si resetta ogni qual volta chiudiamo una connessione con l'esterno, e possiede due liste per le creazioni di alcune eccezioni, white list e black list. Con questa soluzione però sorge un problema lampante, ovvero non sarà possibile connettersi con nessuno sulla rete, questo perché tutti saremo l'esterno per tutti. Per far fronte a questo notevole problema, è stato quindi ideato una tipologia di filtraggio chiamata WAF.

I firewall con filtraggio WAF, sono presenti all'interno delle aziende. Queste ultime per poter comunicare con quelli che saranno possibili futuri clienti o utilizzatori di determinati servizi, avranno a disposizione una zona particolare, chiamata DMZ (Demilitarized zone). Esse sono zone che consentono a qualunque dispositivo di connettersi, ragion per cui subentra il filtro WAF; il firewall con questo particolare filtro prenderà tutti i pacchetti in arrivo dalla DMZ, li spacchetterà, ed andrà alla ricerca di codice malevolo. Il confronto per la verifica avviene in due modi, il primo è inserendo nel firewall una tabella contenenti tutte le informazioni volte a rintracciare codice malevolo, ma ciò potrebbe risultare poco efficace poiché contengono un gran numero di dati. Il secondo invece consiste nel confronto con specifiche tabelle presenti

su siti di terze parti come OWASP. Il database di quest'ultimo è frequentemente aggiornato e contiene tutte le informazioni relative a possibili malware, fatta eccezione per gli zero days, malware giorno zero, dei quali fino a poco tempo fa non si aveva notizia. La scelta ottimale sarebbe quindi fare affidamento ad OWASP e fornire una tabella contenenti informazioni di specifici malware all'interno del WAF, senza sovraccaricarlo di informazioni.

Altri elementi volti alla difesa della rete di rilevante importanza, sono IDS (Intruder Detection System) e l'IPS (Intruder Protection System). Queste due tecnologie di sicurezza complementari svolgono un ruolo molto importante della protezione di reti e sistemi.

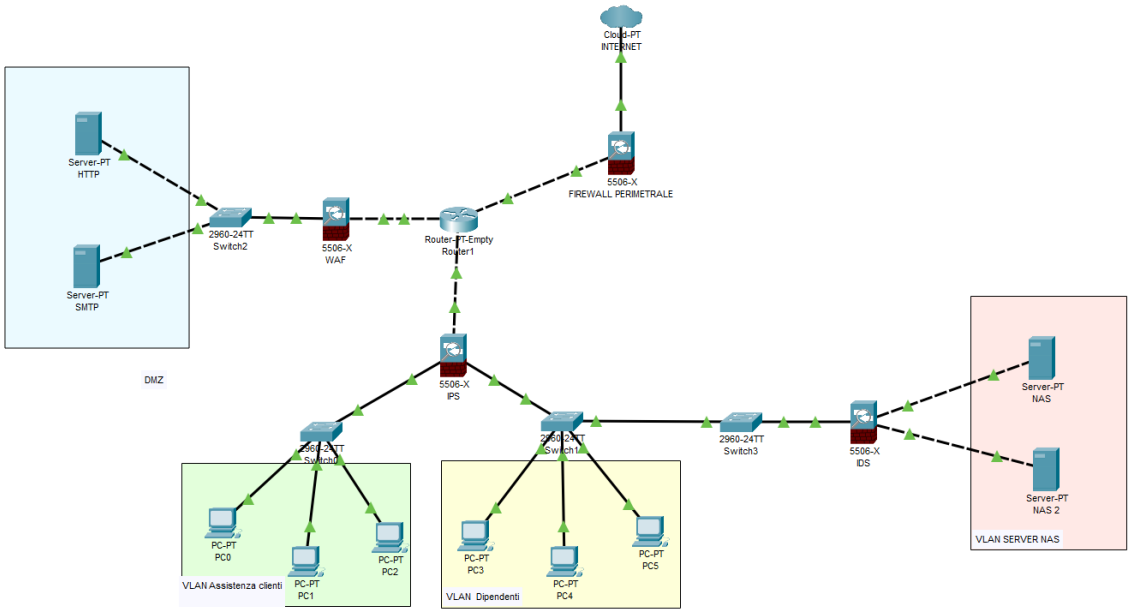
L'IPS può essere collocato in diverse posizioni all'interno della struttura della rete, ad esempio in seguito ad un filtro WAF qualora sia presente una DMZ, oppure come nella rete progettata, affiancando i router gateway. La funzione dell'IPS è quella di spacchettare, controllare un pacchetto malevolo qualora riuscisse a bypassare le prime difese, e nel caso si tratti proprio di file malevolo, questo lo bloccherà automaticamente e invierà un alert per segnalare il fatto che si sia imbattuto in un file malevolo.

L'IDS svolge la medesima funzione dell'IPS, ma con una differenza; anziché bloccare il file malevolo manderà soltanto un alert. Allora perché si preferisce avere più IDS (maggiormente utilizzato nelle aziende) rispetto agli IPS? Questo perché queste due tecnologie possono soffrire di falsi negativi, per cui anche se qualcuno ha l'autorizzazione ad accedere ad un determinato file, nel momento di un riscontro falso negativo, si otterrà comunque un blocco dei pacchetti, causando quindi dei problemi all'interno di un'azienda, nonché l'impossibilità di accesso a quel determinato file. A difesa dei NAS ad esempio (Network-attached storage), dispositivi di archiviazione collegati ad una rete che consentono l'accesso e la condivisione dei dati fra più utenti costituiti da uno o più dischi rigidi, sono spesso posti degli IDS, poiché nel momento in cui si ricevano degli alert, è possibile controllare l'accaduto senza intaccare in modo importante i dati e il lavoro in azienda.

In merito a queste conoscenze la rete progettata è stata quindi suddivisa con un firewall perimetrale tra WAN e LAN, un firewall a filtraggio WAF a difesa dalla DMZ, un IPS a difesa della rete locale in caso di possibili bypass che eludano i firewall, e un IDS a difesa dei server NAS. Ad incrementare ancora di più la sicurezza è stata inoltre effettuata una divisione in più sottoreti ricorrendo alle VLAN (Virtual Local Area Network), una tecnica nata appositamente allo scopo di dividere una rete in più sottoreti.

Sarebbe stato inoltre possibile ricorrere ad altre due opzioni volte ad un ulteriore incremento della sicurezza. La prima opzione è quella di considerare il posizionamento di un secondo firewall di backup, in caso si verifichino guasti accidentali, il quale si potrebbe impostare su active/standby o active/active.

La seconda opzione sarebbe quella dell'aggiunta di un proxy, anche se molto costosa. Un proxy è un server posto tra due indirizzi IP il cui primo grande vantaggio è quello di camuffare il nostro indirizzo IP. Esso si divide in proxy forward, noi utenti che andiamo verso un target, e proxy reverse, quando il mondo passa per questi ultimi fino ad arrivare a noi, come un'azienda che riceve. Il secondo punto forte di un server proxy è che si presenta come una tela bianca, ovvero vi si può inserire qualunque cosa. Nello scenario ideale sarebbe quindi opportuno avere un server proxy (reverse) munito di molteplici servizi, gestiti in modo ottimale grazie alla capacità di gestione del carico che un server proxy possiede, affinché funga da prima grande barriera, fatta ad eccezione del firewall, che sarà invece collocato subito dopo, e in seguito la nostra rete con la corretta e dovuta progettazione.


Cloud-PT
INTERNET
5506-X
FIREWALL PERIMETRALE
Server-PT
HTTP
Server-PT
SMTP
2960-24TT
Switch2
5506-X
WAF
Router-PT-Empty
Router1
DMZ
5506-X
IPS
2960-24TT
Switch1
2960-24TT
Switch3
5506-X
IDS
Server-PT
NAS
Server-PT
NAS 2
VLAN SERVER NAS
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
VLAN Assistenza clienti
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
VLAN Dipendenti