PROGETTO S3L5

Il firewall è una componente (hardware o software) fondamentale nella sicurezza informatica, perché ci permette di proteggere una rete da possibili attacchi.

La decisione di scegliere un firewall di tipo hardware da uno di tipo software non dipenderà dalla potenza della protezione che si vuole ottenere, ma dalle prestazioni necessarie in un ambiente di rete; l’efficienza del firewall dipende da quante connessioni al secondo quel firewall deve gestire, quindi più i componenti sono validi maggiori saranno le prestazioni.

I firewall possono distinguersi in due categorie:

* Perimetrali: che si trovano a perimetro tra una rete interna ed una esterna e che quindi proteggono la lan da attacchi esterni:
* Non perimetrali: che si trovano completamente all’interno di una rete e quindi possono proteggere o l’host a cui si collegano o diversi host collegati ad uno stesso braccio di rete;

Questo sistema di difesa può presentare diversi tipi di filtraggio che si distinguono in base al modo in cui scelgono di filtrare i pacchetti in entrata ed uscita.

* A filtraggio statico: firewall perimetrale che valuta i pacchetti in base a delle regole preimpostate che riguardano indirizzo IP e porte.

Il firewall presenta una tabella interna chiamata ACL in cui verranno inseriti gli indirizzi IP che dovranno essere bloccati e quelli che invece potranno passare. Quando il firewall entra a contatto con il pacchetto lo confronterà con la sua ACL dall’alto verso il basso e alla prima corrispondenza che troverà si fermerà ed eseguirà quello che la tabella impone.

Questo tipo di filtraggio è ormai obsoleto sia per l’aumento spropositato degli indirizzi IP negli anni che rende la pratica di inserirli a mano ormai problematica, sia perché era molto vulnerabile allo spoofing (=falsificazione dell’identità).

* A filtraggio dinamico: utilizzato nella rete in figura perché è il tipo di filtraggio più usato a livello perimetrale.

Anche il filtraggio dinamico, come quello statico, presenta una lista interna che in questo caso è una memoria cash che viene resettata ogni volta che la connessione viene chiusa; e decide se bloccare o far passare il pacchetto in base all’indirizzo IP che lo spedisce, questo perché questo tipo di filtraggio permette invio di pacchetti solo se la connessione parte dall’interno della rete, e blocca tutte le connessioni che hanno origine dall’esterno.

Questo tipo di filtraggio ha però sollevato una problematica; ovvero che in questo modo, se ogni rete presentava un firewall a filtraggio dinamico come perimetrale, nessuno poteva entrare in contatto con nessuno perché ogni pacchetto esterno veniva automaticamente bloccato; per questo motivo si crea la DMZ ovvero una zona demilitarizzata in cui vengono permesse connessioni interne ed esterne a qualsiasi server si trovi all’interno di quella zona. La dmz permette quindi ad un’azienda di mettere in comunicazione con il mondo i server web anche in presenza del firewall a filtraggio dinamico.

Esistono altri due tipi di filtraggio:

* Filtraggio per contenuto = WAF: non ci si basa più soltanto su indirizzo IP e porte, ma anche sull’oggetto presente nel pacchetto.

Il waf compara il contenuto con una tabella o interna o esterna; se da questa comparazione stabilisce che quel pacchetto è malevolo lui gli bloccherà il passaggio.

* Proxy: è un server che fa da filtro tra due indirizzi IP pubblici e/o privati mostrando, durante una connessione, come indirizzo IP quello del proxy stesso e non quello dell’host che protegge.

Esistono, oltre al firewall, altre tecnologie di sicurezza come l’IDS e l’IPS che lavorano come software di sicurezza e che ci permettono di segmentare la rete ulteriormente per renderla più sicura.

La differenza tra questi due software è che l’ids se riconosce un pacchetto come malevolo manderà solamente un allert senza agire; mentre l’ips quando riconosce un pacchetto come malevolo, non solo manderà un allert, ma agirà in maniera attiva, che il 90% delle volte comporta il bloccare il pacchetto in maniera del tutto autonoma.

L’ips però tende a soffrire di falsi positivi; questo suo agire in maniera autonoma può portare al non permettere il passaggio di pacchetti che lui riconosce come malevoli ma che effettivamente non lo sono.

Per questo motivo, all’interno di una rete, si preferisce inserire l’ips a protezione di quella che è la parte più esposta della rete e da cui potenzialmente possono entrare più pacchetti malevoli, ovvero quella all’interno della zona demilitarizzata; ed inserire l’ids a protezione di quelli che sono i dati più sensibili all’interno della mia lan e che molto spesso si trovano all’interno del NAS; cosicché anche se questi dati sensibili verranno riconosciuti come malevoli non ci sarà rischio di perderli.