Il Mio Primo Firewall IP

Si parla molto dell'uso di Firewall nelle reti IP, ma con l'eccezione di pochi esperti, ai più non è chiaro cosa veramente faccia, o meglio possa fare un firewall. In questo articolo cercheremo di descrivere i primi passi per la configurazione di un semplice firewall.

1. Le basi

Come attività minima, un firewall funziona come un filtro e decide se un pacchetto IP può attraversarlo o meno. Supponiamo di avere un firewall con 3 interfacce fisiche Ethernet dagli ovvi nomi: `WAN`, `LAN` e `DMZ`. Il firewall contiene una tabella di regole che vengono esaminate nell'ordine dato[1], la prima regola trovata che si applica ad un pacchetto arrivato (in entrata od uscita) su di una interfaccia, viene messa in atto e le seguenti non vengono esaminate. Le azioni principali sono di permettere o pure negare il passaggio del pacchetto IP.

2. Il progetto

Prima di tutto guardiamo il traffico dal punto di vista delle macchine presenti nelle 3 zone nel nostro network ideale, ove poniamo nella DMZ solo dei proxy ed un server Web:

1. da WAN al FW: accesso libero a tutti ma solo verso il server Web e di posta elettronica che sono in DMZ
2. dal FW a WAN: solo dalla DMZ e solo i servizi di posta elettronica, DNS, Web, ftp, SSH
3. da DMZ al FW: solo alla WAN per i servizi di posta elettronica, DNS, Web, ftp, SSH
4. dal FW a DMZ: dalla WAN solo Web e posta elettronica, dalla LAN i servizi di posta elettronica, DNS, Web-proxy, ftp, SSH
5. da LAN al FW: solo alla DMZ per servizi di posta elettronica, DNS, Web-proxy, ftp, SSH
6. dal FW a LAN: nulla

Nell'enunciare queste regole abbiamo assunto la logica di *tutto quello che non è esplicitamente permesso è vietato* ed indicato solo la direzione dei pacchetti che aprono una nuova connessione IP. E' chiaro inoltre che i vari punti della tabella devono corrispondersi, ovvero un servizio che la LAN chiede alla DMZ deve poter entrare nel firewall dalla LAN, uscire verso la DMZ, e poiché in questa configurazione nella DMZ abbiamo posto dei proxy, deve poi rientrare nel firewall dalla DMZ ed uscire verso la WAN, e così via.

Visto che ci sono ripetizioni in questa tabella, potremmo decidere di mettere i filtri solo una volta oppure ripeterli. Se si pongono una volta sola, è conveniente porli sulla interfaccia di ingresso dei

1 Alcuni firewall riordinano le regole inserite dall'utente secondo una logica interna, la maggior parte invece mantiene l'ordine come inserito dall'utente.

pacchetti nel firewall, se si pongono più volte si aumenta la sicurezza, ma si complica la configurazione e si diminuiscono le prestazioni.

3. Il tipo di Firewall

In generale vi sono tre categorie di firewall:

1. **Packet Filtering**: ogni pacchetto passa attraverso la stessa lista di regole, ed è necessario introdurre regole sia per i pacchetti di andata che per quelli di ritorno (richiesta/risposta);
2. **Stateful Firewall**: il primo pacchetto di una connessione IP passa attraverso tutte le regole, e se viene permesso il suo passaggio, il firewall se ne ricorda ed automaticamente permette il passaggio a tutti i pacchetti in entrambe le direzioni che fanno parte della stessa connessione IP.
3. **Proxy e Application Layer**: questi firewall sono in grado di ispezionare il contenuto dei pacchetti al livello 7, ovvero capiscono protocolli quali http, smtp, ftp ecc. e sono in grado di negare il passaggio a pacchetti il cui contenuto si ritiene pericoloso, dai virus della posta elettronica agli applet java per il web.

Ovviamente in commercio ci sono firewall che uniscono caratteristiche di tutte e tre le classi. E' ovvio che la terza classe è la più interessante, ma è anche la più difficile da gestire, richiede maggiori risorse ed inoltre non esistono ad esempio proxy per tutti i protocolli e le applicazioni. Pertanto qui consideriamo uno Stateful Firewall.

4. Le regole

In uno Stateful Firewall dobbiamo fare una differenza fra il primo pacchetto di una connessione IP e tutti i seguenti in quanto il firewall ha una tabella nella quale sono memorizzate tutte le connessioni IP che sono state permesse e sono attive (*established*). Adottando un linguaggio simbolico, scriviamo le regole del nostro firewall in Tabella 1. Il significato di ogni regola è il seguente: il primo è il numero della regola; segue l'azione da fare se la regola si applica al pacchetto in esame, le azioni sono A per Accept, D per Drop o Deny, e R per Reject; segue il protocollo IP (i.e. tcp, udp ecc., ip indica qualunque protocollo), poi l'indicazione dell'interfaccia, del numero IP e della porta (ove significativa) di ingresso e di uscita, ed infine possibili opzioni, flags od azioni aggiuntive.

La regola 1 accetta qualunque pacchetto che corrisponda ad una connessione IP presente ed attiva nella tavola delle connessioni *established* e per le quali un precedente pacchetto è stato accettato dalle altre regole. Questa regola è messa per prima perché la maggior parte dei pacchetti saranno accettati da questa regola e quindi il firewall dovrà fare meno lavoro ed introdurrà minori ritardi. I pacchetti che non sono accettati da questa regola devono pertanto essere pacchetti che vogliono

aprire nuove connessioni. Tutte le regole seguenti servono ad accettare solo pacchetti in arrivo al firewall che richiedono l'apertura di connessioni permesse nell'elenco fatto precedentemente nella sezione 2. Le regole da 2 a 8 negano il passaggio a pacchetti in arrivo da internet sull'interfaccia `WAN` con indirizzi IP non validi o che appartengono alla nostra `DMZ` (1.2.3.0/24). L'estensione `LOG` richiede di inviare un messaggio di errore nei log del firewall nel caso arrivi uno di questi pacchetti. Le regole 9 e 10 impongono che solo pacchetti con il corretto numero IP sorgente possano uscire dalle reti `LAN` e `DMZ` (il ! indica la negazione della condizione). Un pacchetto che ha passato tutte queste regole ha un indirizzo IP sorgente accettabile.
Le regole 11 e 12 permettono il passaggio a pacchetti che incominciano nuove connessioni tcp (flag `syn`) da internet verso il server di posta elettronica (1.2.3.2/32 porta 25) ed il server web (1.2.3.3/32 porta 80 e 443) in `DMZ`. Le regole 13 e 14 permettono al proxy (1.2.3.4/32) in `DMZ` di uscire verso internet. Insieme le regole da 11 a 14 soddisfano i punti 1, 2 e 3 indicati in sezione 2. Le regole 15 e 16 permettono alla `LAN` di comunicare con il proxy in `DMZ` e soddisfano i punti 4 e 5 indicati in sezione 2. La regola finale nega qualunque pacchetto che sia arrivato sino a questo punto. Il punto 6 indicato in sezione 2 è garantito dal fatto che non vi è alcuna regola che permette di aprire connessioni verso la LAN.

5. Conclusioni

Le regole indicate nella Tabella 1 sono solo il primo passo per la costruzione di un vero firewall. Ad esempio non abbiamo considerato i pacchetti di errore di tipo `ICMP` la cui gestione è essenziale per un corretto funzionamento della connettività IP. Bisogna poi considerare per quali protocolli è conveniente utilizzare l'azione Reject che invia un messaggio di errore al mittente oltre a negare il passaggio al pacchetto, piuttosto che l'azione Drop che abbiamo utilizzato; ad esempio per un migliore funzionamento dei server di posta elettronica può essere necessario utilizzare Reject per i pacchetti del protocollo `identd`. Bisogna tenere in considerazione i problemi di Denial of Service (DoS) anche per quanto riguarda i messaggi di errori inviati all'operatore. Vi sono poi protocolli, quali ftp, che richiedono l'apertura di più connessioni contemporanee in modo dinamico, problema che i più moderni firewall sono in grado di gestire automaticamente all'interno delle connessioni IP *established*.

Il problema principale nella costruzione di un firewall IP non è però nella tecnologia o nel linguaggio delle regole, bensì nella strategia e nella logica adottate per la costruzione delle regole di filtro del traffico.

Andrea Pasquinucci
Consulente di Sicurezza Informatica
pasquinucci@ucci.it

Riferimenti Bibliografici:

[1]B. Cheswick e S. Bellovin, *Firewalls and Internet Security*, Addison-Wesley

[2]E.D. Zwicky, S. Cooper e D.B. Chapman, *Building Internet Firewalls*, O'Reilly

[3]Una lista elettronica dedicata ai firewall è Firewall-wizard:
http://honor.icsalabs.com/mailman/listinfo/firewall-wizards

```
1  A ip FROM any any any TO any any any WITH established
2  D ip FROM wan 0.0.0.0/8 any TO any any any WITH log
3  D ip FROM wan 10.0.0.0/8 any TO any any any WITH log
4  D ip FROM wan 127.0.0.0/8 any TO any any any WITH log
5  D ip FROM wan 172.16.0.0/12 any TO any any any WITH log
6  D ip FROM wan 192.168.0.0/16 any TO any any any WITH log
7  D ip FROM wan 224.0.0.0/3 any TO any any any WITH log
8  D ip FROM wan 1.2.3.0/24 any TO any any any WITH log
9  D ip FROM lan !192.168.1.0/24 any TO any any any WITH log
10 D ip FROM dmz !1.2.3.0/24 any TO any any any WITH log
11 A tcp FROM wan any any TO dmz 1.2.3.2/32 25 WITH syn
12 A tcp FROM wan any any TO dmz 1.2.3.3/32 80,443 WITH syn
13 A tcp FROM dmz 1.2.3.4/32 any TO wan any 21,22,25,53,80,443 WITH syn
14 A udp FROM dmz 1.2.3.4/32 any TO wan any 53
15 A tcp FROM lan 192.168.1.0/24 any TO dmz 1.2.3.4/32 21,22,25,53,80,443 WITH syn
16 A udp FROM lan 192.168.1.0/24 any TO dmz 1.2.3.4/32 53
17 D ip FROM any any any TO any any any WITH log
```

Tabella 1