SICUREZZA NELLE RETI a. a. 2012/13 – Riassunto Firewall

by Salvatore Fresta

Un **firewall** è un dispositivo che, secondo una politica di accesso, **stabilisce quale traffico ha accesso alla rete** e quale no. I firewall possono **operare** a diversi livelli:

- livello **applicativo** (proxy)
- livello di **trasporto** (circuit gateway)
- livello di **rete** (packet filter)

Esistono anche firewall chiamati **dynamic packet filter** che **agiscono a più livelli**. Il filtro dei pacchetti avviene in modo isolato (**stateless filtering**) o tenendo conto anche della storia dei pacchetti e dello stato della connessione (**stateful filtering**).

Nello stateless filtering si controlla una **lista di regole** denominata **Access Control List** (ACL) applicata ad ogni pacchetto in scansione. Si controlla la lista regola per regola dall'alto verso il basso fino a trovare quella che combacia con il pacchetto. Nel caso in cui nessuna delle regole specifiche combacia, si usa la regola di default che può essere **default deny**, ovvero **vietare** tutto il traffico che non viene **esplicitamente permesso**, o **default permit** (o allow), ovvero **consentire** tutto il traffico che non viene **esplicitamente vietato**.

Ogni regola è strutturata da un **verso** (IN/OUT), **IP sorgente** e **destinatario**, **protocollo**, **porta sorgente** e **destinazione**, **flag** (ACK attivo o no, solo in TCP), **azione** (permit/deny).

Per **proteggersi dall'ip spoofing** si usano regole chiamate **egress-ingress**. In pratica bisogna vietare il traffico in ingresso ad una rete avente come indirizzo IP sorgente un'indirizzo della rete interna e vietare il traffico in uscita dalla rete avente come indirizzo IP sorgente un indirizzo non appartenente alla rete interna. Esempio:

> *se la rete è 192.168.1.0/24, devo vietare il traffico in ingresso da una rete esterna avente un indirizzo IP come 192.168.1.xxx e vietare il traffico diretto alla rete esterna avente come indirizzo IP sorgente un indirizzo che **non** appartiene a tale classe di indirizzi, come per esempio 172.16.10.13.*

Nello **statefult filtering** invece si tiene conto della storia dei pacchetti e dello stato della connessione, per cui occorre tenerne traccia tramite una **tabella delle connessioni**. Vi sono firewall stateful che possono **analizzare anche il payload** dei pacchetti, generalmente facendo matching di stringhe. Questi ultimi prendono il nome di **deep packet filters** o inspection.

Un **bastion host** è un nodo particolarmente protetto che può essere lasciato al nemico senza compromettere la rete interna.

Esistono **3 tipi di configurazione di una rete con firewall**:

1. **Single Homed Bastion Host**: se il firewall viene compromesso, la rete rimane protetta dal bastion host.

2. **Double Homed Bastion Host**: il bastion host ha due interfacce di rete in modo da creare una rete più protetta ed inaccessibile dall'esterno.

3. **Screened subnet**: si usano due firewall per creare una zona di interdizione (DMZ)

Si dicono **firewall friendly protocols** tutti quei protocolli dove **i ruoli di client e server sono costanti** (ovvero non si scambiano di posto durante la connessione come in FTP) e lo scambio di informazioni è un classico **request/reply**.