Iptables Linux appunti

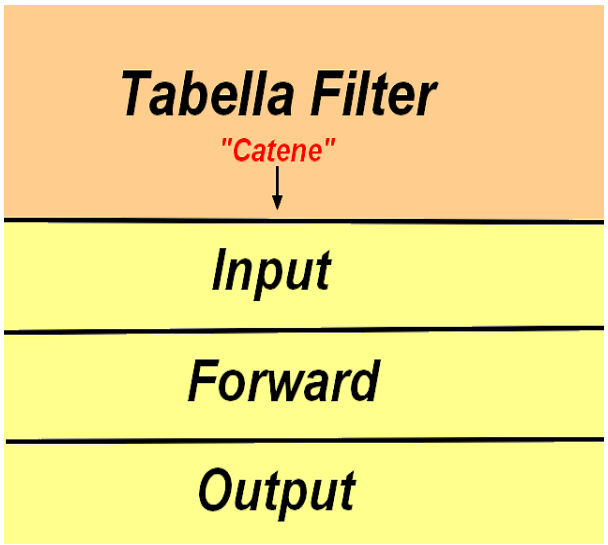
Il firewall sotto Linux è stato sviluppato da **netfilter.org project** il quale ha sviluppato una serie di comandi (il più famoso in realtà è **iptables** una sorta di “framework” di packet filtering). Iptables altro non è che un comando che istruisce il Kernel Linux (direttamente) a fare delle delle operazioni di filtraggio o di mascheramento dei pacchetti tipiche di un firewall passando dei comandi umanamente leggibili tramite il comando iptables.
Iptables non è il firewall, è un programma che va ad istruire il Kernel Linux su come operare.
Praticamente in Linux il firewall è il Kernel stesso, a differenza di altri sistemi operativi dove il firewall è un programma che avviene aggiunto sopra, quindi, se in Linux “crasha” il firewall crasha anche il Kernel perché lavora appunto a livello Kernel.
Iptables è un'interfaccia testuale per passare i comandi al kernel.

IP= indirizzo ip Tables= tabelle

Il firewall Linux con iptables gestisce le regole tramite delle tabelle che sono a loro volta dei contenitori di regole. Queste regole vengono passate (e divise) tramite catene e tabelle.
Ogni tabella ha un nome e ogni tabella contiene delle catene che a loro volta contengono le regole vere e proprie. Le tabelle individuano il ruolo che ha questo programma di filtraggio, la più famosa è la tabella **filter** che è la tabella che contiene le regole vere e proprie di firewall ovvero blocco o permetto il passaggio di alcuni pacchetti .
Per lavorare sulla tabella filter digitiamo il comando:

Iptables -t filter

è talmente importante questa tabella che se non specifichiamo l'opzione -t la prende in automatico (filter infatti è la tabella di default).
Ogni tabella contiene delle catene native;
la tabella filter contiene le catene: **input**, **forward**, **output**. Schema della tabella filter:



Dentro la catena **input** ci vanno inserite le regole di filtraggio per i pacchetti provenienti dall'esterno. Dentro a **output** al contrario ci vanno inserite le regole di filtraggio per i pacchetti provenienti dall'interno verso l'esterno. **Forward** invece gestisce tutte le regole delle connessioni dei pacchetti che attraversano il computer, o meglio che sono rivolte non direttamente al nostro computer ma a un altro che (per raggiungerlo) deve attraversare prima il nostro (come se fosse un router).