# LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS





## Tables

Fiecarui hook/chain NETFILTER ii este asociat un set de reguli definite intr-un tabel. In momentul in care un pachet "loveste" un chain acesta este verificat de fiecare regula din tabel.
O regula contine criterii care trebuie satisfacute de pachet si un target precum ACCEPT, DROP sau SNAT. Targetul este actiunea intreprinsa daca pachetul satisface regula din tabel. Fiecare regula are un target.

### Exemplu

Cerinta: Dorim sa blocam/dropam toate pachetele care vin catre serverul SSH ce ruleaza pe hostul local si asculta pe portul TCP/22.

Mod realizare: Orice pachet destinat hostului local va trece prin chain-ul INPUT. Acesta va fi si chain-ul in care intervenim pentru droparea/blocarea pachetelor ssh. Intr-un tabel (numit filter) atasat chainului INPUT vom adauga o regula compusa din criterii precum: pachetul este destinat hostului local, iar portul destinatie este 22. Target-ul va fi DROP.

In mod implicit NETFILTER ofera 4 tabele ce contin reguli pentru "prinderea" pachetelor si care se ataseaza de cele 5 chain-uri.

Tabele NETFILTER:

1. filter
Este folosit doar pentru filtrarea pachetelor ( ACCEPT sau DROP) si se foloseste doar pe chainurile FORWARD, INPUT sau OUTPUT.

2. nat
Este folosit doar pentru NAT (SNAT si DNAT). Doar primul pachet dintr-un stream va fi procesat de regulile din acest tabel. Asupra celorlalte pachete se va actiona identic. Se poate atasa de chainurile PREROUTING in cazul DNAT (port forwarding) si POSTROUTING in cazul SNAT.

3. mangle
Este folosit pentru manipularea/modificarea pachetelor si anume modificarea headerelor de Layer3 si Layer4 (modificare tos, ttl etc).
Acest tabel poate fi atasat de orice chain.

4. raw
Se foloseste doar pentru marcarea pachetelor care nu trebuie sa fie procesate de "connection tracking system". Tabelul se poate folosi doar pentru chainurile PREROUTING si/sau OUTPUT. Mecanismul de "connection tracking" este consumator de resurse, astfel pentru un anumit tip de trafic se poate opri connection tracking system.
Exemplu: excluderea traficul generat pentru localhost

### Nota

Cele 4 tabele descrise mai sus sunt implicite. Acestea nu pot fi sterse si nici alte tabele nu pot fi create.