LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Sintaxa iptables

Commanda iptables (user space tool) se foloseste pentru a comunica cu NETFILTER.

Important

1. Scopul comenzii iptables este de a adauga, sterge, inlocui, lista, vizualiza etc reguli din cele 4 tabele standard care sunt atasate de cele 5 chainuri. Comanda poate fi folosita doar de root.

2. In mod default nu exista nicio regula in tabele, acestea fiind goale. Implicit nu exista firewall.

3. Un pachet traverseaza in mod secvential regulile din tabelele atasate chainurilor pana in momentul in care o regula "prinde" pachetul, caz in care se executa TARGET-ul regulii. Restul regulilor din tabel nu se mai verifica ulterior.

4. Daca pachetul nu este prins de nicio regula din tabel se executa politica default (-P POLICY) care este implicit ACCEPT.

Structura comenzii iptables este:

```
iptables -t nume_tabel -OPERATIE_ASUPRA_CHAIN NUME_CHAIN -criterii -j TARGET
```

unde:

Nume tabel:
filter
nat
raw
mangle

Nota

Numele tabelului in care se adauga regula trebuie scris cu litera mica. Daca se omite numele tabelului acesta este default filter.

Exemplu

```
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
```

este echivalent cu:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Operatii asupra unui chain
-A -> adaugare regula la sfarsitul tabelului atasat chainului;
-I -> adaugare regula pe prima pozitie in tabelul atasat chainului;
-L -> listare reguli;
-P -> policy, actiunea default care se executa daca nicio regula nu prinde pachetul;
-N -> creare chain nou definit de utilizator;
-X -> sterge chain definit de utilizator;
-F -> flush, goleste regulile din tabelul atasat chainului;
-Z -> zero, reset counters;

Nota

Operatiile asupra regulilor din tabelele atasate chainurilor trebuie scrise cu litera mare.

Exemplu:

Adauga o regula la sfarsitul tabelului filter (default daca nu se specifica) pentru chain-ul OUTPUT care permite trimiterea de pachete catre IP-ul din spatele domeniului www.invata-online.ro

1. iptables -A OUTPUT -d www.invata-online.ro -j ACCEPT

Adauga policy DROP pentru INPUT. Orice pachet destinat hostului local care nu este acceptat de nicio regula din tabelul filter de pe chainul INPUT este dropat
2. iptables -P INPUT DROP

Sterge toate regulile din tabelul filter (default daca nu se specifica) de pe chainul FORWARDING
3. iptables -F FORWARDING

Nume Chain:
PREROUTING
INPUT
OUTPUT
FORWARD
POSTROUTING

Nota

Numele chainului se scrie cu litera mare

Exemplu:

1. Adaugam o regula in tabelul nat din POSTROUTING care realizeaza SNAT. IP-ul privat 10.0.0.3 este inlocuit cu ip-ul public al ruterului linux care este 80.0.0.10
iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.3 -j SNAT --to-source 80.0.0.10

2. Dropeaza toate pachetele generate de hostul local catre orice server http care daca acesta asculta pe portul 80
iptables -A OUTPUT -p tcp --dport 80 -j DROP

Criterii
-s IP_sursa
Exemplu: -s 80.0.0.1 sau -s 192.168.0.0/24 sau -s 0/0. Specifica IP-ul sursa din pachet. 0/0 inseamna orice IP

-d IP_dest
Exemplu: -d 182.0.10.1 sau -d 10.10.0.0/26 sau -d 0/0 -> specifica IP-ul destinatie din pachet. 0/0 inseamna orice IP

-p protocol
Exemplu: -p tcp sau -p udp sau -p icmp

--sport port_sursa
Exemplu: iptables -I INPUT -p udp --sport 53 -j DROP -> dropeaza toatea pachetele UDP care sunt destinante hostului local si vin de la un server DNS (port 53)

--dport port_dest
Exemplu: iptables -A FORWARD -p tcp --dport 8080 -j DROP -> dropeaza toata pachetele catre portul tcp 8080 care tranziteaza ruterul linux

-i interfata_in
Exemplu: iptables -A INPUT -i eth0 -j ACCEPT -> accepta toate pachetele destinate hostului local care intra pe interfata eth0

-o interfata_out
Exemplu: iptables -t mangle -A OUTPUT -o eth1 -j TTL --ttl-set 67 -> modifica TTL-ul din headerul IP setand valoarea 67 pentru toate pachetele generate de hostul local care ies pe interfata eth1

Nota

Intre criterii unei reguli exista SI logic. Acestea trebuie sa fie adevarate simultan pentru ca pachetul sa fie "prins" de regula si sa se executa TARGET-ul regulii.

Target
Specifica actiunea intreprinsa asupra pachetului daca criteriile sunt indeplinite.

ACCEPT -> pachetul este acceptat;
DROP -> pachetul este dropat;
REJECT -> pachetul este rejectat si hostul raspunde cu un mesaj de eroare sursei;
LOG -> logheaza/salveaza informatii despre pachet intr-un fisier;
LIMIT -> limiteaza nr. de pachete pe unitatea de timp;
SNAT -> realizeaza source nat;
MASQUERADE -> realizeaza source nat;

DNAT -> realizeaza destination nat/port forwarding;
TTL -> modifica TTL din pachet (headerul IP);

Nota

Numele targetului se scrie cu litera mare.

Important

Cuvintele cheie de mai sus trebuie scrise cu litera mare sau litera mica intocmai, altfel rezulta o eroare.

Rezumat:

- numele tabelului se scrie cu litera mica (-t nat);
- operatia asupra chain-ului se scrie cu litera mare (-A);
- numele chain-ului se scrie cu litera mare (FORWARD);
- criteriile se scriu cu litera mica (-s 192.168.0.0/16);
- targetul se scrie cu litera mare (-j DROP);

Resurse

- iptables syntax