LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Port Forwarding(DNAT)

Prin procesul de NAT intrega retea privata din spatele routerului este ascunsa pe Internet.
De multe ori se doreste conectarea la un serviciu (Exemplu: un server web) care ruleaza pe un host din LAN care este configurat cu IP privat (Exemplu: 10.0.0.1)

Procesul prin care Routerul se configureaza astfel incat sa ofere posibilitatea conectarii de pe Internet la un host din LAN cu IP privat se numeste DNAT (Destination Network Address Translation) sau Port Forwarding.

Exemplu topologie: Routerul are configurat un IP public pe interfata de WAN (Exemplu: 88.0.0.1) si un IP privat pe interfata de LAN (Exemplu: 10.0.0.1). In LAN exista un server web care asculta pe portul 80 si care are configurat IP-ul 10.0.0.10. Utilizatorii de pe Internet care doresc conectarea la serverul web privat nu-l pot accesa fara ca routerul sa fie configurat pentru DNAT.
Pentru userii de pe Internet reteaua 10.0.0.0/24 si implicit 10.0.0.10 sunt ascunse (nu exista).

Modul de functionare DNAT este urmatorul: userul de pe Internet se conecteaza la IP-ul public al routerului si anume 88.0.0.1 si portul 80. Routerul in momentul in care primeste pachete catre portul 80 le redirecteaza catre serverul din LAN 10.0.0.10 modificand IP-ul destinatie din fiecare pachet (88.0.0.1 se transforma in 10.0.0.10) - de unde si numele de DNAT. Pachetele ajung astfel la serverul web intern care raspunde catre IP-ul sursa public (acesta nu se modifica).

Nota

Din perspectiva clientilor de pe Internet acestia se conecteaza la serverul web care ruleaza pe router si nu la serverul web din spatele routerului.

Din punct de vedere al configurarii NETFILTER urmatoarele aspecte sunt importante:

- DNAT se realizeaza pe chainul PREROUTING folosind tabelul nat care este suficient sa contina o singura regula. Chainul folosit este PREROUTING fiindca regulile din acesta sunt evaluate inainte de procesul de rutare. In momentul in care are loc decizia de rutarea, routerul trebuie sa aiba acces la IP-ul final si anume cel privat pentru o deciezie de rutare corecta;
- se foloseste targetul DNAT;

Exemplu configurare router pentru DNAT:

```
#presupunem ca IP-ul public este 88.0.0.1 iar IP-ul serverului web din LAN este 10.0.0.10.
#Pachetele din exterior catre 88.0.0.1 vor fi redirectate la 10.0.0.10
iptables -t nat -A PREROUTING -p tcp -d 88.0.0.1 --dport 80 -j DNAT --to-destination 10.0.0.10
```

Important

Pentru ca DNAT sa functioneza Routerul linux trebuie sa fie configurat si pentru SNAT. Altfel pachetele ca raspuns ale serverului web din LAN care au ip sursa privat nu ar putea fi trimise catre IP-ul public destinatie care este pe Internet.

Resurse

- Port Forwarding - Wikipedia