Administrarea Retelelor

Configurarea unui firewall in Linux

Ce este un firewall

- Un firewall este un program menit sa protejeze calculatorul/reteaua locala de agresiuni din exterior
- Cel mai cunoscut firewall pentru Linux este *iptables*
- Functiile pe care le poate indeplini iptables sunt:
  - translatare de adrese sursa sau destinatie (SNAT / DNAT)
  - port forwading,
  - rejectare sau forwadare de pachete ,
  - routing.

Avantaje / dezavantaje

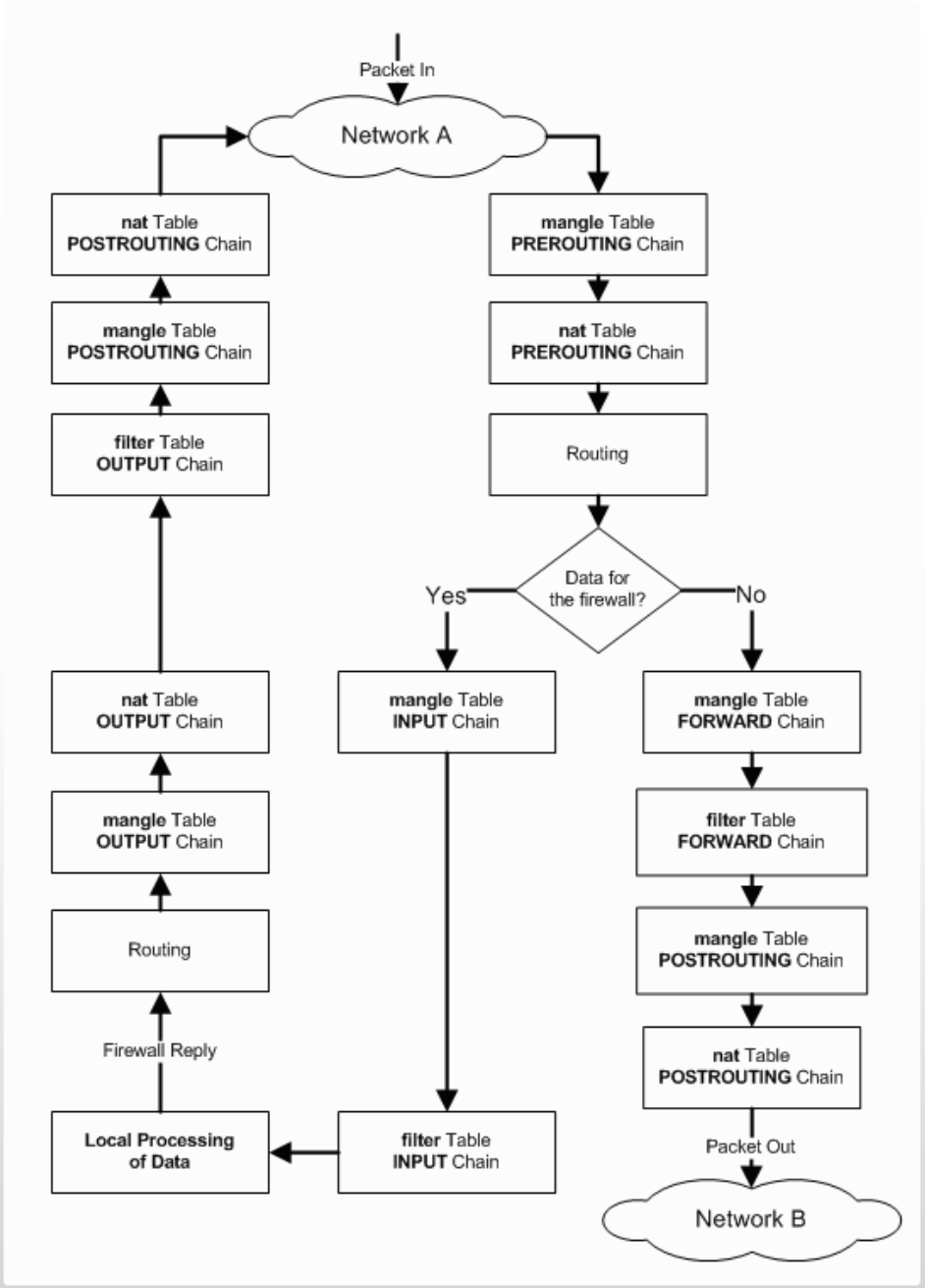
- O alternativa la iptables este Firestarter care are si GUI
- Avantaje iptables:
  - Nu are nevoie de interfata grafica pentru configurare
  - Poate fi configurat de la distanta printr-o conexiune ssh la calculatorul pe care ruleaza
- Dezavantaje:
  - In cazul conexiunii de la distanta, daca nu stim e facem putem sa ne intrerupem accesul inclusiv noua si sa nu mai putem sa deblocam decat mergand direct la calculatorul pe care il configuram. Daca acesta este in “China” acest lucru poate fi cam dificil.

Masuri de siguranta

- Pentru ca probabil dorim cel mai adesea configurarea firewalului de la distanta cum am putea proceda:
  - Instalam o masina virtuala si incercam pe ea configurarea si rularea iptables. Daca functioneaza bine, exportam setul de reguli de pe ea si il importam pe calculatorul “adevarat”
  - Daca lucram de la distanta, am putea sa configuram in prealabil un cron job care sa reseteze automat setul de reguli din iptables la o anumita ora, de exemplu cu 15 minute dupa ce am inceput. Daca am configurat totul bine si merge, anulam cron jobul inainte de a fi pornit.
    - crontab –e pentru scrierea sau stergerea unor cron job -uri
    - 30 08 31 07 * iptables –F

      Unde:

      30 – minutul 30; **08** – ora 8 AM; **31** – ziua a 31-a; **07** – luna a 7-a(iulie); ***** - in fiecare zi a saptamanii
    - Salvarea (pentru ca este folosit editorul vi) se face cu <Esc> :wq
    - Inceperea editarii (pentru ca este folosit editorul vi) se face cu *i


Packet In
Network A
nat Table POSTROUTING Chain
mangle Table POSTROUTING Chain
filter Table OUTPUT Chain
mangle Table PREROUTING Chain
nat Table PREROUTING Chain
Routing
Data for the firewall?
Yes
No
nat Table OUTPUT Chain
mangle Table OUTPUT Chain
Routing
Firewall Reply
Local Processing of Data
mangle Table INPUT Chain
filter Table INPUT Chain
mangle Table FORWARD Chain
filter Table FORWARD Chain
mangle Table POSTROUTING Chain
nat Table POSTROUTING Chain
Packet Out
Network B

Lanturi (chains)

- Sunt 3 lanturi predefinite in tabela de filtrare la care putem adauga reguli pentru procesarea pachetelor IP care traverseaza aceste lanturi. Acestea sunt:
  - INPUT – toate pachetele destinate calculatorului gazda.
  - OUTPUT - toate pachetele care au originea in calculatorului gazda.
  - FORWARD - toate pachetele care nu sunt nici destinate nici nu au originea in calculatorului gazda, dar sunt rutate (trec prin) calculatorul gazda. Acest lant este folosit daca folosim calculatorul ca un router
- In cea mai mare parte, ne vom ocupa de lantul INPUT pentru a filtra pachetele care intra calculatorul nostru – pentru a ne feri de atacuri.

1. Instalarea iptables

- Instalare
  - sudo apt-get install iptables — pentru Debian/Ubuntu
  - yum install iptables — pentru CentOs/Red Hat/Fedora
- Se poate edita manual fisierul de configurare
  - /etc/sysconfig/iptables
- Salvarea regulilor nu se face automat (nu persista unei reporniri).
- Pentru a salva setul de reguli putem folosi
  - service iptables save

Cum se porneste / reseteaza

- Pornirea sau oprirea iptables se face la fel ca orice alt serviciu:
  - service iptables start — porneste serviciul pentru sesiunea curenta
  - service iptables stop — opreste serviciul
  - service iptables status — verifica starea serviciului
  - service iptables save — pentru RH/CentOS/Fedora salveaza regulile iptables in fisierul /etc/sysconfig/iptables
  - iptables-save > /root/my.active.firewall.rules — iptables-save salveaza regulile iptables. In plus am facut si o copie de siguranta in fisierul my.active.firewall.rules (pentru celelalte distributii Linux). Utila la restaurarea iptables
- Automatizarea pornirii
  - chkconfig iptables on — seteaza ca serviciul iptables sa porneasca pe nivelele 2-5
  - chkconfig — pentru a verifica ce am facut

2. Restaurarea iptables

- Daca am sters tot sau partial iptables il putem restaura:
- Pentru RH/Fedora/CentOS cu
  - service iptables restart
- Pentru celelalte distributii, din fisierul de backup
  - iptables-restore < /root/my.active.firewall.rules

3. Stergerea

- Stergerea totala a listei de reguli
  - Iptables -F
- Stergerea doar a unei tabele (nat in acest exemplu)
  - iptables -t nat -F
- Stergerea doar a unui lant
  - Iptables –F INPUT
- Precautii. Inainte de a sterge toate regulile, sa stabilim politica de baza a celor 3 principale lantul ca fiind ACCEPT
  - iptables -P INPUT ACCEPT
  - iptables -P FORWARD ACCEPT
  - iptables -P OUTPUT ACCEPT

4. Listarea si stergerea unei reguli

- Afisarea regulilor iptables cu numerotarea liniilor
  - iptables -n -L -v --line-numbers
  - iptables -L INPUT -n --line-numbers
- Al doilea exemplu afiseaza doar lantul INPUT. In locul lui se poate pune un alt lant, OUTPUT sau FORWARD
- Daca dorim apoi sa stergem doar linia a 4-a din lantul INPUT:
  - iptables -D INPUT 4

5. Inserarea unei reguli noi

- Listam lantul de INPUT:
  - iptables -L INPUT -n –line-numbers
- Obtinem ceva ca mai jos, de exemplu:

Chain INPUT (policy DROP)

num	target	prot	opt	source	destination
1	DROP	all	--	202.54.1.1	0.0.0.0/0
2	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0

- Ca sa inseram o regula noua intre regulile 1 si 2:
  - iptables -I INPUT 2 -s 202.54.1.2 -j DROP

6. Blocarea unui domeniu

1. Aflarea IP-ului domeniului:
   host -t a www.facebook.com
2. Ar putea returna
   www.facebook.com has address 69.171.228.40
3. Pentru a afla CIDR pentru 69.171.228.40 dam
   - whois 69.171.228.40 | grep CIDR
4. Ar putea returna
   CIDR: 69.171.224.0/19
5. Blocarea accesului la www.facebook.com
   iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP

7. Politicile implicite

- Sunt 2 politici DROP si ACCEPT. La un firewall instalat nou politica este fie ACCEPT pentru toate lanturile fie DROP. Se poate verifica cu comanda

  iptables -L -v –n

7.1 Exemplu de firewall cu toate lanturile DROP

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables -L -v –n

In aceasta varianta nu ne vom putea conecta niciunde, tot traficul va fi oprit (DROPed)

7.2 Exemplu in care merge doar conexiunea catre exterior

7.2 Exemplu de firewall cu toate lanturile de INPUT si FORWARDING pe DROP si permite pachetele de iesire

iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -P FORWARD DROP

iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -L -v –n

In aceasta varianta ne vom putea conecta in exterior, iar traficul de intrare si care trebuie rutat va fi oprit (DROPed), cu exceptia traficului ca raspuns la o cerere originata la noi in sistem. Astfel conexiunile stabilite de noi vor functiona si nu vor fi respinse de lantul de intrare

7.3 Exemplu de firewall Stateful Packet Inspection (SPI) care va permite conexiuni catre exterior dar va bloca toate conexiunile de intrare nedorite

```
iptables -P INPUT ACCEPT
iptables -F
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
iptables -L -v
```

8. Blocarea unei adrese (interval)

iptables -A INPUT -i eth1 -s 192.168.0.0/24 -j DROP

9. Deschiderea unui interval de porturi

iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 7000:7010 -j ACCEPT

Bibliografie

- Manualul iptables (man iptables)
- Vivek Gite - Linux: 20 Iptables Examples For New SysAdmins https://www.cyberciti.biz/tips/linux-iptables-examples.html
- Mitchell Anicas - How to List and Delete Iptables Firewall Rules https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules
- Mitchell Anicas - Iptables Essentials: Common Firewall Rules and Commands **https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands**
- Tutorial IPTABLES firewall linux – comenzi de baza **http://tutoriale.eajutor.ro/unix-linux/tutorial-iptables-firewall-linux-comenzi-de-baza.html**
- Ramesh Natarajan - 25 Most Frequently Used Linux IPTables Rules Examples http://www.thegeekstuff.com/2011/06/iptables-rules-examples