Introducere

The Linux Firewall

Netfilter / Iptables

drd. Adam Mihai Gergely

Definiție

IPTABLES

- Firewall / Program de protecție și control a traficului pe sisteme Linux
- Reprezintă un Framework de aplicații la nivel de Kernel
- Structură ierarhică matriceală bazată pe CLI
- Operează pe bază de comandă cu parametri

Proprietăți

- Rulează pe sisteme Linux
- Operarea se face prin introducerea de comenzi de consolă (CLI)
- Operarea se face doar de către Supervizor (Root)
- Poate rula ca instanță individuală sau prin intermediul unor scripturi de configurare
- Este necesară încarcarea modulelor necesare de Kernel
- La activarea unei directive (comenzi), aceasta intră în efect imediat, fără delay
- Parcurgerea regulilor de firewall se face de SUS până JOS, în ordine, astfel încât prima regulă cu care se potrivește un pachet, aceea este executată direct fără a mai parcurge toată lista
- Dacă nu există vreo regulă pentru un pachet, atunci automat acel pachet se va accepta sau se va filtra în funcție de politica lanțului (Policy ACCEPT sau Policy DROP)

Operare (tabele de zone)

- Din punct de vedere al zonelor de operare, există 3 mari zone:
  - **FILTER** (-t filter):

    Tabelul de FILTER reprezintă zona de operare pe partea de **filtrare** prin acceptare/refuzare a traficului care îndeplinește anumite condiții

  - **NAT** (-t nat):

    Tabelul de NAT reprezintă zona de operare pe partea de **translație** de adrese de rețea din adrese private în adrese publice, și vice-versa în scopul rutării din rețele interne în rețele publice și vice-versa

  - **MANGLE** (-t mangle):

    Tabelul de MANGLE reprezintă zona de operare pe partea de **alterare** de pachete în tranzit prin schimbarea anumitor proprietăți în scopuri specifice.

Operare (moduri de manipulare)

- Din punct de vedere al modurilor de operare, există 3 moduri principale de operare:
  - **INSERT** (-I):

    Acest mod inserează o regulă chiar la început, pe prima poziție din lista firewall-ului, chiar dacă există deja reguli în lista de firewall
  - **APPEND** (-A):

    Acest mod inserează o regulă pe ultima poziție a listei de reguli din firewall. Dacă nu există reguli curente, atunci acest mod e identic cu “-I”
  - **DELETE** (-D):

    Acest mod șterge o regulă din lista de reguli din firewall
  - **LIST** (-L):

    Acest mod afișează pe ecran toate regulile active din firewall

Chain-uri (lanțurile de direcție)

- În stabilirea aplicării regulilor de firewall, există 3 mari direcții de filtrare:
  - Chain **INPUT**:

    Validează toate pachetele care **provin de oriunde** (din interior/exterior) și care **au destinație finală sistemul local** pe care rulează firewall-ul
  - Chain **FORWARD**:

    Validează toate pachetele care **provin de oriunde** (din interior/exterior) dar **nu se opresc în sistemul local** ci doar **trec prin sistemul local**, având ca **destinație o altă locație** (interior/exterior)
  - Chain **OUTPUT**:

    Validează toate pachetele care **originează (pornesc) în sistemul local** și au ca **destinație o altă locație** (interior/exterior)
  - Alte chain-uri (POSTROUTING/PREROUTING):

    Aceste chain-uri se folosesc în tabela de NAT pentru funcții de translație

Parametri (sursa și destinația)

- Parametri sunt opționali. Dacă nu se introduce un parametru, atunci automat nu se ține cont de el, și implicit este luat ca și global (all).

  (de exemplu dacă nu se specifcă sursa, atunci se considera ORICE sursă. Sau dacă nu se specifică destinația, atunci se consideră ORICE destinație.)

- Cu cât se introduc mai mulți parametri, cu atât regula de firewall devine mai explicită și are efect tot mai restrâns cu aplicare tot mai exactă.

  (deoarece regula trebuie să îndeplinească și criteriul A și criteriul B și criteriul C, toate în același timp)

- Clasificarea parametrilor principali:
  - **SOURCE** (-s):

    Definește sursa de unde provine pachetul. Poate fi o adresă IP sau o clasă de adrese IP notată prin adresa de rețea cu prefixul rețelei.
  - **DESTINATION** (-d):

    Definește destinația către care trebuie să ajungă pachetul. Poate fi o adresă IP sau o clasă de adrese IP notată prin adresa de rețea cu prefixul rețelei.

Parametri (protocol și port)

- Parametri sunt opționali. Dacă nu se introduce un parametru, atunci automat nu se ține cont de el, și implicit este luat ca și global (all).

  (de exemplu dacă nu se specifcă protocolul, atunci se considera ORICE protocol. Sau dacă nu se specifică portul, atunci se consideră TOATE porturile sau ORICE port.)

- Cu cât se introduc mai mulți parametri, cu atât regula de firewall devine mai explicită și are efect tot mai restrâns cu aplicare tot mai exactă.

- Pentru a folosi parametrul de PORT **trebuie neapărat** să specificați și PROTOCOLUL. Nu se poate declara portul dacă nu specificați și protocolul !

- Clasificarea parametrilor secundari:

  - **PROTOCOL** (-p):

    Definește protocolul de Layer #4 folosit: TCP / UDP sau/și ICMP

  - **DESTINATION PORT** (--dport):

    Definește portul de destinație, sau un interval de porturi de destinație

  - **SOURCE PORT** (--sport): Definește portul sursă

Acțiune finală asupra regulii

- Partea de acțiune reprezintă efectiv aplicarea regulii de firewall
- Aplicarea poate fi de tipul ACCEPTARE sau REFUZARE
- Acceptarea se face, de obicei, în caz că politica principală este de Respingere, caz în care regulile de ACCEPT devin Excepții de la filtrare
- Refuzarea se face, de obicei, în caz că politica principală este de Acceptare, caz în care regulile de DROP/REJECT devin Filtrări propriu-zise
- Clasificarea acțiunilor finale:
  - Jump to: **ACCEPT** (-j ACCEPT):

    Acceptă traficul care îndeplinește condițiile regulii introduse
  - Jump to: **REJECT** (-j REJECT):

    Respinge traficul care îndeplinește condițiile regulii introduse

    Respingerea se face trimițând înapoi un mesaj/cod de eroare
  - Jump to: **DROP** (-j DROP):

    Respinge traficul care îndeplinește condițiile regulii introduse

    Respingerea se face pur și simplu fără notificare, netrimițând înapoi niciun mesaj

Format

- Exemplu generic:

  iptables -t TABEL -? LANȚ -s IP -d IP -p PROTO --dport PORT -j ACȚIUNE

  unde,

  -t TABEL – tabelul folosit

  -? LANȚ – acțiunea în lanț

  -s – sursa

  -d – destinația

  -p – protocolul

  --dport – portul destinație

  -j – acțiunea de îndeplinit

Exemple

- Filtrați accesul de Web din clădirea B, care are clasa de IP-uri 192.168.0.0/25, către oriunde:

  iptables -t filter -I FORWARD -s 192.168.0.0/25 -p tcp --dport 80 -j DROP

- Filtrați accesul SSH de oriunde din lume către sistemul local:

  iptables -t filter -I INPUT -p tcp --dport 22 -j DROP

- Blocați tot traficul de DNS din sistemul local înspre o clasă de IP-uri:

  iptables -t filter -I OUTPUT -d 172.16.0.0/12 -p udp --dport 53 -j DROP

- Permiteți doar la o adresă dintr-o clasă să trimită e-mail către exterior, în rest blocați toate celelalte adrese pentru a trimite e-mail către exterior:

  iptables -t filter -I FORWARD -s 192.168.0.1 -p tcp --dport 25 -j ACCEPT

  iptables -t filter -A FORWARD -s 192.168.0.0/24 -p tcp --dport 25 -j DROP

Exemple

- Filtrați accesul de Web de la un calculator la serviciul web al sistemului local:

  iptables -t filter -I INPUT -s 192.168.1.2 -p tcp --dport 80 -j DROP

- Acceptați doar trafic Web de la o clasă de adrese IP către exterior, în rest blocați tot accesul la Internet:

  iptables -t filter -I FORWARD -s 192.168.0.0/24 -p tcp --dport 80 -j ACCEPT

  iptables -t filter -A FORWARD -s 192.168.0.0/24 -j DROP

- Blocați tot traficul de trimitere de e-mail, de oriunde, către oriunde:

  iptables -t filter -I FORWARD -p tcp --dport 25 -j DROP

- Blocați tot accesul la Internet, pe toate protocoalele și toate porturile, de la o clasă de adrese IP:

  iptables -t filter -I FORWARD -s 192.168.0.0/24 -j DROP