Firewall i IPTABLES v1.0

Tehnički fakultet "Mihajlo Pupin" – Zrenjanin
Zrenjanin, oktobar 2004.

SADRŽAJ

IPTABLES

Firewall koristi pravila za filtriranje konekcija i paketa u svakom lancu. Svaka linija koja se unese u lanac je pravilo. To pravilo koristi kernel sistema da bi znao šta treba da radi sa odgovarajućim paketom. Pravila se pišu na sledeći način:

iptables [-t table] command [match] [target/jump]

- [table] se mora navesti sa imenom tabele, kada se želi koristiti određena tabela. Ako se ova opcija izostavi podrazumevana tabela je filter tabela.
- command govori da li pravilo treba da se doda ili obriše.
- match govori ernelu koji se paketi proveravaju. To se radi upisom IP adrese sa koje dolazi paket ili interfejsa itd.
- [target/jump] govori kernelu šta treba da se uradi sa paketom, tj. da li se paket odbacuje, blokira ili propušta. Takođe se može poslati i odgovarajuća poruka.

TABELE (TABLES)

Opcija -t određuje koja se tabela koristi Podrayumevana tabela je filter. Postoje tri tabele: NAT, MANGLE I FILTER

NAT TABELA

NAT tabela se koristi uglavnom za Network Address Translation, tj. za translaciju polja sa adresom izvorišta ili polja sa adresom odredišta paketa. Paketi u nizu (stream) prolaze tabelu samo jedan put. Samo prvi paket prolazi kroz tabelu, a ostali se automatski maskiraju ako je to potrebno. Ova tabela ima tri ugrađena lanca (chains). PREROUTING lanac se koristi za pakete koji ulaze u firewall, OUTPUT lanac za lokalno generisane pakete, POSTROUTING lanac za pakete koji izlaze iz firewall-a.

Opcije koje se dostupne sa ovom tabelom su:

- DNAT
- SNAT
- MASQUERADE

DNAT (Destination Network Address Translation) se koristi u slu čaju kada postoji IP adresa za koju je potrebno preusmeriti saobaraćaj na drugi host, tj. kada se želi promeniti adresa odredišta u paketu i izvršiti njegovo prerutiranje na drugi host.

SNAT (Source Network Address Translation) se koristi za izmenu izvori šne adrese paketa. Time se postiže skrivanje lokalne mreže i DMZ (demilitarizovana zona). Kao primer za ovo se može navesti slučaj u kome su u LAN mreži dodeljene privatne IP adrese (npr. 192.168.x.x). U tom slučaju se saobraćaj sa spoljne mreže ne bi mogao odvijati ka računarima u LAN mreži bez upotrebe SNAP opcije.

MASQUERADE se koristi na isti način kao SNAT samo što vrši proveru IP adrese koja se koristi. Zato je podesnija za primenu u okruženju sa dinamički dodeljenim adresama (PPP; SLIP i DHCP).

MANGLE TABELA

Ova tabela se koristi za mangling paketa. Paketi se mogu menjati izmenom TTL, TOS ili MARK polja. Tabela se sastoji od dva ugrađena lanca. PREROUTING lanac se koristi za pakete koji su ušli u firewall pre rutiranja, a OUTPUT lanac za lokolno generisane pakete pre rutiranja. Mangle tabela se ne može koristiti za Network Address Translation ili Masquerading. Takođe se ne preporučuje upotreba ove tabele za filtriranje:

Opcije koje se dostupne sa ovom tabelom su:

- TOS
- TTL
- MARK

TOS se koristiza izmenu Type of Service polja u paketu, TTL se koristiza izmenu Time To Live polja u paketu, a MARK se koristi za postavljanje specijalne mark vrednosti za iproute2 i CBQ.

FILTER TABELA

Filter tabela se koristi za filtriranje paketa uz pomoć DROP, LOG, ACCEPT i REJECT opcija. Postoje tri ugrađena lanca. FORWARD se koristi za ne-lokalno generisane pakete koji nisu usmereni ka lokalnom hostu, tj. firewall-u. INPUT se koristi za sve pakete usmerene na lokalni host, a OUTPUT se koriti za sve lokalno generisane pakete.

TARGETS/JUMPS OPCIJE

Ove opcije govore koja akcija treba da se sprovede nad paketom koji odgovara pravilu. Dve osnovne TARGET opcije su ACCEPT i DROP. JUMP opcija omogu ćava prelazak iz jednog lanca na neki drugi lanac. Povratak na prvobitni lanac se vrši kada se proveri zadnje pravilo iz drugog lanca.

ACCEPT TARGET

Opcija koja dozvoljava prolaz paketu. Opcija se koristi sa -j ACCEPT.

DROP TARGET

Opcija koja odbacuje primljeni paket koji zadovoljava pravilo.

REJECT TARGET

Opcija slična DROP opciji samo što pored blokiranja paketa šalje i poruku o grešci. Koristi se u INPUT, FORWARD i OUTPUT lancima.

Primer:

iptables -A FORWARD -p TCP -dport 22 -j REJECT -reject-with tcp-reset

Opcija REJECT može da vrati nekoliko porka o graškama: icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibited, icmp-host-prohibited, echo-reply i tcp-reset. Podrazumevana poruka je port-unreachable.

DNAT TARGET

Opcija DNAT se okristi za Destination Network Address Translation, tj. za promenu odredišne IP adrese paketa koji zadovoljava pravilo. Ovo se može koristi u slučaju kada se Web server nalazi skriven u unutrašnjosti LAN mreže, iza firewall-a. Firewall može pomoću ove opcije preusmeriti sve zahteve upućene na http port 80, na taj server. Ova opcija se može koristiti samo u PREROUTING i OUTPUT lancima

Primer:
iptables -t nat -A PREROUTING -p tcp -d 15.45.23.67 --dport 80 -j DNAT -to-destination 192.168.1.1-192.168.1.10

Navedeni primer šalje sve pakete upućene na 15.45.23.67 i port 80 na računare sa IP adresama u opsegu od 192.168.1.1 - 192.168.1.10

Pored opsega IP adresa mogu se navesti i odredišni portovi, npr.
-to-destination 192.168.1.1:80 ili
-to-destination 192.168.1.1:80-100

Kada se navodi port potrebno je da su odabrani TCP ili UDP protokoli u -protocol opciji

MASQUERADE TARGET

MASQUERADE je slična SNAT opciji ali ne zahteva -to-source parametar, tj. unos izvorišne IP adrese. Razlog za ovo je što se MASQUERADE okristi kod dial-up ili DHCP konekcija, tj. kada postoje dinamične IP adrese.

Kada se koristi ova opcija to znači da se IP adresa specifičnog mrežnog interfejsa koristi umesto adrese navedene u -to-source parametru. Moguće je koristiti MASQUERADE i u kombinaciji sa statičkim adresama. Ova opcija je validna samo u POSTROUTING lancu NAT tabele.

Primer:
iptables -t nat -A POSTROUTING -p TCP -j MASQUERADE -to-ports 1024-31000

-to-ports opcija se koristi za navođenje porta na koji se paketi koji će biti maskirani usmeravaju

Može se navesti jedan (-to-ports 1025) ili opseg portva (-to-ports 1024-3000)

-to-ports opcija je validna samo sa TCP ili UDP protokolom navedenim sa -protocol opcijom.

REDIRECT TARGET

REDIRECT se koristi za preusmeravanje paketa na drugi host. Npr. mogu se preumeriti svi paketi upućeni na port 80 (http) na port 8080 (http proxy). REDIRECT je jedino validno sa PREROUTING i OUTPUT lancima nat tabele.

Primer:
iptables -t nat -A PREROUTING -p tcp -dport 80 -j REDIRECT -to-ports 8080

-to-ports određuje odredišni port
-to-ports 8080-8090 određuje više odredišnih portova

Opcija je moguća samo sa TCP ili UDP protokolima u –protocol parametru

SNAT TARGET

SNAT se koristi za Source Network Address Translation, tj. za promenu izvorišne IP adrese u zaglavlju paketa. Ovo se koristi kada više računara koristi istu konekciju ka Internetu. Računarima su dodeljene privatne IP adrese koj nisu vidljive sa Interneta. Da bi se omogućila njihova komunikacija sa Internetom potrebno je da im se dodeli javna IP adresa računara koji je direktno povezan na Internet. SNAT vrši translaciju adresa, i omogućava da računari iz lokalnog LAN dobiju javnu IP adresu hosta na kome se nalazi firewall. SNAT se koristi samo sa POSTROUTING lance.

Primer:
iptables -t nat -A POSTROUTING -o eth0 -j SNAT
-to-source 194.236.50.155-194.236.50.160:1024-32000

-to-source se koristi da označi izvorište čiji se paketi koriste
opseg IP adresa se navodi sa 194.236.50.155-194.236.50.160

Opseg portova se navodi sa :1024-32000

LOG TARGET

Opcija se koristi za logovanje eventualnih pokušaja napada na sistem ili debagovanje i otkrivanje grešaka.

Primer:
iptables -A FORWARD -p tcp -j LOG -log-level debug

Opcija govori koji log level da se koristi.

Primer:
iptables -A INPUT -p tcp -j LOG -log-prefix "INPUT packets"

Opcija kojom se podešava prefiks svih poruka koje se loguju.

iptables -A INPUT -p tcp -j LOG -log-tcp-sequence

Opcija kojom se loguje TCP Sequence numbers

iptables -A FORWARD -p tcp -j LOG -log-tcp-options

Opcija kojom se loguju različiti podaci iz TCP zaglavlja

iptables -A FORWARD -p tcp -j LOG -log-ip-options

Opcija kojom se loguju različiti podaci iz IP zaglavlja

KOMANDE (COMMANDS)

Komande govore iptables softveru šta da uradi sa ostatkom komandne linije. Ta linoja se može dodati ili obrisati

-A, -append

Komanda koja dodaje pravilo na kraju lanca
iptables -A INPUT ...

-D, -delete

Komanda koja briše pravilo u lancu
Pravilo se može brisati na dva načina. Prvi je navođenjem pravila koje se želi obrisati u potpunosti ali sa komandom delete. Na primer, postojeće pravilo

iptables -A INPUT -dport 80 -j DROP

Briše se komandom

iptables -D INPUT -dport 80 -j DROP

Drugi način brisanja je navođenje rednog broja pravila u lancu. Pravila u lancu su poređana po rednim brojevima od vrha na dole i prvo pravilo ima redni broj jedan.

iptables -D INPUT 1

-R, -replace

Komanda zamenjuje pravilo novim
iptables -R INPUT 1 -s 192.168.0.1 -j DROP

-I, -insert

Komanda koja unosi pravilo u određeni deo lanca
iptables -I INPUT 1 -dport 80 -j ACCEPT

Pravilo se dodaje u lanac sa određenim rednim brojem koji je naveden posle naredbe –I INPUT

-L, -list

Komanda lista pravila u naznačenom lancu
iptables -L INPUT

U prikazanom primeru listaju se pravila u INPUT lancu. Ako se ne navede naziv lanca prikazuju se svi lanci u tabeli. Često se koristi sa –n i -v komandama.

-F, -flush

Komanda briše sva pravila u lancu
iptables -F INPUT

U prikazanom primeru brišu se pravila u INPUT lancu. Ako se ne navede naziv lanca, brišu se svi lanci u tabeli. Često se koristi sa –n i -v komandama.

-Z, -zero

Komanda resetuje sve brojače u naznačenom lancu ili svim lancima.
iptables -Z INPUT

Ako se koristi -v komanda sa komandom -L mogu se videti kaunteri paketa na početku svakog polja.

-N, -new-chain

Komadna kreira novi lanac sa naynačenim imenom
iptables -N allowed

-X, -delete-chain

Komadna briše kreirani lanac sa naznačenim imenom

iptables -X allowed

-E, -rename-chain

Komanda menja prvo ime lanca drugim imenom
iptables -E allowed disallowed

OPCIJE (OPTIONS)

-v, -verbose

Komanda daje verbose output i uglavnom se koristi sa 'list komandom. Koristi se sa i sa -append, -insert, -delete i -replace komandama.

Upotreba sa -list comandom prikazuje i brojač paketa za svako pravilo. Brojači koriste K
(x1000), M (x1,000,000) i G (x1,000,000,000) množioce.

-x, -exact

Komadna daje širi numerički prikaz bez K, M ili G množilaca. Umesto toga daje se tačan prikaz broja paketa za dato pravilo. Koristi se sa –list komandom

-n, -numeric

Komanda daje numeričke vrednosti kao izlaz. IP adrese i brojevi portova se prikazuju numerički a ne kao imena hostova i servisa. Koristi se sa –list komandom.

-line-numbers

Koristi se za prikaz brojeva pravila. Koristi se sa –list komandom.

MATCHES

Su vrste opcija koje se uglavnom odnose na proveru paketa na osnovu protokola. Postoje pet grupa ovih opcija. To su opšte, TCP, UDP, ICMP i specijalne opcije.

OPŠTE MATCHES OPCIJE

Opcije koji se koriste bez obzira na protokol.

-p, -protocol

iptables -A INPUT -p tcp

Ova se komanda koristi za proveru određenog protokola TCP, UDP ili ICMP. Znak ! se koristi ako želimo da navedemo koji se samo protokol ne proverava. Npr. -protocol ! znači da se proveravaju ICMP i UDP paketi.

-s, -src, -source

iptables -A INPUT -s 192.168.1.1

Komanda se koristi za proveru paketa koji dolaze sa navedenom izvorišnom IP adresom. Može se navesti samo IP adresa kao u primeru bez ili sa mrežnom maskom (192.168.0.0/255.255.255.0) ili sa mrežnim prefiksom (192.168.0.0/24). Ako se

navede -source ! 192.168.0.0/24 proveravaju se samo paketi koji ne dolaze sa navedene adrese.

-d, -dst, -destination

iptables -A INPUT -d 192.168.1.1

Komanda se koristi za proveru paketa koji dolaze sa navedenom odredišnom IP adresom. Mrežna maska ili mrežni prefiks se takođe mogu navesti kao u prethodnom slučaju. Ako se navede -destination ! 192.168.0.1 proveravaju se samo paketi koji ne odlaze na navedeno odredište.

-i, -in-interface

iptables -A INPUT -i eth0

Komanda se koristi za proveru paketa koji dolaze sa naznačenog interfejsa. Upotreba komande je dozvoljena u INPUT, FORWARD i PREROUTING lancima. Ako se navede -i ! eth0, proveravaju se svi dolazeći paketi sa svih interfejsa osim sa eth0.

-o, -out-interface

iptables -A FORWARD -o eth0

Komadna se koristi za proveru paketa koji odlaze preko odredđenog interfejsa. Koristi se samo sa OUTPUT, FORWARD i POSTROUTING lancima. Može se koristiti i znak za inverziju - !, kao u slučaju -in-interface komande.

TCP MATCHES OPCIJE

Opcije koje se koriste za pakete zasnovane ne TCP protokolu. Koriste se u kombinaciji sa -protocol TCP komandom

-sport, -source-port

iptables -A INPUT -p tcp -sport 22

Komada proverava TCP pakete koji dolaze sa izvorišnog porta koji je naveden. Ako se navede -source-port 22:80 tada se proveravaju paketi koji dolaze sa opsega portova od 22 do 80, a ako se izostavi prvi port, npr. -source-port :80, podrazumeva se da je prvi port 0 a zadnji 80. Ako se izostavi zadnji port, npr. -source-port 22:, zadnji port je 65535. Ako se navede -source-port 80:22, to se prihvata kao i -source-port 22:80, a ako se -source-port ! 22, tada se proveravaju paketi koji dolaze sa svih portova osim porta 22. Moguće je navesti i -source-port ! 22:80.

-dport, -destination-port

iptables -A INPUT -p tcp -dport 22

Komanda proverava sve TCP pakete koji su upućeni na naznačeni port. Sintaksa je ista kao i kod -source-port komande.

-tcp-flags

iptables -p tcp -tcp-flags SYN,ACK,FIN SYN

Komanda se koristi za proveru TCP flagova u paketu. Pravila prepoznaju SYN, ACK, FIN, RST, URG, PSH flagove, ali i reči ALL i NONE. -tcp-flags ALL proverava pakete sa bilo kojim flagom, a NONE nijedan paket. Može se koristiti i inverzni ! znak.

-tcp-option

iptables -p tcp -tcp-option 16

Komada se koriti za proveru TCP paketa na osnovu navedene TCP opcije.

UDP MATCHES OPCIJE

Opcije koje se koriste za pakete zasnovane ne UDP protokolu. Koriste se u kombinaciji sa -protocol UDP komandom

-sport, -source-port

iptables -A INPUT -p udp -sport 53

Komanda se koristi na isti način kao i ista komanda za TCP protokol.

-dport, -destination-port

iptables -A INPUT -p udp -dport 53

ICMP MATCHES OPCIJE

Opcije koje se koriste za pakete zasnovane na ICMP protokolu. Ovaj protokol se uglavnom koristi za poruke o greškama i kontrolu veze. Koriste se u kombinaciji sa -protocol ICMP komandom

Komanda se koristi na isti način kao i ista komanda za TCP protokol.

-icmp-type

iptables -A INPUT -p icmp -icmp-type 8

Komadna se koristi da naznači pakete sa određenim ICMP type vrednostima. ICMP type vrednosti mogu se navesti numeričkim vrednostima ili imenima. Numeričke vrednosti su navedene u RFC 792. A ICMP imena se dobijaju sa iptables -protocol icmp –help. Ako se navede -icmp-type ! 8 proveravaju se svi paketi osim onih koji imaju navedeni tip.

PRIMERI

1. Zadatak – Obrisati sva pravila u Firewall-u.

```
/sbin/iptables -F
```

2. Zadatak –

```
# Telnet - zastita
/sbin/iptables -A INPUT -p tcp -s 212.200.54.130/32 --dport 23 -j ACCEPT
/sbin/iptables -A INPUT -p tcp -s 192.168.0.0/16 --dport 23 -j ACCEPT
/sbin/iptables -A INPUT -p tcp -s 0.0.0.0/0 --dport 23 -j REJECT

# NAT za unutrasnju mrezu
/sbin/iptables -F -t nat

/sbin/iptables -A POSTROUTING -t nat -s 192.168.1.0/24 -o eth0 -j SNAT --to-source
192.168.0.2
/sbin/iptables -A POSTROUTING -t nat -s 192.168.2.0/24 -o eth0 -j SNAT --to-source
192.168.0.2
/sbin/iptables -A POSTROUTING -t nat -s 192.168.3.0/24 -o eth0 -j SNAT --to-source
192.168.0.2
/sbin/iptables -A POSTROUTING -t nat -s 192.168.4.0/24 -o eth0 -j SNAT --to-source
192.168.0.2

# Redirekcija iz unutrasnje mreze
/sbin/iptables -A PREROUTING -t nat -p tcp -d 212.200.54.197 -j DNAT --to-
destination 192.168.0.2
```