Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

Zaštita računarskih sistema i mreža

- Peta laboratorijska vežba - Prilog -

IPTABLES *- kratko uputstvo sa primerima.*

`iptables` je komanda kojom se konfiguriše filtriranje paketa na Linux sistemima sa kernelima od verzije 2.4.x.

Za pakete koji ulaze u sistem, izlaze iz njega ili se prosleđuju (rutiraju) iptables traži pravilo koje bi se primenilo na iste. Ako nema pravila, primeniće se *default* akcija.

`iptables` koristi tri različita "lanca" (eng. *chain*) za propuštanje ili blokiranje paketa: **input**, **output** i **forward:**

- **Input** – ovaj lanac se primenjuje za kontrolu paketa koji ulaze u sistem.
- **Output** – ovaj lanac se primenjuje za kontrolu paketa koji izlaze iz sistema.
- **Forward** – ovaj lanac se primenjuje za kontrolu paketa koji prolaze kroz sistem kada je na njemu konfigurisano rutiranje ili NAT.

Default akcija za sve lance je da se propuštaju paketi (*accept rule*) čime se primenjuje polisa "zabranjeno je samo ono što je eksplicitno zabranjeno, a sve ostalo je dozvoljeno". Ako se želi uspostavljanje polise "dozvoljeno je samo ono što je eksplicitno dozvoljeno, a sve ostalo je zabranjeno" polisa može da se promeni sa:

```
iptables --policy INPUT DROP
iptables --policy OUTPUT DROP
iptables --policy FORWARD DROP
```

Prikazivanje pravila

Detaljan prikaz svih aktivnih pravila**:**

```
# iptables -n -L -v
```

…sa brojevima redova:

```
# iptables -n -L -v --line-numbers
```

Izlistavanje samo INPUT/OUTPUT lanaca:

```
# iptables -L INPUT -n -viptables -L OUTPUT -n -v --line-numbers
```

Izlistavanje pravila za specifičan lanac

```
# iptables -L INPUT
```

i sa specifikacijom pravila:

```
# iptables -S INPUT
```

i brojem paketa:

```
# iptables -L INPUT -v
```

Brisanje/Dodavanje pravila

Brisanje pravila po lancu i rednom broju:

```
# iptables -D INPUT 10
```

Brisanje pravila po specifikaciji

```
# iptables -D INPUT -m conntrack --ctstate INVALID -j DROP
```

Brisanje svih pravila, brisanje svih lanaca:

```
# iptables -P INPUT ACCEPT
# iptables -P FORWARD ACCEPT
# iptables -P OUTPUT ACCEPT
# iptables -t nat -F
# iptables -t mangle -F
# iptables -F
# iptables -X
```

Brisanje svih lanaca

```
# iptables -F
```

Brisanje pojedinačnog lanca

```
# iptables -F INPUT
```

Dodavanje pravila

```
# iptables -I INPUT 2 -s 202.54.1.2 -j DROP
```

Primeri pravila

Dozvoli *Loopback* veze

```
# iptables -A INPUT -i lo -j ACCEPTiptables -A OUTPUT -o lo -j ACCEPT
```

Dozvoli *Established* i *Related* dolazne veze

```
# iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Dozvoli *Established* izlazne veze

```
# iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Dozvoli prosleđivanje interni ka eksternim

```
# iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Odbaci nevažeće pakete

```
# iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

Blokiraj IP adresu

```
# iptables -A INPUT -s 192.168.1.10 -j DROP
```

Blokiraj IP adresu i odbaci

```
# iptables -A INPUT -s 192.168.1.10 -j REJECT
```

Blokiraj veze na mrežnom interfejsu

```
# iptables -A INPUT -i eth0 -s 192.168.1.10 -j DROP
```

Dozvoli sve dolazne SSH veze

```
# iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli dolazne SSH veze sa specifične IP adrese ili mreže

```
# iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 22 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli odlazni SSH

```
# iptables -A OUTPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A INPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli dolazni *Rsync* sa specifične IP adrese ili mreže

```
# iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 873 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p tcp --sport 873 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli dolazni HTTP

```
# iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli dolazni HTTPS

```
# iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli dolazni HTTP i HTTPS

```
# iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate
ESTABLISHED -j ACCEPT
```

Dozvoli MySQL sa specifične IP adrese ili mreže

```
# iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 3306 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p tcp --sport 3306 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli MySQL na specificiranom mrežnom interfejsu

```
# iptables -A INPUT -i eth1 -p tcp --dport 3306 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth1 -p tcp --sport 3306 -m conntrack --ctstate
ESTABLISHED -j ACCEPT
```

Dozvoli PostgreSQL sa specifične IP adrese ili mreže

```
# iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 5432 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p tcp --sport 5432 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli PostgreSQL na specificiranom mrežnom interfejsu

```
# iptables -A INPUT -i eth1 -p tcp --dport 5432 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth1 -p tcp --sport 5432 -m conntrack --ctstate
ESTABLISHED -j ACCEPT
```

Blokiraj odlazni SMTP

```
# iptables -A OUTPUT -p tcp --dport 25 -j REJECT
```

Dozvoli sav dolazni SMTP

```
# iptables -A INPUT -p tcp --dport 25 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 25 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli sav dolazni IMAP

```
# iptables -A INPUT -p tcp --dport 143 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 143 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli sav dolazni IMAPS

```
# iptables -A INPUT -p tcp --dport 993 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 993 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli sav dolazni POP3

```
# iptables -A INPUT -p tcp --dport 110 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 110 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Dozvoli sav dolazni POP3S

```
# iptables -A INPUT -p tcp --dport 995 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
# iptables -A OUTPUT -p tcp --sport 995 -m conntrack --ctstate ESTABLISHED -j
ACCEPT
```

Odbaci privatne adrese na internet interfejsu

```
# iptables -A INPUT -i eth1 -s 192.168.1.0/24 -j DROP
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

Odbaci sve odlazne pakete ka Facebook mrežama
preuzmi Facebook autonomni sistem:

```
# whois -h v4.whois.cymru.com " -v $(host facebook.com | grep "has address" |
cut -d " " -f4)" | tail -n1 | awk '{print $1}'
```

Odbaci:

```
# for i in $(whois -h whois.radb.net -- '-i origin AS1273' | grep "^route:" |
cut -d ":" -f2 | sed -e 's/^[ \t]*//' | sort -n -t . -k 1,1 -k 2,2 -k 3,3 -k 4,4
| cut -d ":" -f2 | sed 's/$/;/') ; do  iptables -A OUTPUT -s "$i" -j REJECTdone
```

Loguj i odbaci pakete

```
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix "IP_SPOOF A: "
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

Po defaultu se loguje u `/var/log/messages` fajl:

```
# tail -f /var/log/messagesgrep --color 'IP SPOOF' /var/log/messages
```

Odbaci ili prihvati pakete sa neke MAC adrese

```
# iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
# iptables -A INPUT -p tcp --destination-port 22 -m mac --mac-source
00:0F:EA:91:04:07 -j ACCEPT
```

Odbaci ili prihvati ICMP *Ping Request*

```
# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
# iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP
```

Zaštita od skeniranja portova

```
# iptables -N port-scanningiptables -A port-scanning -p tcp --tcp-flags
SYN,ACK,FIN,RST RST -m limit --limit 1/s --limit-burst 2 -j RETURNiptables -A
port-scanning -j DROP
```

SSH *brute-force* zaštita

```
# iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --
setiptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --
update --seconds 60 --hitcount 10 -j DROP
```

Syn-flood zaštita

```
# iptables -N syn_floodiptables -A INPUT -p tcp --syn -j syn_floodiptables -A
syn_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
# iptables -A syn_flood -j DROPiptables -A INPUT -p icmp -m limit --limit  1/s -
-limit-burst 1 -j ACCEPT
# iptables -A INPUT -p icmp -m limit --limit 1/s --limit-burst 1 -j LOG --log-
prefix PING-DROP:
# iptables -A INPUT -p icmp -j DROPiptables -A OUTPUT -p icmp -j ACCEPT
```

Sprečavanje SYN *Flooding*-a pomoću SYNPROXY

```
# iptables -t raw -A PREROUTING -p tcp -m tcp --syn -j CT --notrack
# iptables -A INPUT -p tcp -m tcp -m conntrack --ctstate INVALID,UNTRACKED -j
SYNPROXY --sack-perm --timestamp --wscale 7 --mss 1460
# iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

Odbaci nove TCP pakete koji nisu SYN

```
# iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

ili

```
# iptables -t mangle -A PREROUTING -p tcp ! --syn -m conntrack --ctstate NEW -j
DROP
```

Odbaci XMAS pakete

```
# iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
```

Odbaci sve NULL pakete

```
# iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

Blokiraj neuobičajene MSS vrednosti

```
# iptables -t mangle -A PREROUTING -p tcp -m conntrack --ctstate NEW -m tcpmss !
--mss 536:65535 -j DROP
```

Blokiraj pakete sa besmislenim TCP flegovima

```
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG
NONE -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,ACK FIN -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,URG URG -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,FIN FIN -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,PSH PSH -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL ALL -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL NONE -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j
DROP
# iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j
DROP
```

Blokiraj pakete sa privatnih mreža (*Spoofing*)

```
_subnets=("224.0.0.0/3" "169.254.0.0/16" "172.16.0.0/12" "192.0.2.0/24"
"192.168.0.0/16" "10.0.0.0/8" "0.0.0.0/8" "240.0.0.0/5")for _sub in
"${_subnets[@]}" ; do  iptables -t mangle -A PREROUTING -s "$_sub" -j
DROPdoneiptables -t mangle -A PREROUTING -s 127.0.0.0/8 ! -i lo -j DROP
```

Snimanje pravila na Linuxima izvedenim od Debiana (npr. Ubuntu)

```
# netfilter-persistent save
```