

GNU/Linuksowy router domowy



Daniel Kubiak
sor@czlug.icis.pcz.pl

Plan prezentacji

- Podstawowa wiedza...
- iptables - wprowadzenie
- Podstawy konfiguracji
- Prosty firewall – praktyczne podejście
- Bardziej zaawansowany firewall
- NAT i PAT
- Bo mi torrenty nie działają ;-)
- Piszemy skrypt
- Q&A

Podstawowa wiedza...

- Co to jest sieć komputerowa?
- Co to jest adres IP?
- Co to jest maska sieci?
- Co to są porty?
- Co to u licha jest ten firewall?
- Co to jest routing?
- Czy sieć też ma warstwy?
- Po co nam protokoły (IP, TCP, UDP, ICMP)

iptables - wprowadzenie

- Filtr pakietów działający w warstwie TCP/IP
- Pierwsza wersja napisana w 1991
- Autorem jest Rusty Russell
- Od kernela 2.4.x (moduł ip_tables)
- Najnowsza wersja 1.4.3.2 (06042009)
- <http://netfilter.org/projects/iptables/index.html>

- Łańcuchy iptables
- Reguły iptables
- Polityki iptables

Podstawy konfiguracji

- Łańcuchy predefiniowane
 - ★ INPUT (-t filer)
 - ★ OUTPUT (-t filter)
 - ★ FORWARD (-t filter)
 - ★ PREROUTING (-t nat)
 - ★ POSTROUTING (-t nat)
- Łańcuchy definiowane przez użytkownika

Podstawy konfiguracji cd.

- Prosta regułka:

```
iptables -A INPUT -i eth0 -s 0/0 -d  
192.168.0.1 -p tcp --dport 80 -j ACCEPT
```

- Przełączniki:

- ★ -s – adres źródłowy
- ★ -d – adres docelowy
- ★ -i – interfejs wejściowy
- ★ -o – interfejs wyjściowy
- ★ -j – akcja
- ★ -p – protokół

Podstawy konfiguracji cd.

- Przełączniki cd.:
 - ★ -A – dodawanie regułki
 - ★ -I – wstawianie regułki
 - ★ -D – usuwanie regułki
 - ★ -R – zmiana regułki
 - ★ -P – polityka domyślna
- Łańcuchy:
 - ★ -N – tworzenie nowego łańcucha
 - ★ -F – czyszczenie łańcucha
 - ★ -X – kasowanie łańcucha
 - ★ -L – przeglądanie regułek łańcucha

Prosty firewall – praktyczne podejście

- Podejście sadomasochisty:

```
iptables -P INPUT DROP
```

- Podejście praktyczne:

```
iptables -P INPUT DROP
```

```
iptables -A INPUT -p tcp --dport 80 -d  
192.168.0.1 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 25 -d  
192.168.0.1 -j ACCEPT
```

```
iptables -A INPUT -p udp --sport 53 -d  
192.168.0.1 -j ACCEPT
```

Zaawansowany firewall

- Rozszerzenia:

- ★ -m state

```
iptables -A INPUT -m state --state  
ESTABLISHED,RELATED -j ACCEPT
```

- ★ -m mac

```
iptables -t nat -A PREROUTING -s 192.168.0.2  
-m mac --mac-source 00:11:22:33:44:55 -j  
REDIRECT --to-port 82
```

- ★ -m set (+ ipset)

```
iptables -A FORWARD -m set --set my_macs -j  
ACCEPT
```

Zaawansowany firewall cd.

- Rozszerzenia cd.:

- ★ -m limit

- ```
iptables -A INPUT -p icmp -icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

- Cele regułek:

- ★ DROP

- ★ REJECT --reject-with tcp-reset

- ★ ACCEPT

- ★ RETURN

- ★ LOG (do sysloga)

- ★ ULOG (osobny demon)

- ★ Łańcuch użytkownika

# Zaawansowany firewall cd.

- Łańcuchy użytkownika (przykład)

```
iptables -N www
```

```
iptables -A www -p tcp -dport 80 -m state --
state NEW -j ACCEPT
```

```
iptables -A www -p tcp -dport 443 -m state --
state NEW -j ACCEPT
```

```
iptables -A www -j DROP
```

```
iptables -A INPUT -d 192.168.0.1 -j www
```

# NAT i PAT

```
iptables -t nat -A POSTROUTING -s
192.168.0.2 -o wlan0 -j SNAT -to 10.0.0.2
```

```
iptables -t nat -A POSTROUTING -s
192.168.0.0/24 -o wlan0 -j MASQUERADE
```

```
iptables -t nat -A POSTROUTING -s
192.168.0.0/24 -o wlan0 -j SNAT -to
10.0.0.2-10.0.0.10
```

Musimy jeszcze włączyć IP forwarding:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "net.ipv4.ip_forward=1" \
> /etc/sysctl.conf
```

# Port forwarding

- Przekierowanie portu routera na port komputera za NAT-em

```
iptables -t nat -A PREROUTING -p tcp -i
wlan0 -d 10.0.0.2 -dport 10101 -j DNAT --to
192.168.0.2:101
```

```
iptables -t nat -A PREROUTING -p udp -i
wlan0 -d 10.0.0.2 -dport 10101 -j DNAT --to
192.168.0.2:101
```

- Jeżeli mamy domyślną politykę **INPUT** i **FORWARD** ustawioną na **DROP** musimy przekierowane porty odblokować

# Piszemy skrypt

```
#!/bin/bash
ipt=/sbin/iptables

MYWANIP=10.0.0.2
MYLANIP=192.168.0.1
MYLAN=192.168.0.0/24

WANINT=wlan0
LANINT=eth0

$ipt -P INPUT DROP
$ipt -P FORWARD DROP
```

## Piszemy skrypt cd.

```
$ipt -t nat -A POSTROUTING -s $MYLAN -o $WANINT -j
SNAT -to $WANIP
```

```
$ipt -A FORWARD -d $MYLAN -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

```
$ipt -A FORWARD -s 192.168.0.2 -p tcp --dport !
135:139 -i $LANINT -j ACCEPT
```

```
$ipt -A FORWARD -s 192.168.0.2 -p udp --dport !
135:139 -i $LANINT -j ACCEPT
```

```
$ipt -A FORWARD -s 192.168.0.2 -p icmp --icmp-type
echo-request -i $LANINT -j ACCEPT
```

## Piszemy skrypt cd.

```
$ipt -A INPUT -d $LANIP -s $MYNET -i $LANINT -j
ACCEPT
```

```
$ipt -A INPUT -d $WANIP -i $WANINT -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

```
$ipt -A INPUT -d $WANIP -i $WANINT -p tcp -dport 22
-m state --state NEW -j ACCEPT
```

```
$ipt -A INPUT -d $WANIP -i $WANINT -p tcp -dport 25
-m state --state NEW -j ACCEPT
```

```
$ipt -A INPUT -d $WANIP -i $WANINT -p tcp -dport 80
-m state --state NEW -j ACCEPT
```

**Q&A**

**Q&A**

**Koniec**

**Dziękuję za uwagę!**