Przykłady składni polecenia iptables

Każda reguła inaczej wygląda podczas formułowania (wpisywania polecenia), a trochę inaczej wyświetlana jest działająca (za pomocą opcji –L lub –vL). Dlatego przykłady zawierają zarówno zrzut ekranu ze składnią, jak i wygląd działającej reguły (w ramce). Wielkie i małe litery są rozróżniane podczas wpisywania reguł.

1. Podstawowe operacje na łańcuchach

```
iptables –F INPUT    – wyczyszczenie łańcucha INPUT
iptables –L          – wyświetlenie zawartości łańcuchów domyślnej tablicy (filter)
iptables –L INPUT    – wyświetlenie zawartości łańcucha INPUT domyślnej tablicy
iptables –t nat -L   – wyświetlenie zawartości łańcuchów tablicy nat
iptables –v -L       – szczegółowe wyświetlenie zawartości łańcuchów tablicy (filter)
```

   Czasami zdarza się, że wyświetlanie reguł zatrzymuje się w pewnym momencie. Można je przerwać naciskając kombinację Ctrl+c. Dzieje się tak w sytuacji, w której reguła dotyczy adresów IP, które nie mogą zostać zamienione na nazwy FQDN (z różnych przyczyn). Aby uniknąć takiej sytuacji należy dodać do argumentu –L opcję –n. W skrócie można kilka opcji zapisać następująco:

```
iptables –nvL        – szczegółowe, numeryczne wyświetlenie zawartości łańcuchów tablicy domyślnej
```

2. Ustalanie domyślnej polityki łańcucha

```
iptables –P INPUT DROP
```

```
Chain INPUT (policy DROP)
target     prot opt source               destination
```

   Powyższe polecenie ustala politykę domyślną łańcucha INPUT na DROP, czyli odrzucanie. Jeżeli w łańcuchu nie będzie reguły jawnie wpuszczającej dane pakiety, zostaną one odrzucone.

3. Filtrowanie z uwzględnieniem interfejsu

```
iptables –A INPUT –i eth1 –j DROP
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
```

   Powyższa komenda powoduje odrzucanie wszystkich pakietów adresowanych do firewalla (łańcuch INPUT), które wchodzą przez interfejs eth1.
   Uwaga: typowe listowanie reguł typowo nie zawiera informacji o interfejsach, należy użyć opcji –v (patrz p. 0):

```
Chain INPUT (policy ACCEPT 146 packets, 10544 bytes)
pkts bytes target     prot opt in     out     source               destination
   0     0 DROP       all  --  eth1   any     anywhere             anywhere
```

4. Filtrowanie z uwzględnieniem źródłowego adresu IP

```
iptables –A INPUT –s 192.168.0.0/16 –j ACCEPT
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.0.0/16       0.0.0.0/0
```

Ta reguła powoduje akceptowanie wszystkich pakietów trafiających do firewalla z dowolnego adresu podsieci 192.168.x.x. Podobna reguła, ale działająca dla pakietów przechodzących przez firewall:

```
iptables –A FORWARD –s 192.168.0.0/16 –j ACCEPT
```

5. Filtrowanie z uwzględnieniem docelowego adresu IP

```
iptables –A FORWARD –d 192.168.0.0/16 –j ACCEPT
```

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            192.168.0.0/16
```

Ta reguła powoduje akceptowanie wszystkich pakietów przechodzących przez firewall, o ile adresem docelowym jest któryś z sieci 192.168.x.x.

6. Filtrowanie z uwzględnieniem typu protokołu i portu docelowego

```
iptables –A INPUT –p tcp --dport 22 –d 192.168.1.254/32 –j ACCEPT
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            192.168.1.254       tcp dpt:22
```

Ta reguła powoduje akceptowanie wszystkich pakietów trafiających do firewalla, o ile adres docelowy odpowiada firewallowi (192.168.1.254) i docelowy port to tcp/22 (ssh).

7. Translacja adresów NAT

```
iptables –t nat -A POSTROUTING –s 172.16.0.0/16 –j MASQUERADE
```

```
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  172.16.0.0/16        0.0.0.0/0
```

lub

```
iptables –t nat -A POSTROUTING –s 172.16.0.0/16 –j SNAT --to-source 10.1.1.2
```

```
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  172.16.0.0/16        0.0.0.0/0           to:10.1.1.2
```

Ta reguła powoduje translację adresów z podsieci 172.16.x.x na adres 10.1.1.2 (lub w pierwszym przypadku automatycznie na adres interfejsu prowadzącego do domyślnej bramy).

8. Translacja adresów PAT

```
iptables –t nat -A PREROUTING –d 192.168.1.254/32 –p tcp --dport 10022
-j REDIRECT --to-ports 22
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  0.0.0.0/0            192.168.1.254       tcp dpt:10022 redir
ports 22
```

lub

```
iptables –t nat -A PREROUTING –d 192.168.1.254/32 –p tcp --dport 10022 –j DNAT
--to-destination 127.0.0.1:22
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  0.0.0.0/0            192.168.1.254       tcp dpt:10022
to:127.0.0.1:22
```

Ta reguła powoduje przekierowanie wszystkich pakietów adresowanych do firewalla do portu tcp/10022 na port 22.

9. Filtrowanie statefull

```
iptables –A INPUT –m state --state ESTABLISHED,RELATED –i eth0 –d 192.168.1.254
–j ACCEPT
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            192.168.1.254       state
RELATED,ESTABLISHED
```

Ta reguła powoduje akceptowanie wszystkich pakietów trafiających do firewalla (192.168.1.254) przez interfejs eth0, jeżeli wcześniej połączenie było z niego inicjowane.