

Iptables – informacje ogólne

Położenie: (nie dotyczy)

© 3bird Projects 2011, <http://3bird.net>

Ogólnie

Logiczna kolejność wprowadzania regułek:

1. Najpierw wprowadzamy to, na co pozwalamy.
2. Na końcu należy zabronić wszystkiego innego.

Jeśli zastosujemy zasadę odwrotną, przetwarzanie wszystkich regułek zostanie zatrzymane na samym początku. Należy pamiętać, że „IP tables support” należy wkompilować do jądra na stałe (system nie potrafi łądować takiego modułu).

Nowe zasady

W nowych wersjach iptables zmienia się polityka obsługi regułek. Oto nowa procedura:

1. Wprowadzamy kolejno regułki w linii poleceń. Należy pamiętać, że zapisane zostaną tylko regułki iptables, inne muszą za każdym razem być wprowadzane inną metodą, na przykład: **echo 1 > /proc/sys/net/ipv4/ip_forward** (możemy dodać do */etc/conf.d/local.start*)
2. Opcje iptables zapisywane są w */etc/conf.d/iptables*
3. Zapisujemy regułki w pliku */var/lib/iptables/rules-save*: # **iptables-save && /etc/init.d/iptables save**
4. Regułki możemy także wczytać z dowolnego pliku: # **iptables-restore < plik.txt**
5. Uruchamiamy iptables: **/etc/init.d/iptables start**

Struktura tabel

Tabele: nat, mangle, filter.

Każda tabela składa się z łańcuchów (chain):

- **input** - przychodzące do tego komputera;
- **output** - wychodzące z tego komputera;
- **postrouting** - przekazywane do innego konkretnego komputera
- **prerouting** - nie wiadomo do jakiego komputera są przeznaczone (naszego czy w LAN),
- **forward** - przekazywane dalej.

Każdy łańcuch składa się z reguł (rules). Do reguł stosuje się targety (wydarzenia):

- **accept** – akceptacja;
- **drop** – zablokowanie pakietu bez powiadomienia nadawcy;
- **queue** -
- **return** -
- **reject** – zablokowanie ze zwróceniem komunikatu ICMP.

Porty

Numer portów można zastępować ich nazwami, np. port 80 można zastąpić nazwą „www”.

Zakresy portów oddzielamy dwukropkiem, np. 1000:1500.

Pakiety

Stany połączeń:

NEW - pakiet rozpoczynający połączenie;

RELATED – pakiety nie należące do sesji, ale związane z nią w jakiś sposób (np. błędy zwracane po ICMP); pakiet przypisywany, jeśli połączenie jest w trakcie negocjacji; moduł odpowiedzialny za ten stan to *ip_conntrack_ftp*; umożliwiamy wszystko, co dzieje się w ramach już istniejących powiązanych połączeń (na które już pozwoliliśmy);

ESTABLISHED - pakiet należy do nawiązanego już połączenia; umożliwiamy wszystko, co dzieje się w ramach już istniejących połączeń (na które już pozwoliliśmy);

INVALID - pakiet niepasujący do żadnego połączenia, niezwiązany z żadną zapamiętaną sesją.

Moduł odpowiedzialny za stany połączeń: *state*.

Jeśli nie działa forwarding FTP lub IRC, musimy uruchomić moduły:

- **modprobe ip_nat_ftp**
- **modprobe ip_nat_irc**

Polecenia

Wyświetla zawartość tabeli "nat":

```
# iptables -v --list --table nat
```

Na początku, na wszelki wypadek, czyścimy cały zestaw tablic:

```
# iptables -F
```

Domyślnie nie wpuszczamy nic:

```
# iptables -P INPUT DROP
```

```
# iptables -P FORWARD DROP
```

```
# iptables -P OUTPUT DROP
```

Kasowanie niestandardowych tablic:

```
# iptables -X
```

Zezwalamy na połączenia przychodzące do interfejsu lo (potrzebne np. do CUPS, lokalnego DNS, itp.) i wychodzące:

```
# iptables -A INPUT -i lo -j ACCEPT
```

```
# iptables -A OUTPUT -o lo -j ACCEPT
```

```
# iptables -A FORWARD -o lo -j ACCEPT
```

Zezwalamy na połączenia do serwera z sieci wewnętrznej LAN:

```
# iptables -A INPUT -i eth0 -s 192.168.0.0/24 -j ACCEPT
```

```
# iptables -A FORWARD -i eth0 -s 192.168.0.0/24 -j ACCEPT (jeśli jest to router)
```

Pozwalamy na wszelki ruch przychodzący od nawiązanych przez nas połączeń:

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

```
# iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT (jeśli jest to router)
```

-m state - uaktywnia moduł stanu pakietów;

--state rodzajSTANU - określenie rodzaju stanu pakietu;

Otwieramy porty dla poszczególnych programów (wykaz portów: */etc/services*); w poniższym przypadku, dla Jabbera:

```
# iptables -A INPUT -p tcp --dport 5222 -m state --state NEW -j ACCEPT
```

```
# iptables -A INPUT -p udp --dport 5222 -m state --state NEW -j ACCEPT
```

Otwarcie portów dla P2P:

```
# iptables -A INPUT -p tcp --dport 4242 -m state --state NEW -j ACCEPT
```

```
# iptables -A INPUT -p udp --dport 4242 -m state --state NEW -j ACCEPT
```

Udostępnienie serwera www (zawsząd):

```
# iptables -A INPUT -p tcp -d 0/0 --dport www -m state --state NEW -j ACCEPT
```

```
# iptables -A INPUT -p tcp -d 0/0 --dport https -m state --state NEW -j ACCEPT
```

Udostępnienie serwera ssh (zawsząd):

```
# iptables -A INPUT -p tcp -d 0/0 --dport ssh -m state --state NEW -j ACCEPT
```

Udostępnienie serwera ssh tylko dla określonego IP:

```
# iptables -A INPUT -p tcp -s 192.168.0.8/24 -d 0/0 --dport ssh -m state --state NEW -j ACCEPT
```

Udostępnienie serwera SMTP (zawsząd):

```
# iptables -A INPUT -p tcp -d 0/0 --dport smtp -m state --state NEW -j ACCEPT
```

Udostępnienie serwera POP3 znajdującego się w sieci wewnętrznej (za NAT-em):

```
# iptables -t nat -A PREROUTING -p tcp -d 83.123.123.1/32 --dport 110 -j DNAT --to-destination 192.168.0.3
```

Ustawiamy maskowanie (wszystkie pakiety pochodzące z LAN będą maskowane):

```
# iptables --table nat --append POSTROUTING -p all -s 192.168.0.0/255.255.255.0 -d 0/0 -o ppp0 -j MASQUERADE
```

Odrzucamy wszelkie inne pakiety przychodzące:

```
# iptables -A INPUT -m state --state NEW -j REJECT
```

Odrzucamy wszelkie połączenia z określonego IP:

```
# iptables -A INPUT -p tcp -s 192.168.0.9/24 -j DROP
```

Odrzucamy wszelkie połączenia z dziwnymi niekompletnymi pakietami (potrzebny eksperymentalny moduł *unclean*; nie zawsze działa poprawnie):

```
# iptables -A INPUT -j DROP -m unclean
```

Zezwalamy na wszelki ruch wychodzący:

```
# iptables -A OUTPUT -j ACCEPT
```

Usługi, które wypuszczamy z naszej sieci:

```
# TCP_OUT_ALLOW=80,8080,22,995
```

```
# UDP_OUT_ALLOW=123,53
```

```
# iptables -A OUTPUT -o ppp0 -p tcp -j ACCEPT -m state --state NEW -m multiport --destination-port $TCP_OUT_ALLOW
```

itd.

Inne

Zmienia zawartość reguły w tabeli "nat" i łańcuchu POSTROUTING:

```
# iptables --table nat --replace POSTROUTING 1 -o eth1 -s 192.168.0.0/24 -j MASQUERADE
```

Zezwalamy, aby serwer przepuszczał pakiety, które pochodzą z naszej sieci lokalnej lub są dla niej przeznaczone:

```
# iptables --table filter --append FORWARD -s 192.168.0.0/255.255.255.0 -d 0/0 -j ACCEPT
```

```
# iptables --table filter --append FORWARD -s 0/0 -d 192.168.0.0/255.255.255.0 -j ACCEPT
```

W logach pokazuje się informacja, że ktoś mnie pinguje:

```
# iptables -t filter -I INPUT -i eth0 -p icmp --icmp-type echo-request -j LOG --log-prefix 'Ktos mnie pinguje:'
```

```
# cat /var/log/kernel/current | grep pinguje | grep eth1
```

Umożliwienie pingowania:

```
# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

Umożliwiamy pingowanie (poprzez nasz router) z sieci wewnętrznej do zewnętrznej:

```
# iptables -A FORWARD -p icmp --icmp-type echo-request -j ACCEPT
```

Zabrania pingowania:

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

Możliwość tylko jednego pinga na 3 sekundy:

```
# iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 3/s -j ACCEPT
```

Zatrzymujemy na routerze podejrzane pakiety pochodzące z WAN (a mające adresy LAN) i odwrotnie:

```
# iptables -A FORWARD -s 83.123.123.0/24 -i ppp0 -j DROP
```

```
# iptables -A FORWARD -s ! 83.123.123.0/24 -i eth0 -j DROP
```

lub po prostu:

```
# echo 1 > /proc/sys/net/ipv4/conf/all/rp_filter
```

Ostatnia aktualizacja: 9 sierpień 2011.