Iptables – informacje ogólne

Położenie: (nie dotyczy)

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 ładować takiego modułu).

Uwaga: W przypadku systemu wirtualnego, firewall systemu macierzystego będzie blokował (nadpisywał) politykę firewalla systemu wirtualnego.

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. Regułki możemy wczytać z dowolnego pliku: # **iptables-restore < plik.txt**
3. Można także użyć skryptu do wprowadzenia reguł: # **.skrypty/./reguly-iptables**
4. Uruchamiamy iptables i aktywujemy reguły: # **/etc/init.d/iptables start**
5. Zapisujemy regułki w pliku */var/lib/iptables/rules-save*: # **iptables-save && /etc/init.d/iptables save**
6. Regułki możemy także zapisać w innym dowolnym pliku, np.: # **iptables-save > /etc/iptables.rules**

Struktura tabel

Wykaz istniejących tabel uzyskamy za pomocą polecenia:

cat /proc/net/ip_tables_names

Każda tabela składa się z łańcuchów (*chain*). I tak, dla tabeli filter (domyślnie stosowana, gdy nieokreślono nic innego):

- **input** - przychodzące i przeznaczone dla tego komputera;
- **output** - wychodzące z tego komputera;
- **forward** - przekazywane dalej;

Dla tabeli nat:

- **prerouting –** zmienia drogę pakietów wchodzących, gdy nie wiadomo do jakiego komputera są przeznaczone (naszego czy w LAN);
- **postrouting** – zmienia drogę pakietów wychodzących, przekazuje do innego konkretnego komputera;
- **output** – ustanawia drogę dla pakietów wychodzących lokalnie;

Dla tabeli mangle (czyli „magiel", do specjalnych modyfikacji drogi):

- **prerouting**;
- **postrouting**;
- **forward**;
- **input**;
- **output**;

Dla tabeli raw (czyli dla pakietów, których celem powinien być „niebyt”):

- **prerouting** – kieruje do „niebytu” pakiety przychodzące z jakiegokolwiek interfejsu;
- **output** – kieruje do „niebytu” pakiety generowane przez lokalne procesy;

Dla tabeli security (czyli dla *Mandatory Access Control* [MAC] używane wraz z *SELinux*):

- **input**;
- **output**;
- **forward**;

Do każdego łańcucha można stosować komendy:

- **-A**, **--append** – dodaje regułę na koniec wybranego łańcucha;
- **-I**, **--insert** – dodaje regułę na początek wybranego łańcucha (lub wkłada ją do wybranej pozycji, gdy jest ona określona numerem);
- **-R**, **--replace** – zamienia regułę w wybranym łańcuchu pod określoną pozycją;
- **-P, --policy** – ustawia domyślną politykę łańcucha dla wybranego celu;
- **-D**, **--delete** – usuwa regułę (jej nazwa lub numer) z wybranego łańcucha;

oraz parametry:

- **-p, --protocol nazwaProtokołu**;
- **-s, --source adresIP**;
- **-d, --destination adresIP**;
- **-i, --in-interface nazwaInterfejsu** – nazwa interfejsu, przez który pakiety mają być wpuszczane;
- **-o, --out-interface nazwaInterfejsu** – nazwa interfejsu, przez który pakiety mają być wysyłane;

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

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

Porty

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

Zakresy portów oddzielamy dwukropkiem, np. 1000:1500.

Możemy sprawdzić, jakie porty są otwarte:

\# **netstat -atnp | grep -w 21** (lub inne: 80, 22, itp.)

\# **netstat -tulpn** (pokazuje tylko połączenia serwerowe)

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 domyślnej tabeli „filter”:
iptables -L
Wyświetla zawartość tabeli "nat":
iptables -v -n --list --table nat

Na początku, na wszelki wypadek, czyścimy cały zestaw tablic:
iptables -F (--flush)
Kasowanie łańcuchów zdefiniowanych przez użytkownika (czyli innych niż wbudowane):
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 (ustawienia tylko na serwerze)

Zezwalamy na wszelki ruch wychodzący:
iptables -A OUTPUT -j ACCEPT

Zezwalamy na połączenia do serwera z sieci wewnętrznej LAN (ustawienia na serwerze):
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 (zewsząd):
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

Akceptujemy połączenia do portu FTP:
iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 21 -j ACCEPT
oraz pasywne połączenia:
iptables -A INPUT -p tcp -m tcp --dport 49152:65534 --syn -j ACCEPT

Akceptujemy połączenia do portu CUPS:

iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 631 -j ACCEPT
iptables -A INPUT -p udp -m state --state NEW -m udp --dport 631 -j ACCEPT

Udostępniany serwer skanera sieciowego SANE (port 6566) tylko dla danego IP:

iptables -A INPUT -p tcp -s 192.168.0.9/24 --dport saned -j ACCEPT

Jeśli chcemy po prostu korzystać ze skanera (bez udostępniania go innym), regułka będzie miała postać:

-A INPUT -p udp -m udp -s 192.168.0.17 -m mac --mac-source A4:EE:57:CC:3B:B7 --sport 3289 -m state --state NEW,ESTABLISHED -j ACCEPT

Generalnie, program *xsane* otwiera losowy port na laptopie, z którego wysyła zapytanie do skanera na port 3289 protokołem UDP. Skaner odpowiada z tego portu na losowy port laptopa. W regułce określony jest MAC i IP skanera.

Udostępnienie serwera ssh (zewsząd):

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 (zewsząd):

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

iptables -A INPUT -j DROP -m unclean

Odrzucamy wszelkie połączenia z określonego IP:

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

Odrzucamy wszelkie połączenia z karty sieciowej o określonym MAC:

iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP

Na końcu odrzucamy wszelkie inne pakiety przychodzące:

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

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

Problemy

Brak modułu „state”

Należy w jądrze uaktywnić:

Networking support / Networking options / Network packet filtering framework (Netfilter) / Core Netfilter Configuration / <> Netfilter Connection Tracking Support →*

<> „state” match support*

Brak tablicy NAT

Należy w jądrze uaktywnić:

Networking support / Networking options / Network packet filtering framework (Netfilter) / Core Netfilter Configuration →

<> IPv4 connection tracking support*

[*] IPv4 nf_tables support

<> IPv4 NAT (wszystkie opcje)*

<> IP tables support*

<> iptables NAT support (wszystkie opcje)*

Networking support / Networking options / Network packet filtering framework (Netfilter) / Core Netfilter Configuration / Netfilter nf_tables support →

<> Netfilter nf_tables masquerade support*

<> Netfilter nf_tables nat module*

A także:

USE=”netlink conntrack nftables” emerge iptables

Ostatnia aktualizacja: 18 sierpnia 2018.