Фильтр пакетов iptables

Администрирование сетевых подсистем

Мишина А. А.

20 октября 2024

Введение

- · Утилита для взаимодействия с Netfilter
- Позволяет определить, какие пакеты будут пропускаться, блокироваться, перенаправляться



Фильтр пакетов iptables

Фильтры пакетов нужны чтобы:

- Контролировать трафик
- Уведомление об отсылке пакетов

Историческая справка

- · 1994 Linux 1.1
- 1998 Linux 2.2
- · 1999 Linux 2.4



Рис. 1: Расти Рассел

Принцип работы iptables

- 1. Правила содержат критерии и цель; Критерии: -protocol, -source, -destination, -jump, -in-interface, -dport, -sport и т.д. Основные действия: ACCEPT, DROP, QUEUE, RETURN, REJECT, DENY, ESTABLISHED.
- 2. Модуль добавляет новые опции;
- 3. Цепочка набор правил;
- 4. Таблица хранит цепочки правил. Raw (PREROUTING, OUTPUT), NAT (PREROUTING, POSTROUTING, OUTPUT), Filter (INPUT, FORWARD, OUTPUT), Mangle (все пять цепочек).

Схема работы iptables

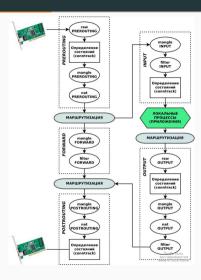


Рис. 2: Схема работы iptables

Практическое применение iptables

iptables [-t таблица] команда [критерии] [действие]

```
[root@server.aamishina.net ~]# iptables --version
iptables v1.8.10 (nf tables)
[root@server.aamishina.net ~]# iptables --list
Chain INPUT (policy ACCEPT)
target
          prot opt source
                                       destination
ACCEPT
          all -- anywhere
                                       anywhere
Chain FORWARD (policy ACCEPT)
target
          prot opt source
                                       destination
Chain OUTPUT (policy ACCEPT)
target
          prot opt source
                                       destination
[root@server.aamishina.net ~]# iptables --line-numbers -L -v -n
Chain INPUT (policy ACCEPT 905 packets, 4317K bytes)
num pkts bytes target prot opt in
                                                                      destination
       36 5088 ACCEPT
                                                  0.0.0.0/0
                                                                       0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in
                                                                       destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target
                          prot opt in
                                                                       destination
[root@server.aamishina.net ~]#
```

Рис. 3: Просмотр версии и текущей конфигурации iptables

Блокировка ІР-адресов

```
[root@server.aamishina.net ~]# iptables -t filter -A INPUT -s 10.0.36.126 -i REJECT
root@server.aamishina.net ~l# iptables -A INPUT -s 10.0.36.0/255.255.255.0 -i REJECT
root@server.aamishina.net ~]# iptables -A OUTPUT -d 10.0.36.126 -j REJECT
root@server.aamishina.net ~]# iptables --line-number -L -v -n
Chain INPUT (policy ACCEPT 942 packets, 4320K bytes)
                                                                        destination
      pkts bytes target
                           prot opt in
                                                    source
              0 REJECT
                                                    10.0.36.126
                                                                         0.0.0.0/0
                                                                                              reject-with icmp-port-unreachabl
         0
              0 REJECT
                                                   10.0.36.0/24
                                                                         0.0.0.0/0
                                                                                              reject-with icmp-port-unreachabl
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
     pkts bytes target
                           prot opt in
                                                                         destination
                                                    source
Chain OUTPUT (policy ACCEPT 42 packets, 3450 bytes)
                                                                         destination
      pkts bytes target
                           prot opt in
                                            out
                                                    source
              0 REJECT
                                                    0.0.0.0/0
                                                                         10.0.36.126
                                                                                              reject-with icmp-port-unreachabl
root@server.aamishina.net ~1#
```

Рис. 4: Блокировка ІР-адресов

Блокировка портов

```
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp --dport ssh -s 10.0.36.126 -i REJECT
 root@server.aamishina.net ~1# iptables -A INPUT -p udp --dport ssh -s 10.0.36.126 -i REJECT
 root@server.aamishina.net ~]# iptables -A INPUT -p tcp --dport 22 -s 10.0.36.126 -i REJECT
 root@server.aamishina.net ~l# iptables -A INPUT -p tcp --dport ssh -i DROP
 root@server.aamishina.net ~1# iptables --line-number -L -v -n
Chain INPUT (policy ACCEPT 947 packets, 4320K bytes)
     pkts bytes target
                           prot opt in
                                                    source
                                                                         destination
              0 REJECT
                                                                                              reject-with icmp-port-unreachabl
                                                    10.0.36.126
                                                                         0.0.0.0/0
              0 REJECT
                                                    10.0.36.0/24
                                                                         0.0.0.0/0
                                                                                              reject-with icmp-port-unreachabl
              0 REJECT
                                                    10.0.36.126
                                                                         0.0.0.0/0
                                                                                              tcp dpt:22 reject-with icmp-port
 unreachable
              0 REJECT
                                                    10.0.36.126
                                                                         0.0.0.0/0
                                                                                              udp dpt:22 reject-with icmp-port
 unreachable
              0 REJECT
                                                    10.0.36.126
                                                                         0.0.0.0/0
                                                                                              tcp dpt:22 reject-with icmp-port
 unreachable
              e DROP
                                                    0.0.0.0/0
                                                                         0.0.0.0/0
                                                                                              tcp dpt:22
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
     pkts bytes target
                           prot opt in
                                                                         destination
                                                    source
Chain OUTPUT (policy ACCEPT 47 packets, 3830 bytes)
      pkts bytes target
                           prot opt in
                                                    source
                                                                         destination
              0 REJECT
                                                                                              reject-with icmp-port-unreachabl
                                                    0.0.0.0/0
                                                                         10.0.36.126
 [root@server.aamishina.net ~]#
```

Рис. 5: Блокировка портов

Разрешение ІР-адреса

```
root@server.aamishina.net ~l# iptables -A INPUT -s 10.0.36.126 -i ACCEPT
froot@server.aamishina.net ~1# iptables -A INPUT -m iprange --src-range 19.8.36.126-18.9.36.156 -i ACCEPT
[root@server.aamishina.net ~]# iptables -A OUTPUT -m iprange --dst-range 10.0.36.126-10.0.36.156 -j ACCEPT
[root@server.aamishina.net ~]# iptables --line-number -L -v -n
Chain INPUT (policy ACCEPT 952 packets, 4321K bytes)
num okts bytes target
                            prot opt in
                                                                         destination
              0 REJECT
                                                    10.0.36.126
                                                                         0.0.0.0/0
                                                                                              reject-with icmp-port-unreachabl
              0 REJECT
                                                    10.0.36.0/24
                                                                         0.0.0.0/0
                                                                                              reject-with icmp-port-unreachabl
              0 REJECT
                                                   10.0.36.126
                                                                         0.0.0.0/0
                                                                                              tcp_dot:22_reject-with_icmp-port
unreachable
              0 REJECT
                                                   10.0.36.126
                                                                         0.0.0.0/0
                                                                                              udp dpt:22 reject-with icmp-port
unreachable
              0 REJECT
                                                    10.0.36.126
                                                                                              tcp dpt:22 reject-with icmp-port
unreachable
                                                                                              tcp dpt:22
              e DROP
                                                    0.0.0.0/0
                                                                         0.0.0.0/0
              0 ACCEPT
                                                    10.0.36.126
                                                                         0.0.0.0/0
                                                    0.0.0.0/0
                                                                         0.0.0.0/0
                                                                                              source IP range 10.0.36.126-10.0
36.156
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target
                            prot opt in
                                                                         destination
Chain OUTPUT (policy ACCEPT 52 packets, 4210 bytes)
     pkts bytes target
                            prot opt in
                                                    source
                                                                         destination
               0 REJECT
                                                    0.0.0.0/0
                                                                         10.0.36.126
                                                                                              reject-with icmp-port-unreachabl
              0 ACCEPT
                                                    0.0.0.0/0
                                                                         0.0.0.0/0
                                                                                              destination IP range 10.0.36.126
10.0.36.156
[root@server.aamishina.net ~]#
```

Рис. 6: Разрешение ІР-адреса

Открытие портов

```
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp --dport 22 -s 10.0.36.126 -i ACCEPT
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp -m multiport --dports 22,80,443 -s 10.0.36.126 -i ACCEPT
[root@server.aamishina.net ~]# iptables --line-number -L -v -n
Chain INPUT (policy ACCEPT 956 packets, 4321K bytes)
num pkts bytes target
                            prot opt in
                                                                          destination
               0 REJECT
                                                    10.0.36.126
                                                                                               reject-with icmp-port-unreachabl
                                                                          0.0.0.0/0
               0 REJECT
                                                    10.0.36.0/24
                                                                          0.0.0.0/0
                                                                                               reject-with icmp-port-unreachabl
               0 REJECT
                                                    10.0.36.126
                                                                          0.0.0.0/0
                                                                                               tcp dot:22 reject-with icmp-port
 unreachable
               0 REJECT
                                                    10.0.36.126
                                                                          0.0.0.0/0
                                                                                               udp_dpt:22 reject-with icmp-port
 unreachable
               0 REJECT
                                                    10.0.36.126
                                                                                               tcp dot:22 reject-with icmp-port
                                                                          0.0.0.0/0
 unreachable
                                                    0.0.0.0/0
                                                                                               tcp dpt:22
               e DROP
                                                                          0.0.0.0/0
               0 ACCEPT
                                                    10.0.36.126
                                                                          0.0.0.0/0
               0 ACCEPT
                                                                                               source IP range 10.0.36.126-10.0
                                                                          0.0.0.0/0
 36.156
               0 ACCEPT
                                                    10.0.36.126
                                                                          0.0.0.0/0
                                                                                               tcp dpt:22
               0 ACCEPT
                                                    10.0.36.126
                                                                                               multiport dports 22,80,443
                                                                          0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
    pkts bytes target
                            prot opt in
                                                                          destination
Chain OUTPUT (policy ACCEPT 56 packets, 4514 bytes)
      pkts bytes target
                            prot opt in
                                                    source
                                                                          destination
                                                                                               reject-with icmp-port-unreachabl
                                                    0.0.0.0/0
                                                                          10.0.36.126
               0 ACCEPT
                                                    0.0.0.0/0
                                                                          0.0.0.0/0
                                                                                              destination IP range 10.0.36.126
-10.0.36.156
[root@server.aamishina.net ~]#
```

Рис. 7: Открытие портов

Запрет и разрешение ІСМР-трафика

```
root@server.aamishina.net ~1# iptables -F
root@server.aamishina.net ~l# iptables -A INPUT -i REJECT -p icmp --icmp-type echo-request
root@server.aamishina.net ~1# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
From 127.0.0.1 icmp seg=1 Destination Port Unreachable
From 127.0.0.1 icmp seg=2 Destination Port Unreachable
From 127.0.0.1 icmp_seg=3 Destination Port Unreachable
 -- 127.0.0.1 ping statistics ---
 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2032ms
[root@server.aamishina.net ~]# iptables -I INPUT 1 -p icmp --icmp-type_echo-request -i ACCEPT
root@server.aamishina.net ~1# ping 127.0.0.1
PING 127.8.8.1 (127.8.8.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp seg=1 ttl=64 time=0.034 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.063 ms
-- 127.0.0.1 ping statistics ---
packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.034/0.049/0.063/0.011 ms
root@server.aamishina.net ~]# iptables --line-number -L -v -n
Chain INPUT (policy ACCEPT 998 packets, 4324K bytes)
num pkts bytes target prot opt in
                                                                        destination
        3 252 ACCEPT
                                                  0.0.0.0/0
                                                                        0.0.0.0/0
                                                                                             icmptype 8
                                                                                            icmptype 8 reject-with icmp-port
        3 252 REJECT
                                                  0.0.0.0/0
                                                                        0.0.0.0/0
unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target
                          prot opt in
                                                                        destination
Chain OUTPUT (policy ACCEPT 113 packets, 9690 bytes)
num okts bytes target
                           prot opt in
                                                                        destination
[root@server.aamishina.net ~1#
```

Рис. 8: Запрет и разрешение ІСМР-трафика

Заключение

- Ключевой инструмент безопасности
- Обеспечивает защиту серверов от различных атак
- Имеет расширяемый функционал