Фильтр пакетов iptables

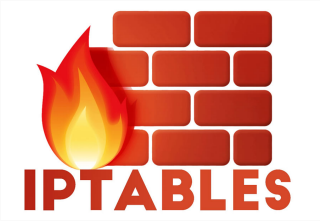
Администрирование сетевых подсистем

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

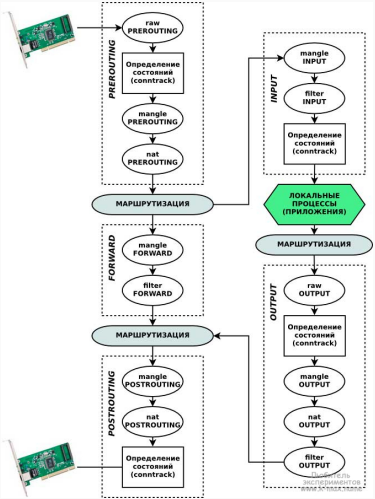


Рис. 2: Схема работы iptables

```
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     out     source               destination
1       36  5088 ACCEPT     0    --  lo     *       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     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
[root@server.aamishina.net ~]#
```

Рис. 3: Просмотр версии и текущей конфигурации iptables

Блокировка IP-адресов

```
[root@server.aamishina.net ~]# iptables -t filter -A INPUT -s 10.0.36.126 -j REJECT
[root@server.aamishina.net ~]# iptables -A INPUT -s 10.0.36.0/255.255.255.0 -j 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)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     0    --  *      *       10.0.36.126          0.0.0.0/0           reject-with icmp-port-unreachabl
e
2        0     0 REJECT     0    --  *      *       10.0.36.0/24         0.0.0.0/0           reject-with icmp-port-unreachabl
e

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 42 packets, 3450 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     0    --  *      *       0.0.0.0/0            10.0.36.126         reject-with icmp-port-unreachabl
e
[root@server.aamishina.net ~]#
```

Рис. 4: Блокировка IP-адресов

Блокировка портов

```
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp --dport ssh -s 10.0.36.126 -j REJECT
[root@server.aamishina.net ~]# iptables -A INPUT -p udp --dport ssh -s 10.0.36.126 -j REJECT
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp --dport 22 -s 10.0.36.126 -j REJECT
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp --dport ssh -j DROP
[root@server.aamishina.net ~]# iptables --line-number -L -v -n
Chain INPUT (policy ACCEPT 947 packets, 4320K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     0    --  *      *       10.0.36.126          0.0.0.0/0           reject-with icmp-port-unreachabl
e
2        0     0 REJECT     0    --  *      *       10.0.36.0/24         0.0.0.0/0           reject-with icmp-port-unreachabl
e
3        0     0 REJECT     6    --  *      *       10.0.36.126          0.0.0.0/0           tcp dpt:22 reject-with icmp-port
-unreachable
4        0     0 REJECT     17   --  *      *       10.0.36.126          0.0.0.0/0           udp dpt:22 reject-with icmp-port
-unreachable
5        0     0 REJECT     6    --  *      *       10.0.36.126          0.0.0.0/0           tcp dpt:22 reject-with icmp-port
-unreachable
6        0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 47 packets, 3830 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     0    --  *      *       0.0.0.0/0            10.0.36.126         reject-with icmp-port-unreachabl
e
[root@server.aamishina.net ~]#
```

Рис. 5: Блокировка портов

Разрешение IP-адреса

```
[root@server.aamishina.net ~]# iptables -A INPUT -s 10.0.36.126 -j ACCEPT
[root@server.aamishina.net ~]# iptables -A INPUT -m iprange --src-range 10.0.36.126-10.0.36.156 -j 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   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     0    --  *      *       10.0.36.126          0.0.0.0/0            reject-with icmp-port-unreachabl
e
2        0     0 REJECT     0    --  *      *       10.0.36.0/24         0.0.0.0/0            reject-with icmp-port-unreachabl
e
3        0     0 REJECT     6    --  *      *       10.0.36.126          0.0.0.0/0            tcp dpt:22 reject-with icmp-port
-unreachable
4        0     0 REJECT     17   --  *      *       10.0.36.126          0.0.0.0/0            udp dpt:22 reject-with icmp-port
-unreachable
5        0     0 REJECT     6    --  *      *       10.0.36.126          0.0.0.0/0            tcp dpt:22 reject-with icmp-port
-unreachable
6        0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
7        0     0 ACCEPT     0    --  *      *       10.0.36.126          0.0.0.0/0
8        0     0 ACCEPT     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     out     source               destination

Chain OUTPUT (policy ACCEPT 52 packets, 4210 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     0    --  *      *       0.0.0.0/0            10.0.36.126          reject-with icmp-port-unreachabl
e
2        0     0 ACCEPT     0    --  *      *       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 IP-адреса

Открытие портов

```
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp --dport 22 -s 10.0.36.126 -j ACCEPT
[root@server.aamishina.net ~]# iptables -A INPUT -p tcp -m multiport --dports 22,80,443 -s 10.0.36.126 -j 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     out     source               destination
1        0     0 REJECT     0    --  *      *       10.0.36.126          0.0.0.0/0            reject-with icmp-port-unreachabl
e
2        0     0 REJECT     0    --  *      *       10.0.36.0/24         0.0.0.0/0            reject-with icmp-port-unreachabl
e
3        0     0 REJECT     6    --  *      *       10.0.36.126          0.0.0.0/0            tcp dpt:22 reject-with icmp-port
-unreachable
4        0     0 REJECT     17   --  *      *       10.0.36.126          0.0.0.0/0            udp dpt:22 reject-with icmp-port
-unreachable
5        0     0 REJECT     6    --  *      *       10.0.36.126          0.0.0.0/0            tcp dpt:22 reject-with icmp-port
-unreachable
6        0     0 DROP       6    --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22
7        0     0 ACCEPT     0    --  *      *       10.0.36.126          0.0.0.0/0
8        0     0 ACCEPT     0    --  *      *       0.0.0.0/0            0.0.0.0/0            source IP range 10.0.36.126-10.0
.36.156
9        0     0 ACCEPT     6    --  *      *       10.0.36.126          0.0.0.0/0            tcp dpt:22
10       0     0 ACCEPT     6    --  *      *       10.0.36.126          0.0.0.0/0            multiport dports 22,80,443

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 56 packets, 4514 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     0    --  *      *       0.0.0.0/0            10.0.36.126          reject-with icmp-port-unreachabl
e
2        0     0 ACCEPT     0    --  *      *       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 ICMP-трафика

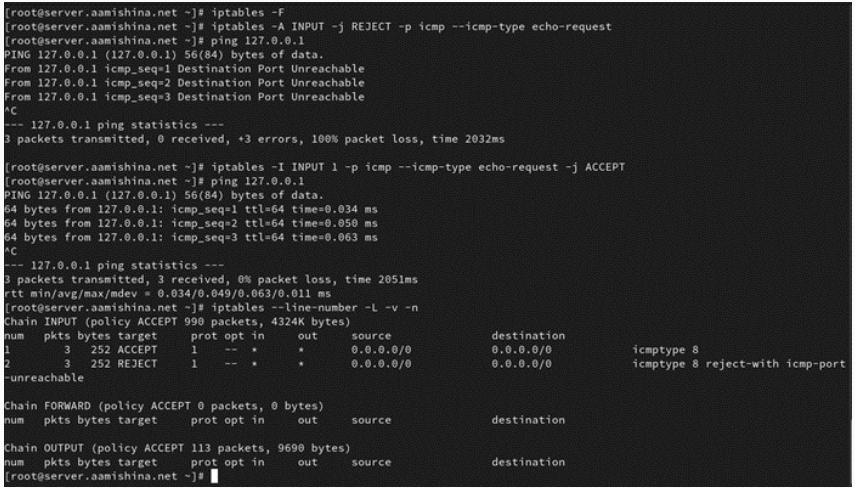


Рис. 8: Запрет и разрешение ICMP-трафика

Заключение

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