ip6tables

linux中防火墙软件

补充说明

ip6tables命令 和iptables一样，都是linux中防火墙软件，不同的是ip6tables采用的TCP/ip协议为IPv6

语法

```
ip6tables(选项)
```

选项

```
-t<表>：指定要操纵的表；
-A向规则链中添加条目；
-D从规则链中删除条目；
-i向规则链中插入条目；
-R替换规则链中的条目；
-L显示规则链中已有的条目；
-F清楚规则链中已有的条目；
-Z清空规则链中的数据包计算器和字节计数器；
-N创建新的用户自定义规则链；
-P定义规则链中的默认目标；
-h显示帮助信息；
-p指定要匹配的数据包协议类型；
-s指定要匹配的数据包源ip地址；
-j<目标>：指定要跳转的目标；
-i<网络接口>：指定数据包进入本机的网络接口；
-o<网络接口>：指定数据包要离开本机所使用的网络接口。
-c<计数器>：在执行插入操作insert追加操作append替换操作replace时初始化包计数器和字节计数器。
```

实例

在命令行窗口输入下面的指令就可以查看当前的 IPv6 防火墙配置：

```
ip6tables -nl --line-numbers
```

/etc/sysconfig/ip6tables文件

使用编辑器编辑/etc/sysconfig/ip6tables文件：

```
vi /etc/sysconfig/ip6tables
```

可能会看到下面的默认 ip6tables 规则：

```
*filter
:INPUT accept [0:0]
:FORWARD ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmpv6 -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d ff02::fb -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 32768:61000 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 32768:61000 ! --syn -j ACCEPT
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j reject --reject-with icmp6-adm-prohibited
COMMIT
```

与 IPv4 的 iptables 规则类似，但又不完全相同。

要开启 80 端口（HTTP 服务器端口），在 COMMIT 一行之前添加如下规则：

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 80 -j ACCEPT
```

`-p tcp`表示仅针对 tcp 协议的通信。`--dport`指定端口号。

要开启 53 端口（DNS 服务器端口），在 COMMIT 一行之前添加如下规则：

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -m udp -p tcp --dport 53 -j ACCEPT
```

同时针对 tcp 和 udp 协议开启 53 端口。

要开启 443 端口，在 COMMIT 一行之前添加如下规则：

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 443 -j ACCEPT
```

要开启 25 端口（SMTP 邮件服务器端口），在 COMMIT 一行之前添加如下规则：

```
-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 25 -j ACCEPT
```

对于那些没有特定规则与之匹配的数据包，可能是我们不想要的，多半是有问题的。我们可能也希望在丢弃（DROP）之前记录它们。此时，可以将最后一行：

```
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

改为：

```
-A RH-Firewall-1-INPUT -j LOG
-A RH-Firewall-1-INPUT -j DROP
```

```
COMMIT
```

保存并关闭该文件。然后重新启动 ip6tables 防火墙：

```
# service ip6tables restart
```

然后重新查看 ip6tables 规则，可以看到如下所示的输出：

```
# ip6tables -vnL --line-numbers
```

输出示例：

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source
destination
1    42237 3243K RH-Firewall-1-INPUT  all      *      *       ::/0
::/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source
destination
1        0     0 RH-Firewall-1-INPUT  all      *      *       ::/0
::/0
Chain OUTPUT (policy ACCEPT 12557 packets, 2042K bytes)
num   pkts bytes target     prot opt in     out     source
destination
Chain RH-Firewall-1-INPUT (2 references)
num   pkts bytes target     prot opt in     out     source
destination
1        6   656 ACCEPT     all      lo     *       ::/0
::/0
2    37519 2730K ACCEPT     icmpv6    *      *       ::/0
::/0
3        0     0 ACCEPT     esp      *      *       ::/0
::/0
4        0     0 ACCEPT     ah       *      *       ::/0
::/0
5      413 48385 ACCEPT     udp      *      *       ::/0
ff02::fb/128       udp dpt:5353
6        0     0 ACCEPT     udp      *      *       ::/0
::/0               udp dpt:631
7        0     0 ACCEPT     tcp      *      *       ::/0
::/0               tcp dpt:631
8      173 79521 ACCEPT     udp      *      *       ::/0
::/0               udp dpts:32768:61000
9        0     0 ACCEPT     tcp      *      *       ::/0
::/0               tcp dpts:32768:61000 flags:!0x16/0x02
10       0     0 ACCEPT     tcp      *      *       ::/0
::/0               tcp dpt:22
11       0     0 ACCEPT     tcp      *      *       ::/0
::/0               tcp dpt:80
12       0     0 ACCEPT     tcp      *      *       ::/0
```

```
::/0                tcp dpt:53
13    4108  380K ACCEPT     udp      *      *       ::/0
::/0                udp dpt:53
14      18  4196 REJECT     all      *      *       ::/0
::/0
```

IPv6 私有 IP

IPv4 通常默认即可保护内部局域网私有 IP 上的主机。但是 IPv6 的地址非常丰富，不再需要使用类似 NAT 等协议的私有网络。这样一来，所有的内部主机都可以拥有公网 IP 而直接连接到互联网，也就同时暴露于互联网上的各种威胁之中了。那么，如何配置 IPv6 防火墙使其默认将除了 ping6 请求之外的所有输入数据包都丢弃呢？可以使用FC00::/7 前缀来标识本地 IPv6 单播地址。

允许特定的 ICMPv6 通信

使用 IPv6 的时候需要允许比 IPv4 更多类型的 ICMP 通信以保证路由和 IP 地址自动配置等功能正常工作。有时候，如果你的规则设置太过苛刻，可能都无法分配到正确的 IPv6 地址。当然，不使用 DHCP 而是手动配置 IP 地址的除外。

下面是一些比较常见的 ipv6-icmp 配置实例：

```
:ICMPv6 - [0:0]
# Approve certain ICMPv6 types and all outgoing ICMPv6
# http://forum.linode.com/viewtopic.php?p=39840#39840
-A INPUT -p icmpv6 -j ICMPv6
-A ICMPv6 -p icmpv6 --icmpv6-type echo-request -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type destination-unreachable -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type packet-too-big -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type time-exceeded -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type router-solicitation -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type router-advertisement -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type neighbour-solicitation -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type neighbour-advertisement -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type redirect -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 141 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 142 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 148 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 149 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 130 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 131 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 132 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 143 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 151 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 152 -s fe80::/10 -j ACCEPT
-A ICMPv6 -p icmpv6 --icmpv6-type 153 -s fe80::/10 -j ACCEPT
-A ICMPv6 -j RETURN
-A OUTPUT -p icmpv6 -j ACCEPT
```