Linux 防火墙 iptables

周旭光
unixzhou@sina.com
2011 年 5 月 10 日

目录

1、Linux 防火墙基础

1、iptables 的规则表、链结构

1.1 规则表

iptables 管理 4 个不同的规则表，其功能由独立的内核模块实现。

filter 表：	包含三个链 INPUT , OUTPUT , FORWARD
nat 表：	PREROUTING , POSTROTING , OUTPUT
mangle 表：	PREROUTING , POSTROUTING , INPUT , OUTPUT , FORWARD
raw 表：	OUTPUT , PREROUTING

1.2 规则链

INPUT 链	当收到访问防火墙本机的数据包（入站）时，应用此链中的规则
OUTPUT 链	当防火墙本机向外发送数据包（出站）时，应用此链中的规则
FORWARD 链	收到需要通过防火墙发送给其他地址的数据包，应用此链
PREROUTING 链	做路由选择之前，应用此链
POSTROUTING 链	对数据包做路由选择之后，应用此链中的规则

2、数据包的匹配流程

2.1 规则表之间的优先级

Raw mangle nat filter

2.2 规则链之间的优先级

入站数据流向： 来自外界的数据包到达防火墙，首先呗 PREROUTING 规则链处理（是否被修改地址），之后会进行路由选择(判断该数据包应该发往何处)，如果数据包的目标地址是防火墙本机，那么内核将其传递给 INPUT 链进行处理，通过以后再交给上次的应用程序进行响应

转发数据流向： 来自外界的数据包到达防火墙后，首先被 PREROUTING 规则链处理，之后进行路由选择，如果数据包的目标地址是其他外部地址，则内核将其传递给 FPRWARD 链进行处理，然后再交给 POSTROUTIING 规则链（是否修改数据包的地址等）进行处理。

出站数据流向： 防火墙本身向外部地址发送数据包，首先被 OUTPUT 规则链处理，之后进行路由选择，然后

交给 POSTROUTING 规则链（是否修改数据包的地址等）进行处理。

2.3 规则链内部各防火墙规则之间的优先顺序

依次按第 1 条规则、第 2 条规则、第 3 条规则……的顺序进行处理，找到一条能够匹配的数据包规则，则不再继续检查后面的规则（使用 LOG 记录日志的规则例外）。如果找不到匹配规则，就按照规则链的默认策略进行处理

2、管理和设置 iptables 规则

2.1 iptables 的基本语法格式

iptables [-t 表名] 命令选项 [链名] [条件匹配] [-j 目标动作或跳转]

2.2 管理 iptables 规则

iptables 命令的管理控制项

选项名	功能及特点
-A	在指定链的末尾添加（--append）一条新规则
-D	删除（--delete）指定链中的某一条规则，按规则序号或内容确定要删除的规则
-I	在指定链中插入一条新规则，若未指定插入位置，则默认在链的开头插入
-R	修改、替换指定链中的一条规则，按按规则序号或内容确定要替换的规则
-L	列出指定链中所有的规则进行查看，若未指定链名，则列出表中所有链的内容
-F	清空指定链中的所有规则，若未指定链名，则清空表中所有链的内容
-N	新建一条用户自定义的规则链
-X	删除表中用户自定义的规则链
-P	设置指定链的默认策略（大 p）
-n	使用数字形式显示输出结果，如显示主机的 IP 地址而不是主机名
-v	查看规则列表时显示详细的信息
-V	查看 iptables 命令工具的版本信息
-h	查看命令帮助信息
--line-numbers	查看规则列表时，同时显示规则在链中的顺序号

2.2.1 添加及输入规则

iptables -t filter -A INPUT -p tcp -j ACCEPT

在 filter 表的 INPUT 链的末尾添加一条防火墙规则

iptables -I INPUT -p udp -j ACCEPT
在 filter 表的 INPUT 链中插入一条防火墙规则（省略 –t filter，按默认处理 filter 表）

iptables -I INPUT 2 -p icmp -j ACCEPT
在 filter 表的 INPUT 链中插入一条防火墙规则，作为链中的第二条规则

2.2.2 查看规则表

iptables -L INPUT - -line-numbers
查看 filter 表中 INPUT 链中的所有规则，同时显示各条规则的顺序号

iptables –nvL
-L 选项放在最后，否则会将 vn 当成链名。查看 filter 表各链中所有规则的详细信息，同时以数字形式显示地址和端口号

2.2.3 删除、清空规则

iptables -D INPUT 2
删除 filter 表 INPUT 链中的第二条规则

iptables -F
不指定表名时，默认情况 filter 表

iptables -t nat –F
清空 nat 表中各链的所有规则

iptables -t mangle -F
清空 mangle 表中各链的所有规则

2.2.4 设置规则链的默认策略

iptables -t filter -P FORWARD DROP
将 filter 表中 FORWARD 规则的默认策略设为 DROP

iptables -P OUTPUT ACCEPT
将 filter 表中 OUTPUT 规则的默认策略设为 ACCEPT

2.2.5 获得 iptables 相关选项的帮助信息

iptables -p icmp –h
查看 iptables 命令中关于 icmp 协议的帮助信息

2.2.6 新增、删除自定义规则链

```
# iptables -t raw -N TCP_PACKETS
```

在 raw 表中新增一条自定义的规则链，链名为 TCP_PACKETS

```
# iptables -t raw -X
```

清空 raw 表中用户自定义的所有规则链

2.3 条件匹配

2.3.1 通用（general）条件匹配

直接使用，而不依赖于其他的条件匹配及其扩展

2.3.1.1 协议匹配（允许使用的协议名包含在/etc/protocols 文件中）

```
# iptables -I INPUT -p icmp REJECT
```

拒绝进入防火墙的所有 icmp 数据包

```
# iptables -I FORWARD -p ! icmp -j ACCEPT
```

允许防火墙转发 icmp 协议以外的所有数据包（叹号表示取反）

2.3.1.2 地址匹配

拒绝转发来自 192.168.1.11 主机的数据，允许转发来自 192.168.0./24 网段的数据

```
# iptables -A FORWARD -s 192.168.1.11 -j REJECT
# iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT
```

2.3.1.3 网络接口匹配

丢弃从外网接口 eth1 进入防火墙本机的源地址为私网地址的数据

```
# iptables -A INPUT -i eth1 -s 192.168.0.0/16 -j DROP
# iptables -A INPUT -i eth1 -s 172.16.0.0/12 -j DROP
# iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

管理员在网关服务器上检测到来自某个 IP 网段（如 10.10.30.0./24）的频繁扫描，希望设置 iptables 规则封堵 IP 地址段，两个小时后解封

```
# iptables -I INPUT -s 10.20.30.0/24 -j DROP//设置封堵策略
# iptables -I FORWARD -s 10.20.30.0/24 -j DROP
# at now +2 hours
at> iptables -D INPUT 1
at>iptables -D FORWAD 1
at> <EOT>
```

job 5 at 2020-09-26 19:15

2.3.2 隐含（implicit）条件匹配

需要指定的协议匹配为前提，其对应的功能由 iptables 自动（隐含）的装载入内核

2.3.2.1 端口匹配

仅允许系统管理员从 202.13.0.0/16 网段使用 SSH 方式远程登录防火墙主机

```
# iptables -A INPUT -p tcp - -dport 22 -s 202.13.0.0/16 -j ACCEPT
# iptables -A INPUT -p tcp - -dport 22 -j DROP
```

允许本机开放从 TCP 端口 20~1024 提供的应用服务

```
# iptables -A INPUT -P tcp - -dport 20:1024 -j ACCEPT
# iptables -A OUTPUT -p tcp - -sport 20:1024 -j ACCEPT
```

作为网关使用时，允许转发来自 192.168.0.0/24 局域网的 DNS 解析请求数据包

```
# iptables -A FORWARD -p udp -s 192.168.0.0/24 - -dport 53 -j ACCEPT
# ipatbles -A FORWARD -p udp -d 192.168.0.0./24 - -sport 53 -j ACCEPT
```

2.3.2.2 TCP 标记匹配

拒绝从外网接口 eth1 直接访问防火墙本机的数据包，但是允许相应防火墙 TCP 请求的数据包进入

```
# iptables -P INPUT DROP
# iptables -I INPUT -i eth1 -p tcp - -tcp-flags SYN,RST,ACK SYN -j ACCEPT
# iptables -I INPUT -i eth1 -p tcp - -tcp-flags ! - -syn -j ACCEPT
```

2.3.2.3 ICMP 类型匹配

禁止其他主机 ping 防火墙主机，但是允许从防火墙上 ping 其他主机（允许接受 ICMP 回应数据）

```
# iptables -A INPUT -p icmp - -icmp-type Echo-Request -j DROP
# iptables -A INPUT -p icmp - -icmp-type Echo-Replay -j ACCEPT
# iptables -A INPUT -p icmp - -icmp-type destination-Unreachable -j ACCEPT
```

Echo-Request 数字代码为 8 请求
Echo-Replay 数字代码为 0 回显
destination-Unreachable 3 目标不可达

2.3.3 显示（explicit）条件匹配

由额外的内核模块提供，因此需要手工指定匹配方式
lsmod 命令查看内核模块

2.3.3.1 MAC 地址匹配（主要用于检查数据包的源 MAC 地址）

禁止转发来自 MAC 地址为 00：0C:29:27:55:3F 的主机数据包

```
# iptables -A FORWARD -m mac - -mac-source 00：0C:29:27:55:3F -j DROP
```

2.3.3.2 多端口匹配（检查数据包的源端口、目标端口时，用于匹配多个不连续的端口号）

允许防火墙本机对外开放 TCP 端口 20、21、25、110 以及被动模式 FTP 端口 1250~1280

```
# iptables -A INPUT -p tcp -m multiport - -dport 20,21,25,110,1250:1280 -j ACCEPT
```

2.3.3.3 多 IP 地址匹配

禁止转发 IP 地址为 192.168.1.20~192.168.1.99 的 TCP 的数据包

```
# iptables -A FORWARD -p tcp -m iprange - -src-range 192.168.1.20-192.168.1.99 -j DROP
```

2.3.3.4 状态匹配

禁止转发与正常 TCP 连接无关的非 - -syn 请求数据包

```
# iptables -A FORWARD -m state - -state NEW -p tcp ! - -syn -j DROP
```

拒绝访问防火墙的新数据包，但允许响应或与已有连接相关的数据包

```
# iptables -A INPUT -p tcp -m state - -state NEW -j DROP
# iptables -A INPUT -p tcp -m state - -state ESTABLISHED,RELATED -j ACCEPT
```

NEW：与任何连接无关的
ESTABLISHED：响应请求或已经建立的连接
RELATED：与已有连接有相关性

2.4 数据包控制

ACCEPT :允许数据包通过
DROP :直接丢弃数据包，不给出任何回应信息
REJECT ：拒绝数据包通过，必要时会给数据发送一个响应信息
LOG ：在/var/log/messange 文件中记录日志信息，然后将数据包传递给下一条规则

对于尝试通过 SSH 方式登录防火墙主机的访问数据，记录日志信息并禁止其访问

```
# iptables -I INPUT -p tcp - -dport 22 -j DROP
# iptables -I INPUT -P tcp - -dport 22 -j LOG
```

将记录日志的频率限制为平均三次/分钟 ，允许的峰值为八次

```
# iptables -R INPUT 1 -p tcp - -dport 22 -m limit - -limit 3/minite - -limit-burst 8 -j LOG
```

用户自定义链 ：将数据包传递给用户自定义的链进行处理
自定义一个新的链 MyLAN1,转发自/至 192.168.1.0/24 网段的数据包均交给该链中的规则处理

```
# iptables -t filter -N MyLAN1
# iptables -A FORWARD -s 192.168.1.0/24 -j MyLAN1
# iptables -A FORWARD -d 192.168.10./24 -j MyLAN1
# iptables -A MyLAN1 -p icmp DROP
```

SNAT :修改数据包的源 IP 地址
DNAT ： 修改数据包的目标 IP 地址

3、使用防火墙脚本

3.1 导出、导入防火墙规则

1.iptables-save
把当前设置的防火墙规则信息输出到终端 将当前调试好的 iptables 规则保存到配置文件，并通过 iptables 服务脚本自动加载

```
# iptables-save > /etc/sysconfig/iptables 或 service iptables save
# service iptables restart
# chkconfig - -level 35 iptables on
```

2.iptalbes-restore
从已保存的配置文件中导入 iptables 规则

```
# iptables-retore < /etc/sysconfig/iptables
```

3.2 编写防火墙脚本

1.设置网段、网卡、IP 地址等变量
2.加载包过滤相关的内核模块
3.开启路由转发功能
4.用户设置的 iptables 规则