Linux 防火墙 iptables 学习笔记（一）入门要领

首先我们要弄明白，防火墙将怎么对待这些数据包。这些数据包会经过一些相应的规则链，比如要进入你的计算机的数据包会首先进入 INPUT 链，从我们的计算机发出的数据包会经过 OUTPUT 链，如果一台计算机做一个网络的网关（处于内网和外网两个网络连接的两台计算机，这两台计算机之间相互通讯的数据包会经过这台计算机，这台计算机即相当于一个路由器），可能会有很多数据经过这台计算机，那么这些数据包必经 FORWARD 链，FORWARD 链即数据转发链。明白了这些“链”的概念我们才能进一步学习使用 iptables。

现在我们再来分析一下 iptables 规则是如何工作的，假如我们要访问网站 www.yahoo.com，我们要对 www.yahoo.com 发出请求，这些数据包要经过 OUTPUT 链，在请求发出前，Linux 的内核会在 OUTPUT 链中检查有没有相应的规则适合这个数据包，如果没有相应的规则，OUTPUT 链还会有默认的规则，或者允许，或者不允许（事实上，不允许有两种，一种是把请求拒绝，告诉发出请示的程序被拒绝；还有一种是丢弃，让请求发出者傻等，直到超时）。如果得到允许，请求就发出了，而 www.yahoo.com 服务器返回的数据包会经过 INPUT 链，当然，INPUT 链中也会有相应的规则等着它。

下面我们介绍几个 iptable 的命令

iptables-L[-tfilter]

这条命令是显示当前有什么已经设置好的防火墙规则，可能的显示结果如下：

```
ChainINPUT(policyACCEPT)targetprotoptsourcedestinationChainFORWARD(policyACCEPT)targetprotoptsourcedestinationChainOUTPUT(policyACCEPT)targetprotoptsourcedestination
```

从这里我们可以看出，iptables 有三个链分别是 INPUTOUTPUT 和 FORWARD.

其中 INPUT 是外部数据要进过我们主机的第一外关卡(当然你前面也可以再加硬件防火墙).

OUTPUT 是你的主机的数据送出时要做的过绿卡

FORWARD 是转发你在 NAT 时才会用到

要设置 iptables 主要是对这三条链进行设置,当然也包括-nat 的另外三个链我们以后再说

你要用 iptables 你就得启到它启动命令 serviceiptablesrestart

iptables 的默认设置为三条链都是 ACCEPT 如下:

```
iptables-PINPUTACCEPT

iptables-POUTPUTACCEPT
```

```
iptables-PFORWARDACCEPT
```

以上信息你可以用 iptables-L 看到

总体来说 iptables 可以有二种设置

1.默认允许,拒绝特别的

2.默认拒绝,允许特别的

二者都有自己有特点,从安全角度看个人偏向于第二种,就是默认拒绝,允许特别的.但 iptalbes 默认是第一种默认允许,拒绝特别的

你可以用命令改变默认值来达到我们的要求命令如下

```
iptables-PINPUTDROP

iptables-POUTPUTDROP

iptables-PFORWARDDROP
```

你再用 iptables-L 查看一下就会觉得默认值以改了

先来谈炎几个参数 XZFL

```
-F 清除规则

-X 清除链

-Z 将链的记数的流量清零
```

一般来说再创建访问规则时都会将原有的规则清零这是一个比较好的习惯,因为某些规则的存在会影响你建的规则.

基本语法:

```
iptables[-tfilter][-AIINPUT,OUTPUT,FORWARD][-iointerface]

[-ptcp,udp.icmp,all][-sip/nerwork][--sportports]

[-dip/netword][--dportports][-jACCEPTDROP]
```

以上是 iptables 的基本语法

```
A 是添加的意思

I 是播入的意思

io 指的是数据要进入或出去所要经过的端口如 eth1eth0pppoe 等

p 你所要指定的协议

-s 指源地址可是单个 IP 如 192.168.2.6 也可以是一个网络 192.168.2.0/24 还可以是一个域名如 163.com 如果你填写的域名系统会自动解析出他的 IP 并在 iptables 里显示

--sport 来源端口

-d 同-s 相似只不过他指的是目标地址也可以是 IP 域名和网络

--dport 目标端口

-j 执行参数 ACCEPTDROP
```

注意:如果以有参数存在则说明全部接受

1 如我要来自己 l0 接口的数据全部接受,我们可以写成这样:

```
iptables-AINPUT-ilo-jACCEPT
```

2 如果我们想接受 192.168.2.6 这个 IP 地址传来的数据我们可以这样写

```
iptablse-AINPUT-ieth1-ptcp-s192.168.2.6-jACCEPT
```

3 如果我们要拒绝来自己 192.168.2.0/24 这个网的 telnet 连接

```
iptablse-AINPUT-ieth1-pudp-s192.168.2.0/24

--sport23-jDROP
```