Linux 防火墙设置-DNS 服务器篇

对于刚刚搭建了 DNS 服务器，需要开启防火墙但又不知道该怎么设置的朋友，可以参考下面的内容，或者直接使用下面给出的脚本程序。

如果服务器是作为 DNS 服务器使用的，针对绝大多数的情况，为了开启防火墙同时又能正常地提供相关的服务，一般的设置如下：

【1】第一步：清除默认防火墙规则

```
iptables -F

iptables -X

iptables -Z
```

参数说明：

-F：清除所有的已制定的规则

-X：清除所有用户自定义的 chain（应该说的是 tables）

（扩展：table--Linux 的 iptables 防火墙默认有三种表，Filter、NAT 与 Mangle，当然还有自定义的，其中 Filter 即是默认使用的表格，chain--条链，比如 filter 有 INPUT、OUTPUT、FORWARD 三条链）

-Z：将所有的 chain 的计数与流量统计清零

设置原因：

filter 的三条链中，默认策略都为 ACCEPT，显然对于 INPUT 来说，这是很危险的，可以使用命令 iptables -L -n 来查看默认设置，或者使用 iptables-save 命令（会列出更详细的防火墙配置信息）。

【2】第二步：设置策略

```
iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT
```

设置原因：

DROP 为丢弃，由 1 中可知，INPUT 策略制定为 DROP 时才比较安全。

【3】第三步：根据所需服务制定各项规则

（1）将本机设置为信任设备

```
iptables -A INPUT -i lo -j ACCEPT
```

（2）制定 ssh 远程连接规则

```
iptables -A（添加） INPUT（链路） -p（指定协议） tcp（指定为 TCP 协议） --dport（指定目标端口号） 22（指定目标端口号为 22） -j（指定操作） ACCEPT（指定操作为接受）
```

（3）制定 dns 服务规则

```
iptables -A INPUT -p tcp --dport 53 -j ACCEPT

iptables -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --sport 53 -j ACCEPT

iptables -A INPUT -p udp --sport 53 -j ACCEPT
```

说明：

允许新的 dns 请求，同时允许以 nslookup 的方式来向服务器查询，即以源端口号 53 来查询 dns 信息。

（4）制定其它规则

```
iptables -A INPUT -p icmp -j ACCEPT
```

说明：

可不用，但为了方便检测服务器的网络连通性，所以还是加上。

【4】写入防火墙配置文件

```
/etc/init.d/iptables save
```

说明：

要保存，否则重启服务器后上面所做的配置会失效。

完整的执行脚本如下：

```
#!/bin/bash

PATH=/sbin:/bin:/usr/sbin:/usr/bin; export PATH

iptables -F

iptables -X

iptables -Z



iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -p tcp --dport 53 -j ACCEPT

iptables -A INPUT -p udp --dport 53  -j ACCEPT

iptables -A INPUT -p tcp --sport 53  -j ACCEPT

iptables -A INPUT -p udp --sport 53  -j ACCEPT

iptables -A INPUT -p icmp -j ACCEPT
```

```
/etc/init.d/iptables save
```

保存为.sh 文件，以管理员权限执行即可。

其它常用命令：

查看防火墙简要配置

```
iptables -L -n
```

查看防火墙详细配置

```
iptables-save
```

重要说明：

进行防火墙的配置一定要格外小心，特别在远程做配置时，如果不小心清除了已定义的规则，又把默认的 INPUT 规则设置为 DROP，这时就没有办法远程连接了，这点特别要注意。