配置和管理主机防火墙

应用场景

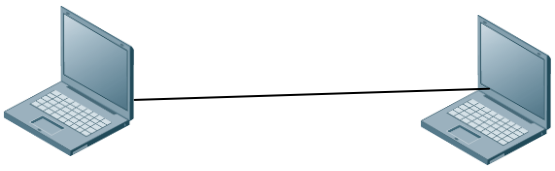
对于 Internet 上的系统，不管是什么情况，首先我们要明确一点：网络是不安全的。因此，虽然创建一个防火墙并不能保证系统 100%安全，但却是绝对必要的。和社会上其它任何事物一样，Internet 经常会受到一些无聊的或者别有用心的人的干扰，防火墙的目的就是将这类人挡在你的网络之外，同时使你仍然可以完成自己的工作。

那么构筑怎样的 Linux 防火墙系统才算是足够安全呢？这是一个很难回答的问题，因为不同的应用环境对安全的要求不一样。用一句比较恰当而且简单的话来回答这个问题：用户了解自己的 Linux 系统和设置，并且可以很好地保护好自己的数据和机密文件的安全，这对于该计算机用户来说就可以称之为他的计算机有足够的安全性。

那么到底什么是防火墙呢？防火墙是一个或一组系统，它在网络之间执行访问控制策略。实现防火墙的实际方式各不相同，但是在原则上，防火墙可以被认为是这样一对机制：一种机制是拦阻传输流通行，另一种机制是允许传输流通过。一些防火墙偏重拦阻传输流的通行，而另一些防火墙则偏重允许传输流通过。了解有关防火墙的最重要的概念可能就是它实现了一种访问控制策略。

一般来说，防火墙在配置上是防止来自“外部”世界未经授权的交互式登录的。这大大有助于防止破坏者登录到你网络中的计算机上。一些设计更为精巧的防火墙可以防止来自外部的传输流进入内部，但又允许内部的用户可以自由地与外部通信。如果你切断防火墙的话，它可以保护你免受网络上任何类型的攻击。防火墙的另一个非常重要的特性是可以提供一个单独的“拦阻点”，在“拦阻点”上设置安全和审计检查。与计算机系统正受到某些人利用调制解调器拨入攻击的情况不同，防火墙可以发挥一种有效的“电话监听”和跟踪工具的作用。防火墙提供了一种重要的记录和审计功能；它们经常可以向管理员提供一些情况概要，提供有关通过防火墙的传输流的类型和数量，以及有多少次试图闯入防火墙的企图等信息。

因此本实验将介绍如何配置 linux 防火墙。



VM Windows　　VM Linux

实验目标

1. 掌握 linux 下基本的 iptables 知识
2. 学会配置 iptables

实验环境

虚拟机： linux,windowsXP；linux 主机用户名：root；密码：root

实验过程指导

一. Iptables 的规则表、链结构

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

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

二. 数据包的匹配流程

1.规则表之间的优先级

raw mangle nat filter

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 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。

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。

三. 管理和设置 iptables 规则

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]

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

1.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

```
[root@localhost ~]# iptables -L INPUT --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    RH-Firewall-1-INPUT  all  --  anywhere             anywhere
[root@localhost ~]# _
```

2.删除、清空规则

iptables -F //不指定表名时，默认情况 filter 表

```
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (0 references)
target     prot opt source               destination
```

3.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

```
[root@localhost ~]# iptables -t filter -P FORWARD DROP
[root@localhost ~]# iptables -P OUTPUT ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (0 references)
target     prot opt source               destination
```

四. 条件匹配

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）

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

```
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere            reject-with
rt-unreachable
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp any
ACCEPT     esp  --  anywhere             anywhere
ACCEPT     ah   --  anywhere             anywhere
```

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

```
[root@localhost ~]# iptables -A FORWARD -s 192.168.1.11 -j REJECT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere            reject-with
rt-unreachable
RH-Firewall-1-INPUT  all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere
REJECT     all  --  192.168.1.11         anywhere            reject-with
rt-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain RH-Firewall-1-INPUT (2 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp any
ACCEPT     esp  --  anywhere             anywhere
ACCEPT     ah   --  anywhere             anywhere
```

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），如果无匹配条件，默认为 REJECT。

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

```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -s 202.13.0.0/16 -j ACCE
PT
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22 -j DROP
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere            reject-with icmp-po
rt-unreachable
RH-Firewall-1-INPUT  all  --  anywhere             anywhere
ACCEPT     tcp  --  202.13.0.0/16        anywhere            tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
RH-Firewall-1-INPUT  all  --  anywhere             anywhere
```

五. 在进行了上述规则讲解与熟悉之后，接下来的步骤进行防火墙规则配置与测试：

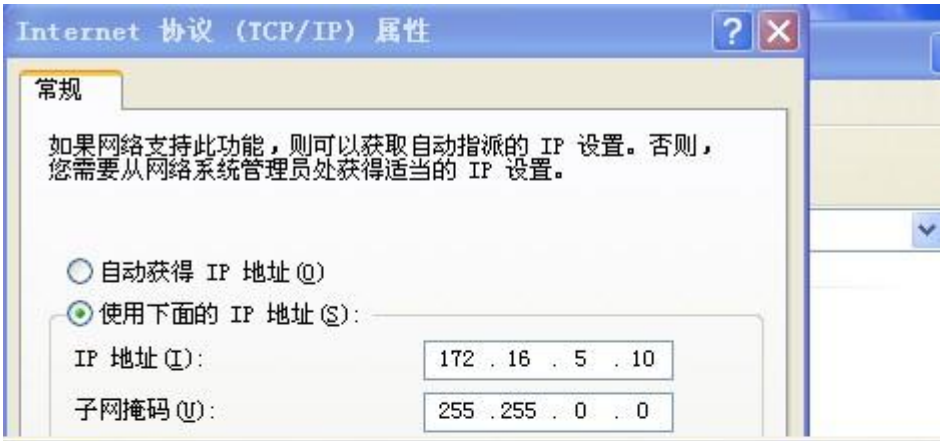
禁止 Windows 主机 ping 防火墙 linux 主机，但是允许从防火墙上 ping 其他主机（允许接受 ICMP 回应数据）

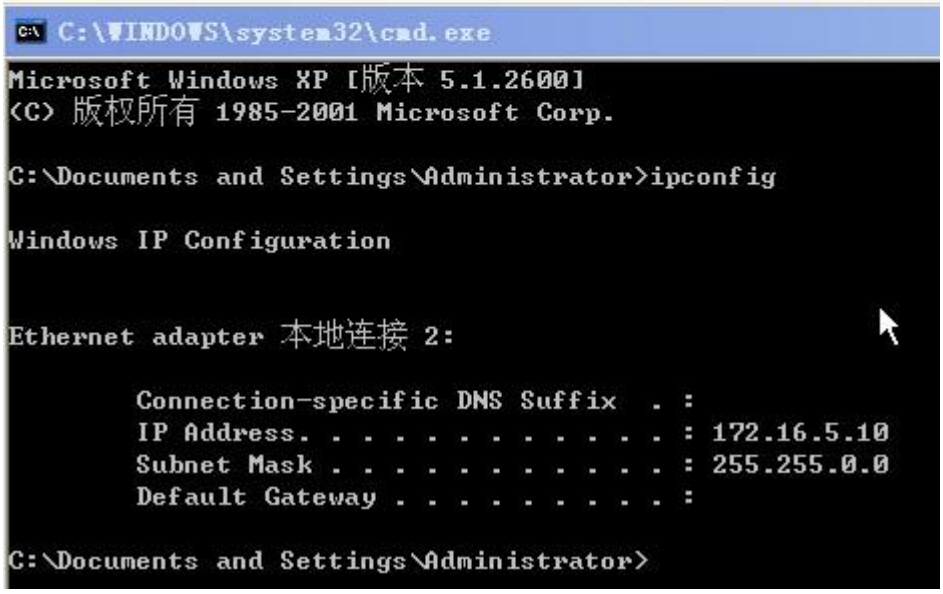
1. 配置 linux 防火墙主机 ip 地址，如下图所示：

```
[root@localhost ~]# ifconfig eth0 172.16.5.20 netmask 255.255.0.0
[root@localhost ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 52:54:00:BD:6A:A3
          inet addr:172.16.5.20  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::5054:ff:febd:6aa3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15277 (14.9 KiB)  TX bytes:490 (490.0 b)
          Interrupt:10

[root@localhost ~]# _
```

2. 配置 windows 主机 ip 地址，如下图所示：





3. 配置 linux 主机防火墙规则，如下图所示：

```
[root@localhost ~]# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
[root@localhost ~]# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p icmp --icmp-type destination-unreachabl
e -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere            icmp echo-request
ACCEPT     icmp --  anywhere             anywhere            icmp echo-reply
ACCEPT     icmp --  anywhere             anywhere            icmp destination-un
reachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@localhost ~]#
```

4. 在此在 windows 主机和 linux 主机上进行相互 ping 测试，测试结果如下图所示：

```
C:\Documents and Settings\Administrator>ping 172.16.5.20

Pinging 172.16.5.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.5.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>
```

windows 主机无法 ping 通 linux 防火墙主机，但是 linux 主机可以 ping 通 windows 主机。

```
[root@localhost ~]# ping 172.16.5.10
PING 172.16.5.10 (172.16.5.10) 56(84) bytes of data.
64 bytes from 172.16.5.10: icmp_seq=0 ttl=128 time=1.18 ms
64 bytes from 172.16.5.10: icmp_seq=1 ttl=128 time=0.243 ms
64 bytes from 172.16.5.10: icmp_seq=2 ttl=128 time=0.166 ms

--- 172.16.5.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.166/0.532/1.188/0.465 ms, pipe 2
[root@localhost ~]# _
```

实验思考

1) 如何在 linux 主机上配置防火墙规则以防止 DDOS 高级
2) linux 主机防火墙处理数据包的顺序是什么