基于 Linux 的防火墙系统

林子杰

摘　要　介绍了防火墙系统的基本概念，提出一种基于 Linux 的防火墙系统，并详细说明了在 Linux 为基础的个人电脑上安装包过滤式防火墙系统的步骤。

关键词　Linux　防火墙　包过滤

An Firewall Based on Linux

Lin Zijie

Abstract　In this paper,we describe the basis of firewall system,and propose a firewall based on Linux。Then we give you some details on setting up an filtering firewall on a Linux based system。

Keyword　Linux　Firewall　Packet Filtering

国际互联网从其产生之时就在安全方面存在着一定的脆弱性，安全性和开放性是一对基本的矛盾[1]。解决网络安全问题的一个有效方法就是在内部网络和外部网络之间设置防火墙。因此，研究防火墙技术，无论从理论上还是实际应用中都具有十分重要的意义。本文根据 Linux 核心本身的“伪装”机制提出了一种基于 Linux 的包过滤技术防火墙系统。

1　防火墙技术

防火墙技术主要分为包过滤技术和代理（Proxy）[3]两大类。包过滤技术，一般作用在网络层（IP 层），主要根据防火墙系统所收到的每个数据包的源地址、目的地址、TCP/UDP 源端口号、TCP/UDP 目的端口号及数据包头中的各种标志位来进行判定，根据系统设定的安全策略来决定是否让数据包通过。

当我们拨号连接上 Internet 后，我们的电脑会被赋予一个 IP 地址，可让其它人回传资料到我们的电脑。入侵者就是用你的 IP 来窃取你电脑上的资料。Linux 所用的“IP 伪装”法，就是把你的 IP 藏起来，不让网络上的其它人看到。当你有一部安装 Linux 的电脑，设定要使用“IP 伪装”时，它会将内部与外部两个网络连接起来，并自动解译由内往外或由外至内的 IP 地址，通常这个动作称为网络地址映射（Network Address Translation，NAT）。内部网络地址可以采用 RFC1597[2]定义的专供网络内部使用“Internet 专用地址”：

10.0.0.0–10.255.255.255　1 个 A 类地址

172.16.0.0–172.31.255.255　16 个 B 类地址

192.168.0.0–192.168.255.255　255 个 C 类地址

这些地址可以通过在 RFC1631[3]中定义的地址映射技术来实现到外部合法 IP 地址的转换。

2　设定 Linux 系统

2.1 编辑内核（Kernel）

首先利用 Linux 版本重新安装 Linux 系统（如 RedHat3.0.3，此后实例均以这一版本为准）。本文以 Linux 2.0.14 的内核设置为基础。根据适当的选项（options）重新编辑内核。以下是在‘make config’内与网络有关的设定。

2.1.1 在 General setup 中设 Networking Support 为 ON。

2.1.2 在 Networking Options 中：

（1）设 Network firewall 为 ON；

（2）设 TCP/IP Networking 为 ON；

（3）设 IP forwarding/gatewaying 为 OFF（除非要用 IP 过滤）；

（4）设 IP Firewalling 为 ON；

（5）设 IP firwall packet loggin 为 ON（不是必要，设了更好）

（6）设 IP:masquerading 为 OFF（不属本文范围）；

（7）设 IP:accounting 为 ON；

（8）设 IP:tunneling 为 OFF；

（9）设 IP:aliasing 为 OFF；

（10）设 IP:PC/TCP compatibility mode 为 OFF；

（11）设 IP:Reverse ARP 为 OFF；

（12）设 Drop source routed frames 为 ON。

2.1.3 在 Network device support 项下：

林子杰　厦门集美大学信息工程学院计算机与通信工程系讲师（361021），主要从事计算机网络、移动通信网络等方面的教学与研究工作。

修改稿收到日期：2000-11-03

(1) 设 Network device support 为 ON

(2) 设 Dummy net driver support 为 ON

(3) 设 Ethernet (10 or 100Mbit) 为 ON

(4) 选择网卡。

现在重新编辑,重新安装内核,重新启动,网卡应在启动的提示中显示。

2.2 设定地址

由于不打算让外部网络进入内部网络的任何部分,因此内部网络的地址可采用前述介绍的 "Internet 专用地址",我们以 192.168.xxx 来作说明。

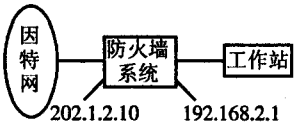

图 1

由于防火墙系统同时身处两个网络(见图 1),因此它能居中传送两边的数据。通过"IP 伪装"设定,防火墙就会转送数据包,并加附实际的 IP 地址送往外部网络(如因特网)。在网卡的外端得设定真正的 IP 地址,在以太网卡的内端设为 192.168.2.1。受保护的内部网络的所有其它电脑均可选用 192.168.2.xxx 中的任何一个作为地址 (从 192.168.2.2 到 192.168.2.254)。在 RedHat Linux 中,得在/etc/sysconfig/networkscripts 目录下增加一个 ifcfg-eth1 档,以便在启动时,通过这个档设定网络和路由表(routing)。ifcfg-eth1 的参数可设定如下:

```
#! /bin/sh
#>>>Device type:ethernet
#>>>Variable declarations:
DEVICE=eth1
IPADDR=192.168.2.1
NETMASK=255.255.255.0
NETWORK=192.168.2.0
BROADCAST=192.168.2.255
GATEWAY=202.1.2.10
ONBOOT=yes
#>>>End variable declarations
```

可试用这些参数通过调制解调器(Modem)与 ISP 自动连接,不妨看看 ipup-ppp 档,如用 Modem 连接上因特网,ISP 会在连接时指定外端的 IP 地址。

3 IP filtering 的设置(IPFWADM)

建立包过滤防火墙,应确认使用的 Linux 版本中是否有 IP Firewall Administration 工具(IPFWADM),若没有可从网上下载下来[4]。首先设定内核的 IP Forwarding 功能,系统应开始转送每一信息。路由表(routing table)应已设定,因此应该可以通往任何地点,从网内可以联到网外,从网外也可进到网内。但是防火墙的作用是不让任何人可以随便进出内部网络。在系统中设定了两套指令(script),对防火墙的 forwarding 和 accounting 作了规定。系统在运行/etc/rc.d 时调用这两套指令,因此在系统启动时就对系统作了设置。Linux 的内核自设转送一切信息的 IP Forwarding 系统。因此,防火墙的指令应首先禁止一切进入系统的权利,清除上次运行后留下的任何 ipfw 规则。下面的指令可以达到这项目的。

```
#
#setup IP packet Accounting and Forwarding
#
#Forwarding
#
#By default DENY all services
ipfwadm -F -p deny
#Flush all commands
ipfwadm -F -f
ipfwadm -I -f
ipfwadm -O -f
```

通过以上设定,一切都被屏蔽在外面。根据实际需要,设定相应的功能。下面的例子可作参考。

```
#Forward email to your server * 转送电子邮件到服务器
ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535-D 192.1.2.10 25
#Forward email connections to outside email servers * 将电子邮件连到网络外的电子邮件服务器
ipfwadm -F -a accept -b -P tcp -S 196.1.2.10 25 -D 0.0.0.0/0 1024:65535
#Forward Web connections to your Web Server * 将 Web 连到 Web 服务器
/sbin/ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 1024:65535-D 196.1.2.11 80
#Forward Web connections to outside Web Server * 将 Web 连到外界 Web 服务器
/sbin/ipfwadm -F -a accept -b -P tcp -S 196.1.2.* 80 -D 0.0.0.0/0 1024:65535
#Forward DNS traffic * 转送 DNS 信息
/sbin/ipfwadm -F -a accept -b -P udp -S 0.0.0.0/0 53 -D196.1.2.0/24
```

如果想知道通过防火墙的信息来往情况,下列指令会统计所有数据包。

```
#Flush the current accounting rules
ipfwadm -A -f
```

(下转第 27 页)

其中 tID 将作为要创建的多媒体定时器的标识 ID。

在 implimentation 定义一个 CallBack 过程：

```
procedure CallBack (uTimerID,uMessage:UINT;dwUser,dw1,dw2:
DWORD);stdcall;// stdcall 在这里是不能省
begin
Inc(i);
end
```

放一个 Timer 控件 Timer1 (Enabled 的属性设置为 false)和两个 Edit 控件，定义 Timer1 的 OnTimer 事件为：

```
procedure TForm1.Timer1Timer(Sender:TObject);
begin
Inc(j)
Edit1.Text:=IntToStr(i);// 多媒体定时器的执行结果
Edit2.Text:=inttostr(j);// Timer 的执行结果
end ;
```

用一个 SpinEdit 来设置定时器的周期，添加两个 Button 控件，Button2 的 Enabled 设置为 false。Button1,Button2 的 Onclick 分别为：

```
procedure TForm1.Button1Click(Sender:TObject);
var Intv:integer;
begin
Intv:=SpinEdit1.Value;
if Intv<1 then Intv:=1000;// 值小于 1，就把周期设为 1 秒
Timer1.Interval:=Intv;
Timer1.Enabled:=true;// 激活 Timer1
if tID=0 then tID:=TimeSetEvent (Intv,1,CallBack,0,1);// 创建一个多媒体定时器，回调过程为 CallBack
Button1.Enabled:=false;
Button2.Enabled:=true;
end;
procedure TForm1.Button2Click(Sender:TObject);
begin
TimeKillEvent(tID);// 关闭多媒体定时器
Timer1.Enabled:=false;// 关闭 Timer1
Button1.Enabled:=true;
Button2.Enabled:=false;
tID:=0;
i:=0;
j:=0
end;
```

如果在创建多媒体定时器后，没有关闭它就退出程序，再次执行时，有时会有意外结果，可以定义 Form1 的 OnDestroy 来避免：

```
procedure TForm1.FormDestroy(Sender:TObject);
begin
if tID>0 then TimeKillEvent(tID);
end;
```

运行程序，设定好周期后，单击 Button1 就可以观察两个定时器的工作情况。通过改变周期，定时器工作时拖动窗口等，就会发现多媒体定时器与 Timer 相比的优势了。

上面程序只是在 Delphi 中简单实现了多媒体定时器，其实只要编制合适的 CallBack 过程，可以用它来完成诸如数据采集、多媒体播放的许多实时性要求高的工作。

（上接第 13 页）

```
#Accounting
/sbin/ipfwadm -A -f
/sbin/ipfwadm -A out -i -S196.1.2.0/24 -D 0.0.0.0/0
sbin/ipfwadm -A out -i -S 0.0.0.0/0 -D 196.1.2.0/24
sbin/ipfwadm -A in -i -S196.1.2.0/24 -D 0.0.0.0/0
sbin/ipfwadm -A in -i -S 0.0.0.0/0 -D 196.1.2.0/24
```

至此，包过滤防火墙设置完毕。

4 结 束 语

防火墙技术作为目前用来实现网络安全措施的一种主要手段，它主要是用来拒绝未经授权的用户访问，阻止未经授权的用户存取敏感数据，同时允许合法用户不受妨碍地访问网络资源，如果使用得当，可以在很大程度上提高网络安全性能。但是没有一种技术可以百分之百解决网络上的信息安全问题，基于 Linux 的包过滤防火墙同样存在安全隐患：如无法处理应用层发起的攻击，如基于电子邮件的攻击；无法防止来自内部网络的攻击。因此网络安全单靠防火墙技术是不够的，还需要有一些其它技术和非技术的因素要考虑，比如信息加密技术、制定法规、提高网络管理使用人员的安全意识等。

参 考 文 献

1. Andrew S Tanenbaum.Computer networks.Third edition. USA:Prentice Hall,1996

2. IETF.RFC1597:Address allocation for private internets. http://NIC.DDN.MIL/internet/documents/rfc/,Mar 1994.

3. IETF.RFC1631:The IP network address translator (NAT).http://NIC.DDN.MIL/internet/documents/rfc/,May 1996.

4. http://www.xos.nl/linux/ipfwadm/