基于Linux的路由器和防火墙技术

肖 明 胡金柱 肖 毅
(华中师范大学计算机科学系 电子与计算机研究所 武汉 430079)

摘 要 随着Internet应用的普及，其安全性问题也日渐突出。本文首先介绍Internet常见攻击原理与防范及当前防火墙采用的一般技术，并以S.u.S.E公司的Linux5.1为例，介绍防火墙和代理服务器的配置。

关键词 防火墙 代理服务器 Linux操作系统

1 Internet常见攻击与防范

Internet的安全问题主要源于以下几方面：

- 各种应用程序中包含的Bug和漏洞。
- 网络管理员及用户的安全意识薄弱。
- TCP/IP协议本身在其安全性方面的缺陷。
- 社会因素：如公众对黑客才智的赞赏和信息间谍的存在等。

网络攻击大致有以下几种：

1)特洛伊木马(Trojan Horse)

特洛伊木马是一个独立的程序，看起来完成某一功能，实际执行另一功能。比如做一个假的登录界面来骗取他人登录时的帐号和口令，即可进入系统。由于系统中程序众多，木马的隐蔽性强，管理器很难发现、防范特洛伊木马，关键是要配置好系统，防止系统被入侵，并要慎用免费软件。

2)嗅包(Sniffing)

嗅包是利用以太网的广播特性CSMA/CD(carrier Sense Multiple Access with Collision Detect：带碰撞检测的载波侦听多路访问协议)，用软件在原以太设备上侦听或通过将网络接口置为混杂模式(Promiscuous Mode)接收进出本网段的所有MAC包。由于Internet上的信息通常是明文传输的，当发现了满足一定条件的

收稿日期：1998年11月3日

防火墙获取。

信元加/解密、密钥捷变　采用虚电路级加密的方式加密信元，在协商好安全参数，建立虚电路后，在该虚电路上传输的所有信元净荷在进入WAN之前由本模块进行加密处理。信元到达后，密钥捷变进程迅速查找Cache中相应虚电路的会话密钥，然后使用DES算法、以Counter模式对信元净荷进行加密，得到的密文传送给WAN模块，目的端防火墙的解密过程与之相似。信元的DES加密用硬件ASIC芯片实现，选取6块加密块长度为64bits的加密芯片，利用Count模式，可以使6个芯片同时处理密钥，并行加密信元的48个bytes(384bits)，使用6块100Mb/s吞吐率的DES加密ASIC芯片并发处理，可以满足622Mbps的传输率的要求。

同步信元和完整性检查部分　考虑信息流是AAL5的情形，AAL5-PDU不易在ATM层判断其结束边界，因而我们定义一种新的OAM F5信元来进行同步(在信元头标增加一新类型)，每100个信元后跟一个OAM F5同步信元。远端ATM防火墙在收到同步信元后重置加密计数器的初始向量IV，开始新的一轮的加密。完整性检查部分在ATM层完成，利用同步信元的净荷传送完整性检验值，即每100个信元明文的校验和经过哈希计算，并用会话密钥加密后，和同步OAM一起发送给目的端防火墙，目的端的完整性检查和同步处理同时进行。一旦发现信元在途中丢失或受到破坏，就要求源端重传。

模型中流量统计以信元为单位，一条虚电路建立时，在内存中的流量统计表中登记上他的ATM地址VPI/VCI以及QOS参数，就将登记表中的相应值加一，统计内存区的大小达到一定的门限值，就用SNMP Trap给网管工作站，同时清空流量统计表。

配置管理部分　用GUI操作界面在网管工作站上完成访问控制中的过滤规则和安全策略的设置，配置结果通过SNMP协议安装到防火墙上。

5 结论与展望

本文在分析ATM网络攻击种类和CLIP的安全漏洞的基础上，提出了一个基于CLIP模式的安全模型。但在软，硬件的具体实现上，还要更进一步的研究。ATM网络是新兴的技术，各种标准和协议都在制定，完善之中，抓住这个机遇，推出我们自己的产品，定能占领未来通信领域的广阔市场。

参考文献

1 Uyless Black. ATM:Foundation For Broadband Networks. 清华大学出版社, Prentice Hall, 1998. 4
2 Uyless Black. ATM:Signaling in Broadband Networks. 清华大学出版社, Prentice Hall, 1998.4
3 郭 戈. ATM安全系统设计与实现. 武汉大学硕士论文, 1998.5

包，则可将其内容记入一文件或进行其他操作(如劫持、拒绝服务等)。通过捕获FTP或TELNET包的前128个字节即可实现。嗅包是黑客攻击网络的主要方法之一。

3)冒充(Spoofing)

冒充是指一主机以另一主机的名义进行操作。被冒充的信息包括IP地址、域名，路由信息等实现。最常见的是冒充内部网主机地址而试图通过代理进入内部网，可在路由器上滤掉所有目的地址和原地址是内部地址的包来防范这类冒充。

4)拒绝服务攻击(Denial of Service)

拒绝服务攻击能使服务器不能为客户提供良好的服务。这类攻击主要有：逻辑炸弹，ICMP包攻击，TCP的序列数攻击，ICMP包洪泛，NFS和NIS攻击。

2　防火墙的概念

防火墙是设置在内部网络与Internet之间的一个或一组系统。用以实施两个网络之间的访问控制和安全策略。拒绝服务攻击从结构上可分为屏蔽路由器(Screened Router)，双穴主机(Dual_home Host)，混合网关(Hybrid Gateways)等，从运行机制上，主要有过滤型防火墙(Filtering Firewall)，电路层网关(Circuit Gate Way)，代理服务器(Proxy Server)。

这里介绍两种常用的方法：过滤型防火墙和代理服务器。

1)过滤型防火墙

也称为分组过滤，它是基于路由的技术，通常由分组过滤路由器对IP分组进行选择，允许和拒绝特定的分组通过。过滤一般是基于一个IP分组的IP地址和服务端口号等域进行的。分组过滤的优点是速度快、透明性好，但缺乏用户审计(Audit)和日志(Log)信息，缺乏用户认证机制，安全性较差。不过分组过滤技术是实现防火墙系统的灵活而有效的手段。

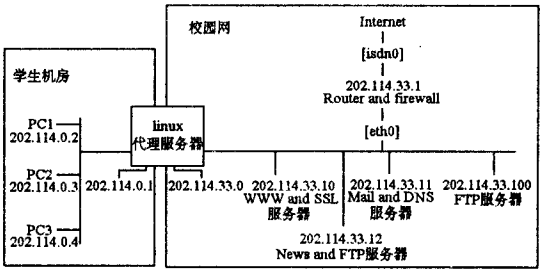
2)代理服务器

该技术是由一个高层的应用路由器作为代理服务器，接受外来的应用连接请求，进行安装检查后，再与被保护的网络应用服务器连接，使得外部服务用户可以在受控制的前提下使用内部网络的服务。同样，内部网络到外部网络的服务连接也可以受到监控。代理服务可大大降低分组过滤规则的复杂性，并可实施用户认证，详细的用户日志和审计跟踪功能及对具体协议的过滤(如阻塞Java和JavaScript)。代理防火墙具有更高的灵活性和安全性，但可能影响网络性能，可能对用户不透明，却是分组过滤技术的有效补充。

3　基于Linux的路由器和防火墙配置

随着Internet应用的日益普及，免费网络操作系统Linux受到越来越多的网络爱好者的关注。通过简单的安装，人们就可以获得Linux提供的多项网络服务，诸如Web服务、E_mail服务、FTP服务、Gopher服务、UseNet服务等。同时，它还提供了UNIX操作系统所具有的X windows系统Xfree86软件包。可以说，Linux已经具备了网络服务器的所有功能。在此，笔者想结合自己的工作经验，谈谈将Linux作为路由器连接两个不同的网段，并在其上配置防火墙和代理服务器，以实现机房内网络的存取访问控制和流量统计的功能。

要想使一台装有Linux的PC具有路由器的功能，首先要进行硬件配置。如下图所示，名为Linux的PC上装有Linux系统，并配有两块网卡，每块网卡连接一个不同的网段，该机作为路由器在两个网段间转发IP数据包。为了防止两块网卡的中断发生冲突，需要网卡驱动程序将中断分别设为不同值。笔者在实践时将其中断号和I/O地址分别设置为：3,0x300H和5,0x340H。



硬件配置完毕，还需要在软件上做相应的配置。以笔者使用的S.u.S.E.公司的Linux5.1为例，在通常的安装模式下，Linux5.1系统具备路由器和防火墙的功能，但需配置确定的选项，用户可选择系统缺省值。

```
networking options  --->
[*]Network firewalls              /*内核是否支持防火墙*/
[ ]Network aliasing               /*内核是否支持网络别名*/
[*]TCP/IP networking              /*主机是否连接TCP/IP网络*/
[*]IP:forwarding/gatewaying /*主机是否转发数据库或作为网关*/
[ ]IP:multicasting          /*是否在TCP/IP网络内设置IP广播*/
[*]IP:firewalling           /*是否在TCP/IP网络内设置防火墙*/
[ ]IP:firewall packet logging        /*是否在防火墙上登记数据包*/
[*]IP:masquerading(EXPERIMENTAL)  /*是否将主机设置为代
                                    理*/
[*]IP:transparent proxy support (EXPERIMENTAL)
[ ]IP:always defragment
[*]IP:accounting                     /*是否对数据包计帐*/
[ ]IP:optimize as router not host    /*是否将主机设置为路由器*/
<>IP:tunneling
[ ]IP:multicast routing(EXPERIMENTAL)    /*路由器是否向外广
                                           播路由信息*/
<>IP:aliasing support
[ ]IP:PC/TCP compatibility mode
<>IP:Reverse ARP
[ ]IP:Disable Path MTU Discovery (normally enabled)
[*]IP:Drop source routed frames
```

[ ]IP:allow large windows (not recommended if<16Mb of memory)

<>The IPX protocol

<>Appletalk DDP

[ ]Amateur Radio AX.25 Level 2

[ ]Bridging

[ ]Kernel/User network link driver

因为我们要将此主机配置为路由器，并在其上设置防火墙，故对这些选项统一选"*"。

需对两块网卡的TCP/IP部分进行设置，使其能有效地连接两个不同的网段，并能在两个网段进行IP数据包的转发。设置步骤为(其中的参数依图中所示)。

1) 对于NE2000兼容的网卡，修改"/etc/rc.config"文件；

```
ne  io=0x300，0x340          /*识别两块网卡*/
```

2) 修改"/etc/rc.config"文件，设置两块网卡的IP地址、掩码及到两块网卡的路由信息；

```
IPADDR="202.114.33.8"
NETWORK="202.114.33.0"
BROADCAST="202.114.33.255"
IPADDR1="202.114.0.1"
NETWORK1="202.114.0.0"
BROADCAST1="202.114.0.255"
NETMASK="255.255.255.0"
/sbin/ifconfig eth0 ${IPADDR} broadcast${BROADCAST} netmask${NETMASK}
/sbin/ifconfig eth1 ${IPADDR1} broadcast${BROADCAST1} netmask${NETMASK}
/sbin/route add_net ${NETWORK} netmask${NETMASK} eth0
/sbin/route add_net ${NETWORK1} netmask${NETMASK} eth1
```

3)修改"etc/rc.config"文件，设置防火墙和代理服务器。

配置路由器和防火墙：

```
FW_START="YES"
FW_LOCALNETS="202.114.33.0/255.255.255.0" /*局域网列表*/
FW_FTPSERVER="202.114.33.12  202.114.33.100"
FW_WWWSERVER="202.114.33.10"
FW_SSLSERVER="202.114.33.10" /*设置Secure_Socker_WWW服务器*/
FW_SSLPORT=443
FW_MAILSERVER="202.114.33.11"
FW_DNSSERVER="202.114.33.11"
FW_NNTPSERVER="202.114.33.12"
FW_NEWSFEED="news.ccnu.edu.cn"
FW_WORLD_DEV="eth0"
FW_INT_DEV="eth1"
FW_TCP_LOCKED_PORTS="1:1023"
FW_UDP_LOCKED_PORTS="1:1023"
```

配置代理服务器：

```
MSQ_START="YES"
MSQ_DEV="eth1"
MSQ_NETWORKS="202.114.0.0"
MSQ_MODULES="ip_masq_cuseeme ip_masq_ftp ip_masq_irc ip_masq_quake ip_masq_raudio ip_masq_vdolive"
```

4)在"etc/lilo.conf"文件中增加一行，使其在启动时识别第二块网卡。

```
append="ether=1,0x340,eth1"
```

5)在"etc/rc.config"文件中增加几行，使其进入etc/fw-friends中不能进入局域网。

```
# /etc/fw-friends
host.ccnu.edu.cn
news.ccnu.edu.cn
```

完成上面的设置后，应重新启动计算机，系统会识别到两块网卡，并按照"/etc/rc.config"文件中的说明对网卡的IP地址、掩码进行设置。启动完成后，以超级用户root的身份进入系统，键入下面的命令即可看到关于网卡和路由的信息。

```
#ifconfig          /*显示网卡的详细信息*/
#route             /*显示系统的路由表*/
```

笔者曾将学生机房局域网内的PC通过Linux路由器与校园网相接，并进一步通过校园网进入Internet。此外，笔者又在Linux路由器上配置了防火墙。实践证明，防火墙有效地控制住了学生对非法IP地址的访问，并成功地记录下每个IP地址的网络流量，为计费和网管提供了依据。Linux的防火墙和代理配置可以通过简单的命令逐条进行，也可编写shell程序放到系统的启动目录下自动执行。其命令格式非常简单，现举例如下：

```
# /sbin/init.d/firewall start
# /sbin/init.d/masquerade start   /*激活firewall 和 masquerade */
# ipfwadm-A                /*对通过路由器的所有数据包进行计帐*/
# ipfwadm-I -a accept -S 162.105.0.0/16  /*接受来自162.105.0.0网络的所有数据包*/
# ipfwadm-O -a reject -S 2l0.32.0.0/12   /*丢掉发往2l0.32.0.0网络的所有数据包，并发送拒绝信息包给请求者*/
```

读者可根据实际需要进行防火墙和代理的配置，以达到期望的效果。

参考文献

1 Installation, Configuration and First Steps with S.u.S.E. Linux5.1 9th edition 1997,11,S.u.S.E.Inc

2 Scott Fuller, Kevin Pagan著，董 春，张红雨，刘英杰译. Intranet防火墙，电子工业出版社，1997

3 Stang. DJ著，程佩青译. 计算机网络安全奥秘. 电子工业出版社，1994

4 Phil Cornes著，童寿琳等译. Linux从入门到精通. 电子工业出版社，1998.7

5 Dee-Ann LeBLanc著，齐 曼，李茂贞等译. Linux的Internet站点建立与维护. 清华大学出版社 西蒙与舒斯特国际出版公司，1997.1