基于 Linux 实现局域网共享 IP 访问 Internet

郑沛峰　谢瑞和
(华中科技大学电子与信息工程系,武汉 430074)
E-mail:zhpfmail@263.net

摘　要　文章旨在介绍如何设置一个基本的 Linux 防火墙系统，允许局域网用户通过 IP 伪装使用一个 IP 上网联入 Internet,在防火墙上对所有局域网进出的封包加工处理,使外界认为所有的封包和请求都是防火墙发出的,觉察不到内部局域网的存在。运行防火墙系统可以提升整个网络的安全性,保护内部局域网不会轻易受到外界的攻击。在防火墙上可以控制内部网络对 Internet 的访问权限,禁止内部网络访问一些受限制的站点。

关键词　Linux　防火墙　IP 伪装　Internet

文章编号 1002-8331-(2002)06-0169-03　**文献标识码** A　**中图分类号** TP311

A Implemantation of Connecting Local Network with Internet Sharing one IP Based on Linux System

Zheng Peifeng　Xie Ruihe
(Dept.of E&I,HuaZhong Univ.of Science and Technology,Wuhan 430074)

Abstract: This paper introduces how to set up a basic linux firewall system,which permit local users to be connected with internet using one IP through IP_Masquerade.The firewall analyses and processes all packages traversing it,which seems that the firewall send and receive all messages with the hosts outside not perceiving the interior network.Running the firewall system can promote the whole network security and protect interior local network from being attacked easily.The administrator can control access of interior network to internet and forbid it to visit some limited sites.

Keywords: Linux,firewall,IP_Masquerade,Internet

1　引言

随着 Internet 的飞速发展，越来越多的人连入 Internet,IP 的地址非常紧缺，不可能为每个上网的计算机都分配一个 IP 地址。许多单位仅仅拥有一个 IP 地址,为了使单位内部的计算机都能联入互联网,就必须采用局域网共享 IP 技术,使得对外界看来整个局域网就如同拥有一个 IP 的一部计算机。

免费的 Linux 操作系统由于其强大的网络服务和管理功能,在网络方面得到了广泛的应用。通过安装 Linux 操作系统,人们可以获得很多的网络服务如 Web、FTP、E_mail、Gopher 等。同时,它还提供非常友好的图形管理界面 XWindows 系统。尤其,它能为低配置的计算机提供高效的网络服务,这使得其他的操作系统如 Windows NT 相形见绌。

通过在 Linux 主机中运行防火墙软件,可以使局域网通过一个 IP 地址连入 Internet。在防火墙中按照一定的规则,对进出防火墙的包进行处理,允许一些或所有的内部网机器出入防火墙访问 Internet。对外界而言,所有局域网的包都是从 Linux 主机发出,而觉察不到防火墙内部网络的存在。

2　设计思路

防火墙是设置在内部局域网与 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。通常,防火墙的实现有两种方式：基于应用层的 Socket 协议和基于网络层的分组过滤。应用层的防火墙可以针对用户设置密码和访问权限,能实现较为复杂的功能,缺点是速度慢,必须对每一种应用设置权限,要求内部网的计算机支持 socket 协议。常见的这种防火墙有 UNIX 的 Squid 和 Windows 的 WinGate。网络层的防火墙对所有进出的 IP 包基于它们的 IP 地址、网络协议和服务端口等域进行过滤,速度快、透明性好,内部局域网感觉不到防火墙的存在,如同直接接入 Internet,缺点是无用户权限的设置,在同一台计算机上的不同用户权限相同。网络层的分组过滤是一种实现防火墙的灵活而有效的方式。

IP 伪装是 Linux 中不断发展的一项网络功能，包含在 2.0 以后的版本中，支持所有常见的网络协议，如 telnet、ftp、irc、news、realaudio 等。通过设置网络层防火墙,对局域网内部的计算机通过防火墙访问 Internet 的进出包进行 IP 伪装,这使得一些计算机可以隐藏在防火墙后面存取 Internet 信息，从而将没有合法的公共网络地址的计算机连入 Internet。Linux 2.2 内核用 ipchains 代替了 2.0 内核中的 ipfwadm 支持新的防火墙配置方式。在 Redhat 6.0 及其以后的版本中,ipfwadm 不能再用了。

一般而言实现 Linux 防火墙功能有两种策略,一种是首先全面禁止所有的输入/输出/转发包,然后根据需要逐步打开所要求的各项服务,这种方式最安全,但必须全面考虑到自己所要使用的各项服务功能,不能有任何遗漏,如果对要实现的某种服务和功能不能清楚地知道应该打开哪些服务和端口,那会比较麻烦；另一种方式是首先默认打开所有的输入/输出包,对转发包,不必打开,因为内部网段用保留地址,不能直接与

作者简介：郑沛峰,硕士,主要研究方向为多媒体网络通信。谢瑞和,教授,主要研究方向为多媒体网络通信。

互联网交换数据，是通过用 IP 伪装的方式透明地进行交换数据的)，然后禁止某些危险包如 IP 欺骗包，广播包，ICMP 包等，对于应用层服务象 http，sendmail，pop3，ftp 等，若不打算提供某些服务，就不要启动它，或者根本就不要安装，这种方式虽然没有第一种方式安全，但是比较方便，容易配置，用户不必过多地了解该如何打开一种服务 如 FTP)所需要执行的 ipchains 命令细节就能配置一个比较安全的防火墙系统。后文就采用第二种方式，利用 "IP 伪装 "(IP Masquating)和 Kernel 2.2.X 使用的 IPChains 来构造网络层防火墙，使内部局域网共享 IP 连入 Internet。它的主要步骤如下：

()在一台装有 2.2 及其以上核心的 Linux 主机上安装两个网络界面，这两个界面可以是两个网卡、两个 Modem，也可以是一个网卡。为每个网络界面分配一个 IP 地址，一个是内部局域网的私有网络地址，用于与内部网络通讯；另一个是合法的公共网络地址，用于与 Internet 通讯；

()在 Linux 主机上安装网络层的防火墙，设置输入、转发和输出防火墙的规则；

()设置局域网内计算机的网络。

整个网络联接如图 1 所示。

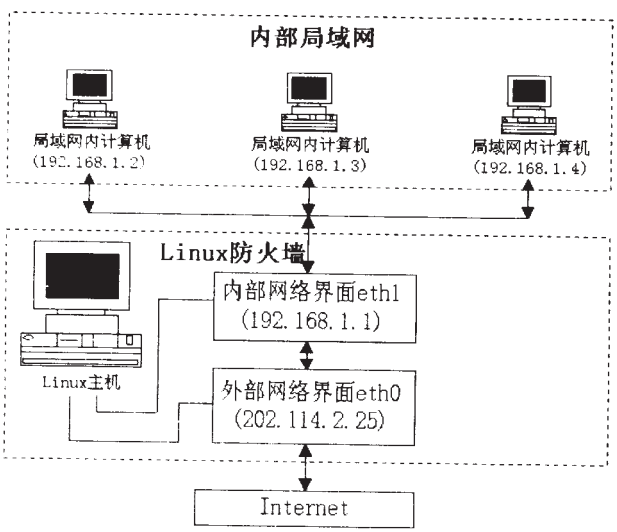

图 1 网络联接图

内部局域网使用的是私有网络地址，根据 RFC1597 中的规定，以下三段地址保留给私有网络使用：10.*.*.*，172.16.*.* 与 192.168.*.*。这些地址不会在公共网络中出现，但是每个网络保留一个网络地址和广播地址不能分配给任何计算机使用。在文中为了说明方便，在 Linux 主机上安装两个网卡，eth0 为外部网段网卡接口，eth1 为内部网段网卡接口，内部网络使用 192.168.1.*，公共网络地址 即 eth0 地址)为 202.114.2.25，Linux 操作系统采用 Redhat6.1。

局域网中的计算机可以采用任何操作系统，执行所有常见的网络协议。这是因为网关上的防火墙规则工作于网络层，局域网的访问请求和响应均在应用层上完成。防火墙重写经过其转发的包，它们看起来就象从防火墙自身发出，并且重写返回的包使他们看起来是发往原来的局域网内部的申请者。Internet 对局域网的计算机而言，如同透明。

具体的网络设置如下：

()防火墙主机的 eth1 地址为 192.168.1.1，局域网中的计算机的网络地址为 192.168.1.*，不含 192.168.1.0 内部网的网络地址)和 192.168.1.255 内部网的广播地址)；

()私有网络上机器的默认路由 别名网关)设定为指向防火墙机器的内部网络地址；

()私有网络的 DNS 需要正确设置，设定为防火墙机器的内部网络地址 需要在防火墙机器上运行 DNS 代理服务)。

3 防火墙规则设置

使用 ipchains 配置的防火墙规则可以分成四类：IP input 链、IP output 链、IP forward 链、user defined 链。一个防火墙规则指定包的格式和目标。当一个包进来时，核心使用 input 链来决定它的命运。如果它通过了，那么核心将决定包下一步该发往何处。假如它是送往另一台机器的，核心就运用 forward 链。如果不匹配，进入目标值所指定的下一条链，那有可能是一条 user defined 链，或者是一个特定值：ACCEPT，DENY，REJECT，MASQ，REDIRECT 等。ACCEPT 意味着允许包通过，DENY 扔掉包就象没有收到过一样，REJECT 也把包扔掉，但 假如它不是 ICMP 包)产生一个 ICMP 回复来告诉发包者，目的地址无法到达 请注意 DENY 和 REJECT 对于 ICMP 包是一样的)。MASQ 告诉核心伪装此包，它只对 forward 链和 user defined 链起作用，想让它起作用，编译核心时必需让 IP Masquerading 起作用。REDIRECT 只对 input 链和 user defined 链起作用。它告诉核心把无论应送到何处的包改送到一个本地端口。只有 TCP 和 UDP 协议可以使用此指定。想让它起作用，编译内核时，必须让 CONFIG_IP_TRANSPARENT_PROXY 起作用。

下面是一个包进入一台机器的完整路径：

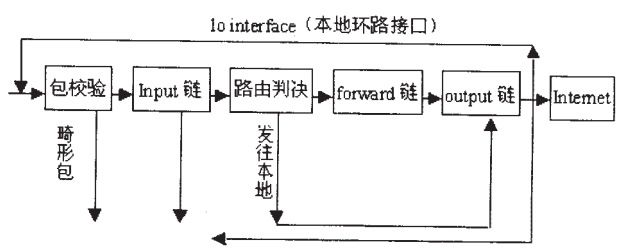

图 2

当安装好了核心以及其它需要的组件，完成了内部计算机的地址、网关和 DNS 的设定后，就可以用 ipchains 来设置具体的防火墙规则。

```
# 刷新防火墙的转发规则
/sbin/ipchains -F forward
# 允许局域网内的 IP 包转发
echo "1" > /proc/sys/net/ipv4/ip_forward
/sbin/ipchains -A forward -j MASQ -s 192.168.1.0/24 -d
0.0.0.0/0 -i eth0
```

这就可以使局域网没有限制地访问所有的 Internet 站点。

也可以对每个局域网地址分别进行设置和封锁一些站点。例如允许 192.168.1.111 和 192.168.1.254 能访问 Internet，但 192.168.1.254 不能访问 202.114.2.1

```
/sbin/ipchains -A forward -j MASQ -s 192.168.1.111/32 -d
0.0.0.0/0 -i eth0
/sbin/ipchains -A forward -j MASQ -s 192.168.1.254/32 -d !
202.114.2.1/32 -i eth0
```

提供对 DHCP 或 BOOTP 的支持：

```
#The "bootp_client_net_if_name" should be replaced the name of
```

the link that the

#DHCP/BOOTP server will put an address on to.This will be something like "eth0","eth1".

/sbin/ipchains -A input -j ACCEPT - i bootp_clients_net_if_name -s 0/0 67 -d 0/0 68 -p udp

为了网络安全,还有必要封掉一些有危险的包例如:

禁止 IP 欺骗

/sbin/ipchains -A input -j DENY -i eth0 -s 192.168.0.0/16

/sbin/ipchains -A input -j DENY -i eth0 -d 192.168.0.0/16

/sbin/ipchains -A output -j DENY -i eth0 -s 192.168.0.0/16

/sbin/ipchains -A output -j DENY -i eth0 -d 192.168.0.0/16

/sbin/ipchains -A input -j DENY -i eth0 -s 202.114.2.25/32

/sbin/ipchains -A output -j DENY -i eth0 -d 202.114.2.25/32

禁止来自或发向本地环路接口的包

/sbin/ipchains -A input -j DENY -i eth0 -s 127.0.0.0/8

/sbin/ipchains -A input -j DENY -i eth0 -d 127.0.0.0/8

/sbin/ipchains -A output -j DENY -i eth0 -s 127.0.0.0/8

/sbin/ipchains -A output -j DENY -i eth0 -d 127.0.0.0/8

最后,在 Linux 主机的/etc/rc.d/目录下创建一个 script 叫 rc.firewallrules 来保存防火墙规则 执行 #chmod u+x rc.firewallrules 确保为可执行文件),然后在/etc/rc.d/rc.local 中加入一行/etc/rc.d/rc.firewallrules,以确保每次机器重新启动后即运行所设定的各项防火墙规则。限于篇幅具体的防火墙设置从略。

4 结束语

通过设置的防火墙,使整个局域网共享一个 IP 地址连入 Internet,有效地解决许多单位和用户 IP 地址不足的困难。这种防火墙机制虽然比较简单,但可抵御除最高级的黑客攻击外的绝大部分的网络攻击,既为您的上网提供方便,又为网络安全提供一定保障。 (收稿日期:2001 年 3 月)

参考文献

1.Linux Firewall HOWTO

2.Linux Kernel HOWTO

3.Linux IP-Masquerade HOWTO

4.陈向阳,方阳编著.Linux 实用大全[M].科学出版社,1999

5.Scott Fuller,Kevin Pagan 著.董春,张红雨,刘英杰译.Intranet 防火墙[M].电子工业出版社,1997

6.Dee Ann LeBLanc 著.齐曼,李茂贞等译.Linux 的 Internet 站点建立与维护[M].清华大学出版社,西蒙与舒斯特国际出版社,1997

(上接 158 页)

总重传时延	$D_{retransmition}$
节点接口时延	$T_{interface}$
线路传输时延	T_{cable}
交换机处理时延	T_{spc}
视频服务器处理时延	$T_{server-pro}$

现假设在中型 VOD 系统中,用户终端重传请求包为 64Byte,从用户终端到视频服务器经过 2 根 100m 5 类电缆,2000m 光缆,两个交换机,视频服务器发送数据包为 1518Byte,视频服务器的网络接口满负荷运行,则各时延参数值如下表所示:

$T_{interface}$	250 ns
T_{cable}	570 ns
$T_{optical}$	10000 ns
$T_{spc-64Byte}$	5120 ns
$T_{spc-1518Byte}$	15180 ns
$T_{server-pro}$	21 ms

由上表可得总重传时延为:

$$D_{retransmition}==4*T_{interface}+4*T_{cable}+2*T_{optical}+2*T_{spc-64Byte}+2*T_{spc-1518Byte}+T_{server-pro}==21.064\text{ms} \quad (9)$$

从上述分析可以看出,在总重传时延中,由网络接口、传输线路、交换设备产生的时延是微不足道的 us 级,而视频服务器处理时延则是 ms 级的。在用户终端设置 512Kbyte 的数据接收缓冲区,并采用 70%预充机制,重传时限是非常宽裕的。

5 两种协议的比较

根据上述数据结果可知,从网络容量的角度来讲,由于 TCP 协议方式下的 S_{client} 较大,而 L_{Frame} 较小,因此其网络容量要比 UDP 协议小,在 100M Bit/s 的总线型以太网上,两者的差距约为 7 个 MPEG1 型用户。但是,如果网络采用以以太网交换机为核心的星形拓扑结构,并合理地分配各冲突域内的用户终端数,差距会有所减小。

在时延方面,根据测试结果及实际观察证明,在中小型 VOD 系统中,TCP 协议实现方式完全可以满足所要求的业务质量。尽管 TCP 协议的确认机制会引入一定的时延,但对于 VOD 业务来讲,这并不能构成拒绝采用该协议的理由。同时,如果采用合理的设计,这一瑕疵更是微不足道的。

从对系统其他功能模块的影响来看,采用 TCP 协议,流量控制和丢包重传等工作均由底层的操作系统来完成,而采用 UDP 协议,则必须由上层的用户线程来完成,从而增加了视频服务器的负担。与 TCP 方式相比,其视频服务器的容量将有所下降。

在实现方式方面,已十分成熟的 TCP 协议提供了完备的协议功能,具有很高的可靠性和健壮性;同时,它使设计者无需为流量控制和丢包重传等繁琐的设计而分忧,比较易于实现。而采用 UDP 协议实现,设计者必须自行设计、实现各项协议功能。这将给系统开发带来一定的难度和较大的工作量,这也将意味着开发投资的增加;同时,还要进行较长时间的实践考验、改进、再实践的过程,以达到日趋完善,这将意味着开发周期的延长。

6 结论

根据上述分析笔者认为,在基于以太网的 VOD 系统中,TCP 协议实现方式是完全可行的。从网络结构来讲,TCP 实现方式适用于以交换机为核心的星形网络;从系统规模来讲,它比较适合于中小型规模的 VOD 系统;从软件开发方面来讲,它可以作为一种投资少、见效快的短期实现方式。

(收稿日期:2001 年 3 月)

参考文献

1.TANENBAUM A.Computer Networks[M].3rdEd,Prentice Hall Inc

2.COMER D E.Internetworking With TCP/IP,Volume 1:Principles,Protocols,and Architecture[M].Englewood Cliffs,New Jersey:Prentice-Hall

3.陆传赉.排队论[M].北京邮电大学出版社,1994

4.逯昭义,王思明.计算机通信网信息量理论[M].电子工业出版社