基于Linux包过滤的防火墙技术及应用

何海宾

(西华大学能源与环境工程系 成都 610039)

【摘要】讨论了Linux操作系统内核的Ipchains软件包工作原理。利用Ipchains中的输入链、输出链、转发链和自定义链等防火链，通过设置一系列规则，过滤被主机接收、发送或转发的数据包或主机从一个网卡转发到另一个网卡的数据包，实现根据源地址、目的地址、协议号等信息控制访问，企业无须专门的防火墙产品，即可建立包过滤防火墙。该技术适用于中小企业或部门级用户。最后给出一个在局域网环境下用Ipchains实现Linux防火墙的具体实例。

关 键 词 Linux操作系统; Ipchains软件包; 防火链; 包过滤; 防火墙; 中小企业

中图分类号 TP309 文献标识码 A

Technology and Application of Firewall Based on Packet Filtering of Linux

He Haibin

(Department of Energy and Environmental Engineering, Xihua University Chengdu 610039)

Abstract Mainly on the principle of Ipchains embedded in Linux kernel has been discussed. A series of rules can be set up with the input chains or output chains or forward chains or user defined chains, these rules can filter the packet of input or output or forward by host computer and can also filter packet from one network card to another network card by computer. Therefore, the access control can be implemented base on data of source address and destination address and protocol number. This technology is suitable for the users such as small enterprise or department to set up a firewall without professional firewall production. An example is presented for demonstrating how to use the proposed technology as firewall in LAN.

Key words Linux; Ipchains; firewall chains; packet filtering; firewall; small enterprise

防火墙已经成为企业构建计算机网络不可缺少的系统。专业的防火墙产品价格比较昂贵，中小企业往往无力购买，因而无法建立自己的防火墙。没有防火墙会使企业网络存在安全漏洞和安全隐患，网络容易受到攻击，造成经济损失，因此建立防火墙刻不容缓。Linux操作系统内核具有完善、强大的网络功能，提供了较为完善的审计、日志功能，并且占用系统资源少，效率高。使用Linux构建的放火墙具有操作简单、安全性高、抵御性能强、投入小、性价比高等特点。因此，使用Linux构建内部防火墙，用于控制外部网络对内部网络的访问，屏蔽内部网络的拓扑结构是一种非常合理的选择[1,2]。同时，也要了解Linux防火墙的运行机制和设置的策略，对网络进行有效的设置，才能使网络系统安全高效地运行。

1 防火墙的主要技术类型

防火墙是在计算机上设立的防止内部网络与公共网络直接访问的安全机制，在两个或多个网络间进行

收稿日期：2003 – 10 – 22

作者简介：何海宾(1967 –)，男，硕士，讲师，主要从事计算机网络、数据库技术方面的研究.

访问控制，以保护网络不受来自另一个网络攻击的安全技术[3]。它可看成是过滤器与安全策略的组合，所有的访问都被强制经过防火墙，以便按照事先制定的安全策略来检查和评价这些访问，决定是否放行。根据过滤检查方式的不同，防火墙的主要技术类型分为：应用代理服务器和包过滤防火墙。常见的防火墙系统都是使用这两种技术，通过多种方式来实现不同级别的安全，其方式主要有包过滤路由器或主机型、双宿主机型、屏蔽主机型、屏蔽子网型。

应用代理服务是由位于内部网和外部网之间的代理服务器完成的，它工作在应用层，代理用户进、出网络的各种服务请求，如FTP和Telnet等。

包过滤是指建立IP包过滤规则，工作在网络层。根据规则及IP包头的信息控制包的流动，在网络层判定允许或拒绝包的通过。如允许或禁止FTP的使用，但不能禁止FTP特定的功能(例如Get和Put的使用)。该技术比较安全、可靠、维护容易。包过滤主要有两种策略：

1) 先接受所有的包，然后明确哪些类型的包被拒绝通过。

2) 先丢弃或拒绝所有的包，然后明确允许符合哪些条件的包通过。一般采用第二种策略，因为在防火墙中指定一个较小的规则列表允许通过防火墙，比指定一个较大的列表不允许通过防火墙更容易实现。

2 Linux包过滤防火墙的实现

2.1 Ipchains原理

Linux操作系统内核包含Ipchains数据包过滤策略管理软件，用于构建防火墙。其核心中有三个规则列表，每条规则都是用来判定IP数据包。如果该数据包与第一条规则匹配，则对数据包做相应的处理。如果不匹配，则引入链中的下一条规则。如果没有规则与该数据包匹配，则该规则通知内核将数据包拒绝或丢弃[4,5]。规则列表又称为防火链，分别为输入链(input chains)、输出链(output chains)和转发链(forward chains)。它们分别定义了输入包、输出包、转发包的过滤规则。当一个IP数据包从Internet进入配置了防火墙的Linux主机，Linux内核便使用输入链决定该数据包的取舍。如果该数据包没有被丢弃，则内核用转发链决定该数据包发送到某个出口，但数据包在发送出去之前，内核要使用输出链来决定，即是输出该数据包还是丢弃或拒绝该数据包。除此之外，还可以配置用户自定义的链。在三条链的执行中可随时跳转到自定义链执行，完成后再回到主链，这使过滤规则变得灵活。在防火墙链中有一些特殊的跳转目标值如表1所示。

表1 防火墙链中的特殊策略目标值

目标值	目标值说明
ACCEPT	让数据包通过。
DENY	把数据包丢弃。
REJECT	把数据包丢弃，并向发送者发送ICMP消息告之数据包被丢弃，对于ICMP数据包，DENY和RETURN没有区别。
MASQ	只用于转发链和自定义链，数据包将被伪装成从本地主机发出，回应的数据包自动解伪装。
REDIRECT	只用于输入链和自定义链。数据包被重定向到本地，尽管它们原是发送给远地主机的。可以使用参数指定重定向端口，缺省值为0时表示使用数据包的目的地址端口作为重定向端口。
RETURN	如果用户定义的规则进行到末尾，或一个目标是RETURN的规则被匹配，则从该链返回到调用该链处，顺序执行下面的规则；如果三条内置链到末尾，或一个目标是RETURN的规则被匹配，则有内置策略指定的内置目标来决定数据包的命运。

2.2 防火墙构建

配置一个双宿主机型的Linux过滤包防火墙。假设某企业有一个局域网要连接到Internet上，公共网络地址为202.101.2.26。内部网段192.169.12.0。网络拓扑结构如图1所示。

在Linux主机上安装两块网卡card0和card1。为card0网卡分配一个公共网络IP地址202.101.2.26与Internet相连。为card1网卡分配一个内部网络IP地址191.169.12.1与Intranet相连， Linux主机上设置输入、转发、输出和用户自定义链。采用先允许所有数据包输入、输出、转发，但禁止一些危险数据包，如IP欺骗数据包、

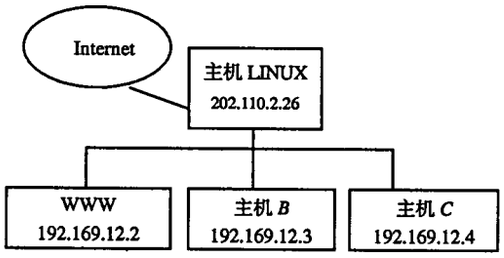

图1　基于Linux防火墙

广播数据包和ICMP服务类型攻击数据包等的设置策略。具体设置如下：

1) 刷新所有规则

/sbin/ipchains　-F forward

/sbin/ipchains　-F input

/sbin/ipchains　-F output

2) 设置初始规则

/sbin/ipchains　-A input　-j ACCEPT

/sbin/ipchains　-A output　-j ACCEPT

/sbin/ipchains　-A forward -j ACCEPT

3) 设置本地环路规则

/sbin/ipchains　-A input -j ACCEPT　-　i lo

/sbin/ipchains　-A output -j ACCEPT　-　i lo

本地进程之间的包允许通过。

4) 禁止IP欺骗

/sbin/ipchains　-A input　-j DENY

-　i　card0 - s 192.169.12.1/24

/sbin/ipchains　-A input　-j DENY

-　i　card0 - d 192.169.12.1/24

/sbin/ipchains　-A output　-j DENY

-　i　card0 - s 192.169.12.1/24

/sbin/ipchains　-A output　-j DENY

-　i　card0 - d 192.169.12.1/24

/sbin/ipchains　-A input　-j DENY

-　i　card0 -s 202.101.2.26/32

/sbin/ipchains　-A output　-j DENY

-　i　card0 -d 202.101.2.26/32

5) 禁止广播包

/sbin/ipchains　-A input　-j DENY

-　i　card1 - s 255.255.255.255

/sbin/ipchains　-A input　-j DENY

-　i　card1 - d 0.0..0.0

/sbin/ipchains　-A output　-j DENY

-　i　card1 - s 240.0.0.0/3

6) 设置card1转发规则

/sbin/ipchains　-A forward　-j MASQ

-　i　card1- s 192.169.12.1/24

7) 设置card0转发规则

/sbin/ipchains -A forward -j ACCEPT

- i card0- s 192.169.12.1/24

/sbin/ipchains -A forward -j ACCEPT

- i card0- d 192.169.12.1/24

8) 设置WWW包过滤

规则为：card1允许所有来自Intranet的WWW包，card0 仅允许目的为内部网WWW服务器的包。WWW端口为80，采用tcp或udp协议。

/sbin/ipchains -A input -p tcp -s 0.0.0.0/0 1024: -d 192.169.12.2/32 www -i card0 -j ACCEPT

/sbin/ipchains -A input -p udp -s 0.0.0.0/0 1024: -d 192.169.12.2/32 www -i card0 -j ACCEPT

/sbin/ipchains -A input -p tcp -s 192.169.12.2/32 www -d 0.0.0.0/0 1024: -i card1 -j ACCEPT

/sbin/ipchains -A input -p udp -s 192.169.12.2/32 www -d 0.0.0.0/0 1024: -i card1 -j ACCEPT

/sbin/ipchains -A input -p tcp -s 192.169.12.0/24 1024: -d 0.0.0.0/0 www -i card1 -j ACCEPT

/sbin/ipchains -A input -p udp -s 192.169.12.0/24 1024: -d 0.0.0.0/0 www -i card1 -j ACCEPT

/sbin/ipchains -A input -p tcp -s 0.0.0.0/0 www -d 192.169.12.0/24 1024: -i card0 -j ACCEPT

/sbin/ipchains -A input -p udp -s 0.0.0.0/0 www -d 192.169.12.0/24 1024: -i card0 -j ACCEPT

将规则保存到/etc/rc.firewallrules文件中，用chmod赋予该文件执行权限，并在/etc/rc.d.rc.local中加入一行/etc/rc.firewallrules。为了让Masq和Redirect起作用，在编译内核时，可以分别选择Config_IP_Masquerading和Config_IP_Transparent_Proxy。当系统启动时，这些规则就生效。

3 结 束 语

本文配置可以建立一个基于Linux操作系统的包过滤防火墙。如果在包过滤的基础上再加上代理服务器，如TIS Firewall Toolkit还可构建更加安全的复合型防火墙，它具有操作简单、安全性高、抵御能力强等优点。特别是可利用闲置的计算机和免费的Linux操作系统构建投入最小化、产出最大化的防火墙，用于替代专业的防火墙产品，非常适合在一些中小企业、机关、学校的局域网上使用。

参 考 文 献

[1] 王 茜, 杨德礼, 杜祥宇. Linux Ipchains用户访问控制系统的实现[J]. 计算机工程, 2002, 28(11): 15-17

[2] 王永滨. Linux放火墙规则的可视化输入与翻译[J]. 计算机应用研究, 2001, 18(12): 107-114

[3] Ellen Siever, Stepben Spainbower, Stepben Figgins, *et al.* LINUX 技术手册[M]. 陈莉君, 孟彩霞, 王曙燕译. 北京：中国电力出版社, 2003: 33-39

[4] Rusty R. Linux Ipchains-howto[EB/OL]. http://www.linux.org/docs/ldp/howto/ ipchains-howto.html, 2002-10-11

[5] Adm M. The unofficial Linux Ipchains-howto［EB/OL］. http://www.flounder.net /Ipchains/Ipchains-howto.html, 2002-12-15

编 辑 漆 蓉