图书馆 Linux 防火墙的架设

王华伟

(武汉工业大学图书馆 武汉 430070)

【摘要】 讨论了在图书馆内部局域网建立防火墙的必要性,并根据图书馆网络建设的需求,以 Linux 操作系统的 Ipchains 作为实例详细介绍了具体的实现方法与步骤。

【关键词】 图书馆网络 防火墙 网络安全 Linux Ipchains 【分类号】 TP393.08

随着 Internet 的普及,人们的日常工作与之的关系也越来紧密,因而越来越多的图书馆提供 Internet 服务。但当图书馆的内部网络接上 Internet 之后,图书馆内部资源就危险,因而系统的安全除了考虑计算机病毒、系统的健壮性等内部原因之外,更主要的是防止非法用户通过 Internet 的入侵。而目前防止的措施主要是靠防火墙的技术完成。

1 什么是防火墙

防火墙(Firewall)是指一个由软件或和硬件设备组合而成,处于网络群体计算机与外界通道(Internet)之间,限制外界用户对内部网络访问及管理内部用户访问外界网络的权限。主要是控制对受保护的网络(即网点)的往返访问,逼使各连接点的通过能得到检查和评估。从诞生到现在,防火墙已经历了四个发展阶段:基于路由器的防火墙、用户化的防火墙工具套、建立在通用操作系统上的防火墙、具有安全操作系统的防火墙。目前防火墙供应商提供的大部分都是具有安全操作系统的软硬件结合的防火墙,象 Neteye、Netscreen、Talentit 等。在 Linux 操作系统上的防火墙软件也很多,除了下面要专门介绍的 Ipchains 外,还有很多,如:Sinus Firewall、Jfwadmin 等。目前的防火墙从结构上讲,可分为两种:

代理主机结构

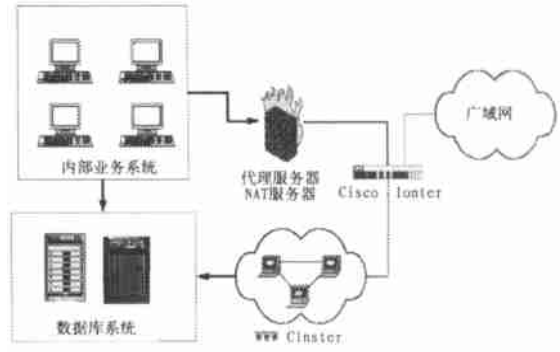
内部网络<- - - - - -> 代理网关(Proxy Gateway)<- - - - - -> Internet

路由器加过滤器结构

内部网络<- - - - - -> 过滤器(Filter)<- - - - - -> 路由器(Router)<- - - - -> Internet

2 图书馆网络结构

图书馆网络采用混合结构,内部业务系统及数据库系统采用内部网段(192.168.1.x),内部业务系统通过代理服务器或 NAT(Network Address Translation)服务器访问 Internet,互联网用户需要访问图书馆的数据资源则要通过图书馆 WWW 服务器才能使用图书馆数据库资源。这样就构成典型双向三层结构,即保证了图书馆数据资源的安全,又有效隔离图书馆内部计算机网络与 Internet。通过采用 Linux 操作系统的软防火墙 Ipchains,使图书馆内部业务系统与 Internet 数据流成为单向流。由于 Linux 操作系统是全免费的,且对硬件的要求也很低。故非常适合图书馆使用。



3 用 Ipchains 构建局域网防火墙的原理

其实从本质上讲,用 Ipchains 构建局域网防火墙也是一种 C/S 模式的交互式的应用。一般服务器提供某特定功能的服务总是由特定的后台程序提供的。在 TCP/IP 网络中,常常把这个特定的服务绑定到特定的 TCP 或 UDP 端口。之后,该后台程序就不断地监听(Listen)该端口,一旦接收到符合条件的客户端请求,该服务进行 TCP 握手后就同客户端建立一个连接,响应客户请求。与此同时,再产生一个该绑定的拷贝,继续监听客户端的请求。

Ipchains 就是这样的一个 Server。对内部网通往 Internet 的请求,或从外部通往内部网的请求,都进行监听、检查、评估、转发、拒绝等动作。

举一个具体的例子:假设网络中有一台服务器 A(IP 地址为 a.b.c.1)提供 WWW 服务,另有客户机 B(a.b.c.4)、C(a.b.c.7)。首先,服务器 A 运行提供 WWW 服务的后台程序(比如 Apache)并且把该服务绑定到端口 80,也就是说,在端口 80 进行监听。当 B 发起一个连接请求时,B 将打开一个大于 1024 的连接端口(1024 内为已定义端口),假设为 1037。A 在接收到请求后,用 80 端口与 B 建立连接以响应 B

收稿日期:2000-11-26

的请求, 同时产生一个 80 端口绑定的拷贝, 继续监听客户端的请求。假如A 又接收到C 的连接请求(设连接请求端口为 1071), 则A 在与C 建立连接的同时又产生一个 80 端口绑定的拷贝继续监听客户端的请求。如下所示, 每个连接都是唯一的。

服务器 客户端

连接 1: a. b. c. 1: 80 < = > a. b. c. 4: 1037

连接 2: a. b. c. 1: 80 < = > a. b. c. 7: 1071

服务端口

每一种特定的服务都有自己特定的端口, 一般说来小于 1024 的端口多为保留端口, 或者说是已定义 端口, 低端口分配给众所周知的服务(如WWW、FTP 等等), 从 512 到 1024 的端口通常保留给特殊的 Unix TCP/IP 应用程序, 具体情况请参考/etc/services 文件或 RFC1700。

4 Ipchains 作防火墙的步骤

4.1 安 装

Ipchains 现在的版本已经发展到 1.3.9。一般在安装Linux 时都会安装上, 如果没有的话可以到 www.linux.org 下载。下面笔者安装 Ipchains。由于它需 IP-MASQ 的支持, 所以确定已安装了 IP-MASQ 模块。

如果你是下载 Ipchains 安装包的话:

如果是 rpm 包:

```
# rpm -ivh *.rpm
```

如果是 tar.gz 包

```
# tar xvfz *.tar.gz(先把包解开)
```

再到解开目录

```
# ./configure
# make
# make install
```

这样就安装成功了。

4.2 启用 Ipchains

手工修改 /proc/sys/net/ipv4/ipforward 文件, 将其内容置为 1。

在/etc/rc.d/目录下用 touch 命令建立 rc.ipfwadm 文件

在/etc/rc.d/目录下的 rc.local 文件中加上下面这段代码: if -f /etc/rc.d/rc.ipfwadm ; then /etc/rc.d/rc.ipfwadm; fi;

以后所有的 Ipchains 的配置命令都将在 rc.ipfwadm 文件里修改。

4.3 配置 Ipchains(基本应用)

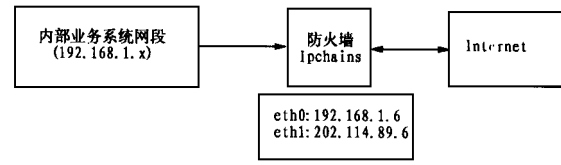
Ipchains 对机器的管理是通过对机器的 IP 地址作为标志的, 因而首先得确保你的局域网的机器的 IP 地址已经配分配好, 并且你对之相当熟悉。

Ipchains 的配置规则一般是围绕着 Input、Output、Ipforward 这三个规则进行的, 其中 Input 是指对内连接请求的过滤规则, Output 是指对外连接请求的过滤规则, Ipforward 是指对内部与外部通讯包的转发。Ipchains 的命令格式一般是:

ipchains [ADC] ipchains 规则 [ipchains 选项]

有关命令的详细用法请参考有关 How to 文档。

现在我们假设图书馆的内部网网段为 192.168.1.0~192.168.1.255, 其中防火墙的主机的 IP 地址分别为: eth0 192.168.1.6, eth1 202.114.89.6。假设目前防火墙是进行代理上网, 拒绝所有的外部 Telnet。对内部用户访问外部站点进行限制、并授予一些机器特权可任意访问外部机器、拒绝内部某些机器访问 Internet 等。网段示意图为:



配置 Ipchains 防火墙规则一般有两种方式:

* 首先允许所有的包, 然后在禁止有危险的包通过防火墙;

* 首先禁止所有的包, 然后再根据所需要的服务允许特定的包通过防火墙。

在本例中, 我们将在 eth0 和 eth1 的 input chain 设置过滤规则。

① 在/etc/rc.d/目录下用 touch 命令建立 firewall 文件, 执行 chmod u+x firewll 以更改文件属性, 编辑/etc/rc.d/rc.local 文件, 在末尾加上 /etc/rc.d/firewall 以确保开机时能自动执行该脚本。

② 刷新所有的 ipchains

```
#!/bin/sh
echo "Starting ipchains rules..
# Refresh all chains
/sbin/ipchains -F
```

③ 设置WWW 包过滤

说明: WWW 端口为 80, 采用 tcp 或 udp 协议。

规则为: eth1=> 允许所有来自 Intranet 的WWW 包; eth0=> 仅允许目的为内部网WWW 服务器的包。

```
# Define HTTP packets
# Allow www request packets from Internet clients to www servers
/sbin/ipchains -A input -p tcp -s 0.0.0.0/0 1024:- -d 198.168.1.11/32 www -i eth0 -j ACCEPT
/sbin/ipchains -A input -p udp -s 0.0.0.0/0 1024:- -d 198.168.1.11/32 www -i eth0 -j ACCEPT
# Allow response from Intranet www servers to request Internet clients
/sbin/ipchains -A input -p tcp -s 198.168.1.11/32 www -d 0.0.0.0/0 1024:- -i eth1 -j ACCEPT
/sbin/ipchains -A input -p udp -s 198.168.1.11/32 www -d 0.0.0.0/0 1024:- -i eth1 -j ACCEPT
# Allow www request packets from Intranet clients to Internet www servers
/sbin/ipchains -A input -p tcp -s 198.168.1.0/24 1024:- -d 0.0.0.0/0 www -i eth1 -j ACCEPT
/sbin/ipchains -A input -p udp -s 198.168.1.0/24 1024:- -d 0.0.0.0/0 www -i eth1 -j ACCEPT
# Allow www response packets from Internet www servers to Intranet clients
/sbin/ipchains -A input -p tcp -s 0.0.0.0/0 www -d 198.168.1.0/24 1024:- -i eth0 -j ACCEPT
```

/sbin/ipchains - A input - p udp - s 0.0.0.0/0 www - d 198.168.1.0/24 1024: - i eth0 - j ACCEPT

④ 设置 ftp 包过滤

说明: ftp 端口为 21, ftp- data 端口为 20, 均采用 tcp 协议。

规则为: eth1= > 允许所有来自 Intranet 的 ftp、ftp- data 包; eth0 = > 仅允许目的为内部网 ftp 服务器的包。

Define FTP packets

Allow ftp request packets from Internet clients to Intranet ftp server

/sbin/ipchains - A input - p tcp - s 0.0.0.0/0 1024: - d 198.168.1.12/32 ftp - i eth0 - j ACCEPT

/sbin/ipchains - A input - p tcp - s 0.0.0.0/0 1024: - d 198.168.1.12/32 ftp- data - i eth0 - j ACCEPT

Allow ftp response packets from Intranet ftp server to Internet clients

/sbin/ipchains - A input - p tcp - s 198.168.1.12/32 ftp - d 0.0.0.0/0 1024: - i eth1 - j ACCEPT

/sbin/ipchains - A input - p tcp - s 198.168.1.12/32 ftp- data - d 0.0.0.0/0 1024: - i eth1 - j ACCEPT

Allow ftp request packets from Intranet clients to Internet ftp servers

/sbin/ipchains - A input - p tcp - s 198.168.1.0/24 1024: - d 0.0.0.0/0 ftp - i eth1 - j ACCEPT

/sbin/ipchains - A input - p tcp - s 198.168.1.0/24 1024: - d 0.0.0.0/0 ftp- data - i eth1 - j ACCEPT

Allow ftp response packets from Internet ftp servers to Intranet clients

/sbin/ipchains - A input - p tcp - s 0.0.0.0/0 ftp - d 198.168.1.0/24 1024: - i eth0 - j ACCEPT

/sbin/ipchains - A input - p tcp - s 0.0.0.0/0 ftp- data - d 198.168.1.0/24 1024: - i eth0 - j ACCEPT

⑤ 设置 smtp 包过滤

说明: smtp 端口为 21, 采用 tcp 协议。

规则为: eth1= > 允许所有来自 Intranet 的 smtp 包; eth0= > 仅允 许目的为 E- mail 服务器的 smtp 请求。

Define smtp packets

Allow smtp request packets from Internet smtp servers to Intranet email server

/sbin/ipchains - A input - p tcp - s 0.0.0.0/0 1024: - d 198.168.1.14/32 smtp - i eth0 - j ACCEPT

Allow smtp response packets from Intranet email server to Internet smtp servers

/sbin/ipchains - A input - p tcp - s 198.168.1.14/32 smtp - d 0.0.0.0/0 1024: - i eth1 - j ACCEPT

Allow smtp request packets from Intranet clients to Internet smtp servers

/sbin/ipchains - A input - p tcp - s 198.168.1.0/24 1024: - d 0.0.0.0/0 smtp - i eth1 - j ACCEPT

Allow smtp response packets from Internet smtp servers to Intranet clients

/sbin/ipchains - A input - p tcp - s 0.0.0.0/0 smtp - d 198.168.1.0/24 1024: - i eth0 - j ACCEPT

⑥ 设置 POP- 3 包过滤

说明: POP- 3 端口为 110, 采用 tcp 或 udp 协议。

规则为: eth1= > 允许所有来自 Intranet 的 POP- 3 包; eth0= > 允许所有目的为 Intranet(E- mail server 除外) 的 POP- 3 包。

Define pop- 3 packets

Allow pop- 3 request packets from Intranet clients to Internet pop- 3 servers

/sbin/ipchains - A input - p tcp - s 198.168.1.0/24 1024: - d 0.0.0.0/0 pop- 3 - i eth1 - j ACCEPT

/sbin/ipchains - A input - p udp - s 198.168.1.0/24 1024: - d 0.0.0.0/0 pop- 3 - i eth1 - j ACCEPT

Allow pop- 3 response packets from Internet pop- 3 servers to Intranet clients (except email server)

/sbin/ipchains - A input - p tcp - s 0.0.0.0/0 pop- 3 - d 198.168.1.0/24 1024: - i eth0 - j ACCEPT

/sbin/ipchains - A input - p udp - s 0.0.0.0/0 pop- 3 - d 198.168.1.0/24 1024: - i eth0 - j ACCEPT

⑦ 设置缺省包过滤规则

说明: 除了以上所允许通过的包以外, 禁止其它包通过。

Define all rules on input chain

/sbin/ipchains - A input - j DENY - l

5 结 语

通过以上各步骤, 我们建立了一个相对完整的防火墙。该防火墙禁止除了提供基本服务以外的包通过。但是该防火墙还有不完善的地方, 比如: 某些搜索引擎会打开一个小于 1024 的但不常用的端口的连接, 这样的包就无法通过该防火墙, 从而使用户不能使用该搜索引擎。但是提高了网络的安全性, 消除了安全隐患安全性重要还是服务重要就要看不同的情况了。

参考文献

1 Howard C. Berkowitz. 企业网路由和交换体系结构设计: 电子工业出版社, 2000, 8

2 张 晶 刘绍中. uGuardian 防火墙设计及实现. 计算机应用, 2000, (6)

3 杨木清 罗惠平. 用 Linux 的 IP 伪装组建网络及与国际网互联. 中南民族学院学报 (自然科学版), 2000, (6)

4 David Pitts. Red Hat Linux 大全. 机械工业出版社, 1999, 1