如何在 Linux 上建立防火墙

●王炜　胡鸿彬

摘　要　本文介绍了防火墙的定义、种类、结构,重点介绍了在 Linux 操作系统上建立防火墙。

关键词　防火墙　结构　Linux

防火墙技术是实现网络安全的一种有效的手段,它能够将非法入侵的访问抵挡在内部网络之外,从而保护内部网络的数据及信息不被盗用与侵害。

一、防火墙的定义及种类

所谓防火墙就是指能够限制外部网络与内部网络间相互访问的某一个设备或某一组设备。目前,防火墙有三种类型:应用代理网关、电路层转发及包过滤。

1. 应用代理网关

应用代理网关的主要组件之一就是 Bastion Host ,它可看作是内部网络与外部网络相联系的一个代表, 内部网对外部网的访问外部网对内部网的访问均通过安装在 Bastion Host 机上的代理进程来完成。代理网关有许多优点:首先,因为这些代理是处于应用层,它们能够充分利用应用层的协议。例如 TELNET, FTP, HTTP 等协议提供的真实性校验能够被代理进程截获并加强校验性, 同样这些协议特指的规则亦能被代理进程利用, 如它可以允许 FTP 通过网关 gets 文件,但不能 puts 文件。另外,广泛的 logging 应用都是处于应用层。非常重要的一点是 Bastion Host 不具有 IP 路由功能。

2. 电路层转发

电路层转发的功能类似于应用代理网关,不同点在于它的代理采用电路转发而不是应用层的进程,这样就失去了许多详细的 logging 能力以及许多协议规则定义。同样它只是具有代理的功能,而不具有 IP 路由的作用。

3. 包过滤技术

包过滤技术是应用最多的防火墙类型,它的工作原理就是根据定义的规则来转发 IP 包, 这些规则的定义是根据对 IP 包的源地址、目的地址,源 port 及目的 port 的判断,根据所

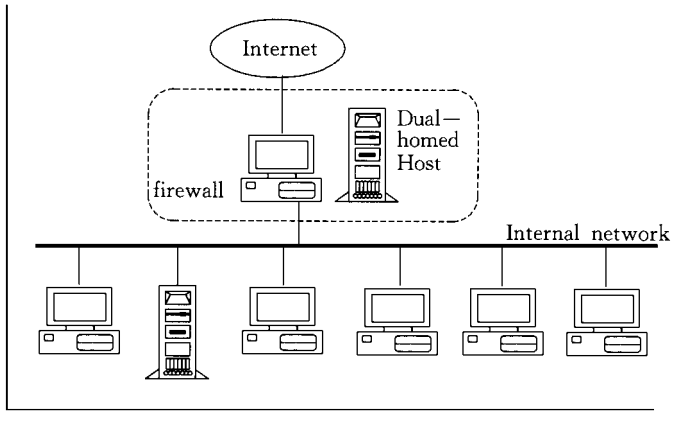

图 1　Dual - Homed Host 结构

net　　加载 Ethernet II 帧
load tcpip　　加载 TCP/IP 模块
bind ip to ipnet addr = 202.201.19.9 GATE = 202.201.17.10　　捆绑 IP 协议、指定 IP 地址和路由参数
load iptunnel peer = 202.201.23.9 local = 202.201.19.9　　加载 IP 隧道、指定 CCS2 地址
bind ipx to iptunnel net = 333
　　捆绑 IPX 协议到 IP 隧道

CCS2 服务器有关配置:

file server name CCS2
ipx internal net 341CD9BB
load 3c59x port = fce0 frame = Ethernet –II name = ipnet
load tcpip
bind ip to ipnet addr = 202.201.23.9 GATE = 202.201.17.10
load iptunnel peer = 202.201.19.9 local = 202.201.23.9
bind ipx to iptunnel net = 333

当 CCS1 子网采用 IP 隧道技术和 CCS2 子网连通后, 因 CCS3、CCS4 和 CCS2 子网同属一个桥组,故 CCS1 子网同时也和 CCS3、CCS4 子网连通。如采用统一的 NDS(目录服务) 管理用户和各种网络资源,就能实现网络资源的逻辑组织、资源独立于物理位置、用户集中或分布的全局管理、整个网络对用户的单一登录等先进的网络技术。

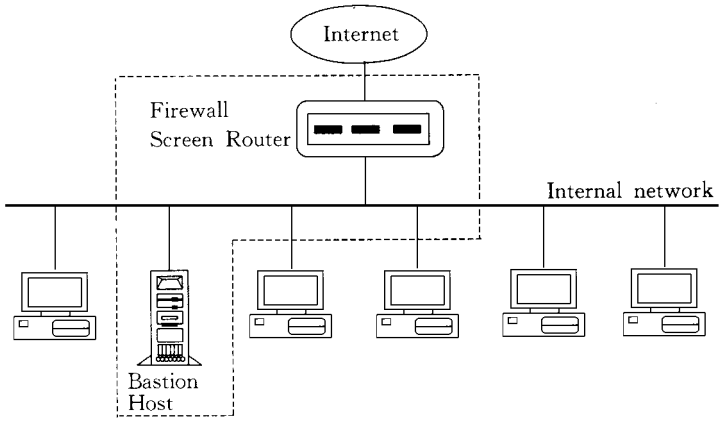

图 2　Screened Host 结构

传输的协议的种类、TCP 标志、IP 标志等等。包过滤技术与其它两种类型的不同点在于，包过滤防火墙相当于一个路由器，它的功能就是对 IP 包的转发。这就意味着你能控制外网的工作站与内网的工作站间的相互通信，因此包过滤技术是非常有用的，它被广泛应用并且费用低廉。

二、防火墙的结构

防火墙大体有以下几种结构：

1. Dual - Homed Host 结构

一个 Dual - Homed Host 结构的防火墙是由一台具有两个网络接口的主机构成，它的一个接口与内部网相连，另一个接口与外部网相连。这就要求它一方面具有防火墙功能，一方面具有路由的功能。防火墙跨接在两个网段之间，关闭它的路由选择，内部网与外部网就完全隔离，不能相互通信。Dual - Homed Host 防火墙的优点是结构简单，缺点是这种结构只能提供代理服务，或由用户登录到 Dural - Homed 主机上再对外访问，这样，网上许多应用受到限制，并给用户带来不便。其结构如图 1。

2. Screened Host 结构

一个 Screened Host 结构的防火墙是由一个 Screening Route 及一个 Bastion Host 构成，Screening Route 跨接在内部网与外部网之间，它可以由包过滤技术组成第一道安全防线，Bastion Host 位于内部网之中。来自外部网对内部网的访问必须经过 Bastion Host，这样通过设置 Bastion Host 的过滤条件，可以构成防火墙的第二道安全防线。与别的防火墙结构相比，这种结构的防火墙有一个弱点，当攻击者一旦攻破 Bastion Host 的防护，那么整个内部网将都暴露在攻击者面前，其结构如图 2。

3. Screened Subnet 结构

一个 Screened Subnet 结构的防火墙，其主要特征就是在内部网段与 Internet 之间增加了一个网段（我们称为外围网），这样外围网在物理结构上就把内部网与 Internet 分隔开来。Bastion Host 是整个内部网络中最易受到攻击的部分，把 Bastion Host 放在外围网上，即使 Bastion Host 受到攻击与破坏，而内部网络中的主机仍可安然无恙。

放在外围网中的 Bastion Host 主要完成以下一些任务：

- 接收外来 E - mail 并转发到相应的地方。
- 转接外来 FTP 到指定 FTP Server 上。
- DNS 的名字查询。

Sreened Subnet 结构的防火墙的主要优点是：既能够有效地构成内部网络的安全防护系统，又能够最大限度地发挥网络的主要功能，其结构如图 3。

三、在 Linux 上建立防火墙

Linux 操作系统是一种安装在 PC 机上的网络操作系统，用 Linux 操作系统来建立网络防火墙，不失为一个经济实用的方案。现以实例简述如下：

1. 物理构成

用安装 Linux 操作系统的 PC 机作为防火墙，采用 Screened Subnet 结构。其拓扑结构如图 4。

同时在安装 Linux 操作系统的 PC 机上安装两块网卡，给这两块网卡的中断向量分别配置为 10、11。并在/ etc/ lilo. conf 文件中加上如下配置信息：

```
append = "ether = 10,0x300,eth0 \
          ether = 11,0x280,eth1"
```

用 ifconfig 命令把 eth0 配置为内部网关地址：192. 168. 1. 1，把 eth1 配置为外部网关地址：20. 2. 51. 33，这样此 PC 机就跨接在内部网与外围网之间，它既具有路由的功能，又具有防火墙的功效。内部网的网址为：192. 168. 1. 0～

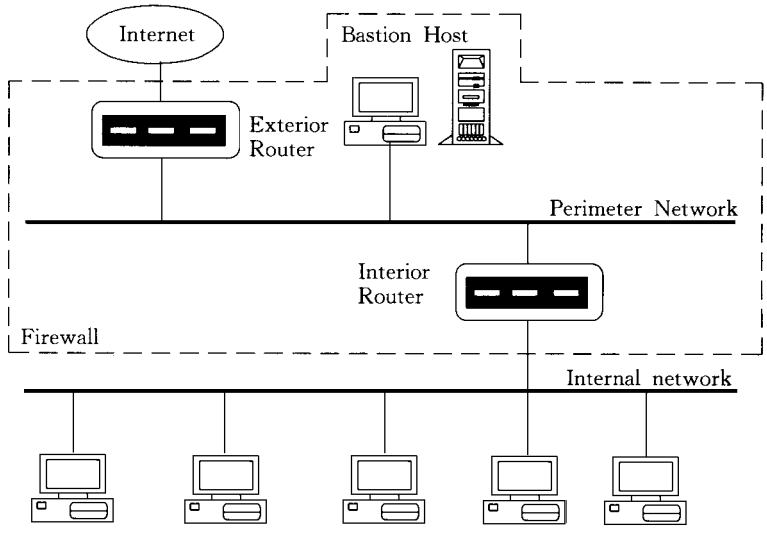

图 3　Screened Subnet 结构(双路由器)

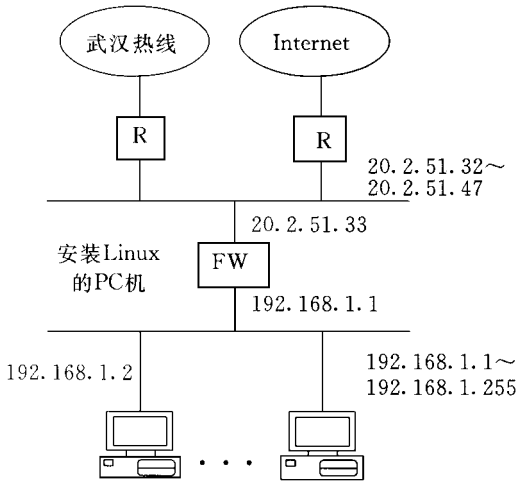

图 4　网络拓扑图

192.168.1.255,外围网的网址为:20.2.51.33～20.2.51.47,外围网再经过一个路由器与 Internet 相连。另外还要用 make menuconfig 命令建立 Linux 的一个新 Kernel,建立新 Kernel 时,打开 Network Firewall 功能。这样 PC 机 Reboot 后 Linux 操作系统就具有 Firewall 的功能。

2. 如何配置防火墙

防火墙主要有以下三种用法:Accounting,Blocking,Forwarding。Accounting 规则用来统计经过防火墙的 IP Packets 流量。Blocking 规则是防火墙用来接收与拒绝途经的 IP Packets。Forwarding 规则是防火墙用来对指定的 IP Packets 进行过滤及转发,它能够基于对 IP Packets 的源地址及目的地址的判断、TCP 或 UDP 的 Port 的筛选、TCP 及 UDP 协议的选择等方法来制定相应的过滤及防护措施。

Linux 操作系统中,用来设置防火墙规则的命令工具有 ipfw、ipfwadm。其中 ipfwadm 能够提供更直观的接口、更好的输出及更好的参考说明。本文主要介绍 ipfwadm 命令。这两个命令都只能由超级用户来使用,它们能够增加、删除或显示防火墙的记帐及防护规则的内容。

在实施防火墙的作用之前,必须首先制定一个防护规则表格,规定哪些机器需要保护,以及什么样的保护。

假设建立的防火墙必须满足以下条件:

①允许内部网络(192.168.1.0/24)的机器能够 Telnet、Ftp 到 Internet 上的任一点,而不允许 Internet 上的其它机器 Telnet、Ftp 到内部网上来。

②允许内部网及外部网的机器能够双向传送 E-mail(SMTP),并且外部网发来的 E-mail 只能够与内部网的 Mailhub(192.168.1.2)相联系。

制定如表 1 所示的 Forwarding 规则。

其中第一条“deny everything”是一条经常用到的规则,这样做了之后,每当需要允许某一个任务时,只要增加一条 accept 规则,这样网络管理员能够很清楚地制定防火墙规则。

另外此表中有些 Port 值写为 > 1023,是由于历史原因造成的。大多数 UNIX 客户机进程(如 Telnet)规定它们的临时 Port 值为 1024～5000。Port 1～1023 作为保留值,以供服务器进程使用,如 telnetd、ftpd 等等。在此用 > 1023,而不用 1024～5000 是因为目前有些设备并不遵守 UNIX 的指定规则。例如,Annex 终端服务器把它们的临时 Port 值定为 1024～10000。

以下就是用 ipfwadm 命令来建立上述的防火墙规则:

```
# ipfwadm -F -f
# ipfwadm -F -p deny
# ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 23 \
-D 192.168.1.0/24 1024:65535
# ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 21 \
-D 192.168.1.0/24 1024:65535
# ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 20 \
-D 192.168.1.0/24 1024:65535
# ipfwadm -F -a accept -b -P tcp -S 0.0.0.0/0 25 \
-D 192.168.1.2 1024:65535
# ipfwadm -F -a accept -b -P tcp -S 192.168.1.2
25 \
-D 0.0.0.0/0 1024:65535
```

其中第一条 # ipfwadm -F -f 的作用是清除以前所定义的所有规则。

用 # ipfwadm -F -l -n 可以列出所定义的规则。

为保证每一条规则都生效并不被遗漏,我们可以把以上所写的命令写入/etc/rc.d/rc.ipfw 文件中,并使 Linux 的 PC 机一开机就运行它。至此,一个基于 Linux 操作系统的简易、实用的防火墙就建成了。

表 1　　Forwarding 规则

Src Addr	Src Port	Dat Addr	Dat Port	Proto	Flags	Action	Comment
*	*	*	*	*		deny	default rule
*	23	192.168.1. *	> 1023	tcp	BIDIR	accept	TELNET in - out
*	21	192.168.1. *	> 1023	tcp	BIDIR	accept	FTP control in - out
*	20	192.168.1. *	> 1023	tcp	BIDIR	accept	FTP data in - out
*	25	192.168.1.2	> 1023	tcp	BIDIR	accept	SMTP send in - out
*	> 1023	192.168.1.2	25	tcp	BIDIR	accept	SMTP recv in - out