第 14 卷第 2 期　　中 南 工 学 院 学 报　　Vol. 14 No. 2
2000 年 6 月　　JOURNAL OF CENTRAL-SOUTH INSTITUTE OF TECHNOLOGY　　Jun. 2000

文章编号: 1006-737X(2000)02-0013-04

在 Red Hat Linux 上实现的“防火墙”

梁　冰

(中南工学院　科研处, 湖南　衡阳　421001)

摘要: 本文讨论了在局域网建立安全体系的意义, 介绍了当前流行的“防火墙”类型和结构, 就一个具体的网络拓扑模型, 基于已有的计费系统, 在 RED HAT LINUX 操作系统上构筑“防火墙”.

关键词: 局域网; 安全; 防火墙

中图分类号: N 39　　**文献标识码**: B

0 引　言

随着 Internet 网络使用的普及和大量企业内部网及校园局域网的建立, 一方面, 给人们提供了一种崭新的信息交互环境, 从根本上改变了获取信息的传统模式, 大量的信息被人们所共享. 另一方面, 由于 Internet 网络协议 (如 TCP/IP 协议等) 的安全机制及服务的缺乏和脆弱, 威胁着网络用户的信息安全. 信息的安全隐患也存在于信息的传递和共享过程中. 为防止非法用户利用网络系统的安全缺陷进行数据窃取、伪造和破坏, 必须建立信息的安全体系.

防火墙就是一种行之有效的安全机制, 是局域网的一道安全防线, 它能够将局域网外部的非法入侵访问拒绝于内部网络之外, 从而保护内部网络的数据和信息不被盗用和侵害.

1 防火墙的种类

“防火墙”是一种能够对外部网络与内部网络之间的访问信息进行控制的一组软、硬件系统, 不同的“防火墙”有不同的侧重点.

1) 基于代理服务 (proxy service) 的“防火墙”. 它可以被看作是外部网络与内部网络相互联系的代表, 它通常由 service 端程序和 client 端程序来构成. 这种 proxy service 可以使网络管理员对改善网络的安全特性有更大的能力. 同时, 由于它需要由 service 和 client 共同完成, 相当多的 proxy service 要求用固定的 client 程序, 这也给软件开发者、网络管

收稿日期: 2000-01-18

作者简介: 梁　冰 (1956-), 男, 山东威海人, 工程师.

理员及用户带来很大的不便. 由于代理服务可采用不同的方式, 它所支持的协议规则也不一样. 如应用代理网关型的主要组件是一台Bastion Host, 内部网和外部网间的相互访问均要通过Bastion Host 上的代理进程来完成. 因为这些代理是处于应用层, 它们能充分利用应用层的 telnet、http、ftp 等协议提供的真实性校验信息加强校验性. 同样, 这些协议的特指规则也能被代理进程所利用, 如它可以允许 ftp 通过网关 gets 文件, 而不能puts 文件. 再如电路层转发的"防火墙", 它的功能与应用代理网关类似, 但由于它的代理是采用电路转发而不是应用层的进程, 因此就失去了许多协议规则定义和许多处于应用层的 logging.

2) 基于包过滤 (packet filter) 形"防火墙". 它是根据 IP 包的源地址、目地地址、源port、目的port 及所定义的过滤规则来转发 IP 包. 因此, 它相当于一个路由器, 具有 IP 路由的功能, 完成外部网站与内部网机器的身份核查及相互通信. 因为是采用 IP 地址核查身份, 因此就无法区分采用合法 IP 地址的不同用户, 安全性就减低. 对用户来讲, 一般查觉不到packet filter 的存在, 具有较好的应用程序透明性.

2 网络拓扑和"防火墙"物理结构

按我院校园网一期工程规划, 将校园内部用户分配在四个不同的子网内, 其 IP 地址分别为:

210.43.115.* 掩码为 255.255.255.0

210.43.118.* 掩码为 255.255.255.0

210.43.125.* 掩码为 255.255.255.0

210.43.126.* 掩码为 255.255.255.0

210.43.112.* (网络设备专用网段)

校园网"防火墙"安装在 Internet 与 Intranet 的连接点上 (见图 1), 可以提供 IP 地址转换的功能, 使得内部网地址在对外部网访问时被修改为网关地址, 以便可对内部网络起到保护作用. 网关主机采用HPE50 机器, 配置为 300M CPU, 64MB 内存, 4GB 增强 IDE 硬盘, 接有两块 10/100MBASE TX 网卡, 一个接口与内部网相连, 另一个接口通过 Exterior router 与 Internet 相连. Firewall 跨接在两个不同的网段之间, 关闭它的路由选择, 就可使内部网与外部网完全隔离, 不能相互通信.

3 在 Red hat linux 实现 firewall

Red hat linux 是一种能安装在 X86 机上的真正多任务网络操作系统. linux 内核具有支持桥的功能, 用该系统建立网络"防火墙", 是一种经济实用的方案. 在 linux 系统中, ipfw、ipfwadm 命令工具, 都可用来设置 firewall 规则. 在 root 状态下, 它们可以增加、删除、显示"防火墙"记帐及防护规则. 配置时要在/etc/lilo.conf 文件中配置网卡信息、用 ifconfig[2]命令配置 interfaces、配置路由建立一个 linux 的新 kernel. 以上工作在装入计费系统时已完成.

配置完的机器:

interface	IP
lo	127.0.0.1

etho　　210.43.126.253
eth1　　210.43.112.36
raiting (network packet forwarding ipv4)
default gateway: 210.43.112.36
default gateway device: etho

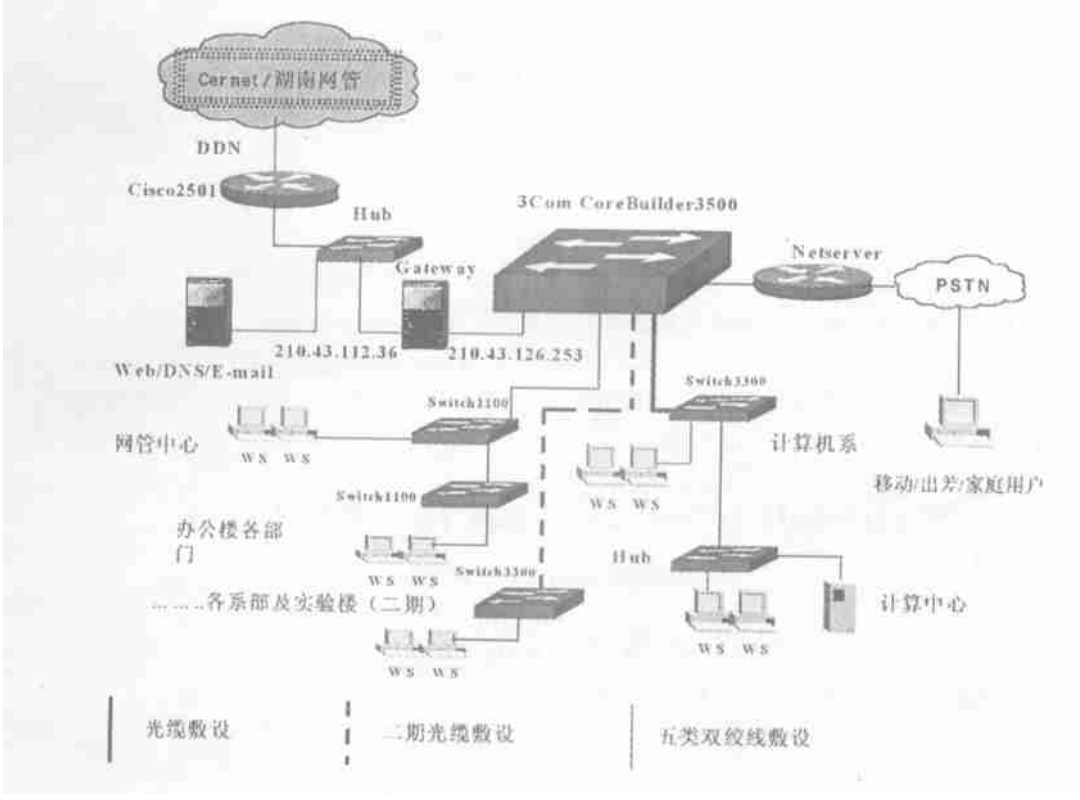

图 1　校园网拓扑图

Fig. 1　Campus net topological

inteface	netwok address	netmask	gatway
etho	210.43.126.0	255.255.255.0	210.43.126.254
etho	210.43.115.0	255.255.255.0	210.43.115.254
etho	210.43.125.0	255.255.255.0	210.43.125.254
etho	210.43.118.0	255.255.255.0	210.43.118.254
eth1	210.43.112.0	255.255.255.0	210.43.112.36
eth1	0.0.0.0	0.0.0.0	210.43.112.253

这样该台 HP 机就跨接到二个子网之间，它既有路由功能，又具有“防火墙”的功能

4　制定 firewall 规则

firewall 规则主要有 IP 包的流量统计规则，进入、外出数据包的控制规则等. 在我院校

园网的网关机上进行了以下配置:

```
# ipfwadm -I -f //刷新过去定义的所有规则//
# ipfwadm -I -a deny -s 0.0.0.0/0 -d 0.0.0.0/0 -w etho //关闭 ipfwadm 路由//
# ipfwadm -I -i accept -s 210.43.126.0/24 -d 210.43.126.253./32 -w etho
# ipfwadm -I -i accept -s 210.43.115.0/24 -d 210.43.126.253./32 -w etho
# ipfwadm -I -i accept -s 210.43.118.0/24 -d 210.43.126.253./32 -w etho
# ipfwadm -I -i accept -s 210.43.125.0/24 -d 210.43.126.253./32 -w etho
//根据需要配置, 允许校园网内部的用户通过 etho 的 interface 进入 internet//
```

配置完的命令, 放在一个 ipflist. ipf 的文件中, 并在开机时启动它. 一个行之有效的"防火墙"就建成了.

参考文献:

[1] 贺津志. 防火墙计费系统的设计与实现[J]. 计算机应用, 1999, 10 (增刊): 280- 282
[2] Jack T J, David G 著, 万 华译. Linux 大全[M]. 北京: 电子工业出版社, 1998. 373- 402
[3] 王海丽. 防火墙技术在华中理工大学校园网建设中的应用[J]. 计算机应用, 1999, 10 (增刊): 612

A Firewall Is Set up at the Red Hat Linux Operation System

LIANG Bing

(Section of Research Work, Central-South Institute of Technology, Hengyang 421001, Hunan, China)

Abstract: The significance of building a safety system at the regional network is described, and types and structure of a popular firewall are epitomized in this paper. And then, a practical/specific topological model is applied on the firewall, based on the RED HAT LINUX operation system and chargeable system.

Key words: network; safety; firewall