



Firewalls
The Complete Reference



网络与信息安全技术丛书

设计、配置和维护当今最流行的防火墙

防火墙 技术大全

(美) Keith E. Strassberg
Richard J. Gondek 等著
Gary Rollie

李昂 刘芳萍 杨旭 程鹏 等译

Mc
Graw
Hill Education



机械工业出版社
China Machine Press

TP393.08

125

42/44

网络与信息安全技术丛书

防火墙技术大全

Keith E. Strassberg

(美) Richard J. Gondek 等著

Gary Rollie

李昂 刘芳萍 杨旭 程鹏 等译



机械工业出版社

China Machine Press

787mm × 1092mm 1/16 × 32印张

印数: 0 001 - 4 000册

凡购本书者,如蒙函索,即寄赠《网络安全技术》一书,由本社发行部函索。

本书介绍了目前流行的七家防火墙产品系列的安装步骤、关键的配置选项及重要的维护工作等内容。还讲述了防火墙的网络基础、支持的网络布局设计、体系结构以及各种高级功能的实现原理。

本书内容具体包括：防火墙的网络基础、针对网络设计考虑、防火墙体系结构、高级功能以及对防火墙攻击的分析；本书重点提供Check Point Firewall-14.1和NG、Cisco PIX、Linux IP table、Microsoft ISA Server、NetScreen、SonicWall以及Symantec等七家不同厂商防火墙系列产品的背景介绍、功能描述、安装、配置和管理知识。

本书涉及的内容新颖全面，基础知识讲解清楚、描述清晰，与实际产品结合紧密、实用性极强。该书适合于网络安全管理员、工程师和技术人员，也适合于广大对防火墙感兴趣的读者作为参考。

Keith E. Strassberg, et al: Firewalls: The Complete Reference (ISBN 0-07-219567-3).

Copyright © 2001 by The McGraw-Hill Companies, Inc.

Original language published by The McGraw-Hill Companies, Inc. All rights reserved. No part of this publication may be reproduced or distributed in any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Simplified Chinese translation edition jointly published by McGraw-Hill Education (Asia) Co. and China Machine Press.

本书中文简体字翻译版由机械工业出版社和美国麦格劳-希尔教育(亚洲)出版公司合作出版。未经出版者预先书面许可，不得以任何方式复制或抄袭本书的任何部分。

本书封面贴有McGraw-Hill公司防伪标签，无标签者不得销售。

版权所有，侵权必究。

本书版权登记号：图字：01-2002-4796

图书在版编目(CIP)数据

防火墙技术大全(美)斯特拉斯伯格(Strassberg, K. E.)等著；李昂等译. - 北京：机械工业出版社，2003.3

(网络与信息安全技术丛书)

书名原文：Firewalls: The Complete Reference

ISBN 7-111-11524-4

I. 防... II. ①斯... ②李... III. 计算机网络-安全技术 IV. TP393.08

中国版本图书馆CIP数据核字(2003)第001669号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑：谢晓竹 李炎

北京瑞德印刷有限公司印刷·新华书店北京发行所发行

2003年3月第1版第1次印刷

787mm × 1092mm 1/16 · 36.5印张

印数：0 001-4 000册

定价：59.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

前言

当网络涉及不同的信任级别时（例如Intranet、Internet或是网络划分），要保证安全必须安装安全控制设备。此类控制设备几乎总是某种形式的防火墙。

防火墙能够确保非授权的访问在经过企业的对外访问点时被阻止。防火墙技术已经出现十多年了。这项技术最初来自在路由器上实现简单的访问控制表。由于网络协议的复杂性，路由器的ACL被证明是不够的。例如文件传输协议FTP，会建立一个来自目标主机的反向通道。于是基于主机的防火墙诞生了。各种有竞争力的防火墙技术不断出现，不过到20世纪90年代末期，基于包的状态防火墙出现，并因为协议的灵活性和性能而成为最佳选择。

这几年出现的另一个现象是用专用网络设备代替通用计算机（Wintel, Sun）来实现防火墙。网络速度从10Mb增加到1G，一下提高了两个数量级。基于主机的防火墙并不是为这种高速网络环境设计的，从而加速了向专用平台的转移。采用专业网络设备的附带好处是因为操作系统的简化而相对比较容易配置和管理。

在过去的五年中，防火墙供应商之间的差别已经缩小了。大多数供应商重组他们的产品，来包含状态包过滤和VPN。新的操作系统集成了一些防火墙的功能，例如Windows 2000/XP、Solaris 8以及Linux。大多数网络设备，包括防火墙，在管理和监控的可扩展性方面仍然比较薄弱。这对于大规模的防火墙设置是个重要问题，在这方面没有一家产品控制市场。

VPN比防火墙技术晚出现几年，它和企业的端点位置有关。如果VPN网关位于防火墙的后面，防火墙必须通过加密网络流。不只是目的端网络地址，隧道中的所有信息均加密。最好的解决方法就是在防火墙之前结束IP隧道。对大型企业来说，将防火墙和VPN功能集成在一个设备中还为时过早。将入侵检测加入到同一个平台也还太早。

最好的安全方案是提供多层的访问控制，其中防火墙是重要的一层。以后的几年中，随着安全体系组件的商品化，防火墙的功能还会增加。防火墙将不断发展以满足应用层安全控制日益增加的需求。

——Christopher M. King, CISSP
信息安全业务主管
Greenwich技术联盟

注：参与本书翻译工作的人员还有尚红、刘东卫、吴珍珍、王乐欣、徐洪芳、张飞扬、胡飞志、黄中辛、李欣济等。

目 录

前言

第1章 简介1

- 1.1 防火墙的定义1
- 1.2 为什么使用防火墙2
- 1.3 常见攻击类型2
- 1.4 防火墙的部署3
- 1.5 防火墙的优势和弱点3
 - 1.5.1 优势4
 - 1.5.2 弱点4
- 1.6 完善的安全措施4
 - 1.6.1 完善系统本身4
 - 1.6.2 补丁5
 - 1.6.3 硬件与操作系统5
 - 1.6.4 层次防御5
 - 1.6.5 创建安全策略6
 - 1.6.6 监测与记录6
 - 1.6.7 审计和测试6

第2章 防火墙管理的TCP/IP基础7

- 2.1 TCP/IP网络中的数据传输7
- 2.2 在数据传输中应用的OSI七层模型8
- 2.3 理解IP协议是如何工作的10
 - 2.3.1 IP地址10
 - 2.3.2 将IP地址转换为二进制格式10
 - 2.3.3 IP地址的层次结构11
 - 2.3.4 子网与地址划分的灵活性及高效性12
 - 2.3.5 IP是如何在网络中路由的14
 - 2.3.6 广播和组播17
 - 2.3.7 IP头部17
 - 2.3.8 用ARP和RARP进行地址解析18
 - 2.3.9 ICMP协议19
- 2.4 传输层协议：与应用程序的接口20

- 2.4.1 无连接通信：用户数据报协议20

- 2.4.2 可靠顺序交付：传输控制协议21

2.5 应用程序及工具23

- 2.5.1 Ping、Traceroute和Netstat23
- 2.5.2 使用地址转换隐藏私有地址24
- 2.5.3 访问控制列表（ACL）26
- 2.5.4 域名服务（DNS）26
- 2.5.5 简单网络管理协议（SNMP）27
- 2.5.6 超文本传输协议（HTTP）27
- 2.5.7 电子邮件（E-mail）27
- 2.5.8 远程登录（Telnet）28
- 2.5.9 远程服务（R-Services）28
- 2.5.10 文件传输协议（FTP）28

第3章 网络设计的考虑29

- 3.1 把安全作为网络设计的一部分29

- 3.2 Intranet、Extranet和Internet——安全的理由29

- 3.2.1 Intranet29

- 3.2.2 Extranet30

- 3.2.3 Internet30

- 3.2.4 Internet服务提供商（Internet - Service Provider, ISP）及分散组织30

- 3.2.5 部门安全31

- 3.2.6 小办公室/家庭办公室（SOHO）31

3.3 网络设计方法31

- 3.3.1 Tyjor公司——设计实例31

- 3.3.2 定义网络的目的31

- 3.3.3 需求32

- 3.3.4 预算37

- 3.3.5 选择销售商37

- 3.3.6 完成设计37

3.3.7 创建实施计划	38	5.2.3 端口转换	67
3.3.8 测试和确认	39	5.2.4 服务器负载平衡	68
3.3.9 提供支持	39	5.3 密码理论	68
3.4 网络	39	5.3.1 加密密码	68
3.4.1 网络拓扑的类型	40	5.3.2 哈希验证	69
3.4.2 路由协议	46	5.4 虚拟专用网络 (VPN)	71
3.5 普通网络防火墙设计	47	5.5 IPSec (IP安全协议)	73
3.5.1 非军事区 (DMZ)	48	5.6 网络监控	73
3.5.2 堡垒主机	48	5.6.1 审计	73
3.5.3 过滤网关	49	5.6.2 会话窃听	74
3.6 创建公司安全策略	49	5.7 病毒免疫	75
3.6.1 接受使用策略	49	5.8 可用性	75
3.6.2 特殊策略	50	5.8.1 状态信息	76
第4章 防火墙的体系结构	52	5.8.2 高可用性	76
4.1 包过滤器	52	5.8.3 负载平衡	77
4.1.1 包过滤的过程	53	5.9 管理	78
4.1.2 创建一个规则库	53	5.10 防火墙的其他特性	79
4.1.3 包过滤的优缺点	56	第6章 防火墙攻击	81
4.2 应用级网关	56	6.1 了解入侵者: 他们的攻击方法	81
4.2.1 应用级网关的工作过程	57	6.1.1 攻击目标的选择	81
4.2.2 应用级网关的缺点	58	6.1.2 跟踪	82
4.3 电路级网关	59	6.1.3 识别并侦察防火墙	86
4.3.1 电路级网关的工作过程	59	6.2 未雨绸缪——准备基础知识	92
4.3.2 电路级网关的缺点	59	6.2.1 包过滤防火墙	92
4.4 状态包检查 (SPI)	59	6.2.2 应用级代理防火墙	92
4.4.1 SPI防火墙的工作过程	60	6.2.3 IP欺骗	92
4.4.2 SPI在安全上的优点	61	6.2.4 会话劫持	93
4.5 实施方式	61	6.2.5 形同虚设的访问控制列表 (ACL)	95
4.5.1 基于网络主机的防火墙	62	6.2.6 隧道	97
4.5.2 基于路由器的防火墙	62	6.2.7 代理服务器的外来访问	98
4.5.3 基于单个主机的防火墙	62	6.2.8 操作系统和应用程序	98
4.5.4 硬件防火墙	63	6.2.9 防火墙提供的远程管理功能	98
第5章 防火墙的高级功能	64	6.2.10 拒绝服务 (DoS)	99
5.1 身份验证和授权	64	6.3 公布的防火墙漏洞	99
5.2 网络地址转换	65	6.3.1 Check Point FireWall-1 IP分片漏洞	99
5.2.1 静态NAT	66	6.3.2 Check Point FireWall-1 RDP头部	100
5.2.2 动态NAT	67	绕过防火墙的漏洞	100

6.3.3 Cisco PIX TACACS+的DoS漏洞	100	8.4 在Unix平台上安装FireWall-1	138
6.3.4 Raptor防火墙在代理HTTP请求中的漏洞	100	8.5 FireWall-1安装结束后再安装许可证	144
第7章 Check Point FireWall-1简介	101	第9章 配置FireWall-1	145
7.1 什么是FireWall-1	101	9.1 远程管理	145
7.2 FireWall-1组件	101	9.1.1 启用远程Windows GUI客户端	145
7.2.1 管理模块	102	9.1.2 登录Windows NT GUI策略编辑器	147
7.2.2 GUI客户端	102	9.1.3 启用远程Unix GUI客户端	147
7.2.3 FireWall-1的防火墙模块	104	9.1.4 登录Unix GUI策略编辑器	148
7.3 不同的管理模块配置	106	9.1.5 在分布式防火墙和管理模块之间建立连接	148
7.3.1 单设备防火墙 (Single Device Firewall)	107	9.1.6 策略编辑器菜单和工具条	149
7.3.2 拥有外部GUI客户端的单设备防火墙	107	9.1.7 策略属性	150
7.3.3 只有单个管理模块的多防火墙	107	9.2 创建FireWall-1规则库	156
7.3.4 有冗余管理模块的多防火墙	108	9.2.1 创建一个标准的NAT规则	157
7.3.5 一对一的防火墙模块和管理模块	109	9.2.2 准规则和显式规则	158
7.3.6 高可用性防火墙	109	9.2.3 清理规则	159
7.3.7 其他防火墙组件	110	9.2.4 隐藏规则	159
7.4 FireWall-1对象	110	9.2.5 FireWall-1的规则顺序	159
7.4.1 管理FireWall-1对象	110	第10章 FireWall-1高级功能	161
7.4.2 服务	119	10.1 身份验证	161
7.4.3 资源	122	10.1.1 用户身份验证	161
7.4.4 用户	124	10.1.2 客户身份验证	163
7.4.5 时间	125	10.1.3 会话身份验证	166
第8章 FireWall-1的安装	127	10.2 内容安全	168
8.1 许可证	127	10.3 内容向量协议	170
8.1.1 评估许可证	127	10.4 URL过滤协议	172
8.1.2 永久许可证	128	10.5 NAT	175
8.1.3 X/Motif许可证	128	10.6 账户管理客户端	180
8.2 FireWall-1的安装前提示	128	10.7 VPN和SecuRemote	182
8.2.1 安装哪一种FireWall-1组件	128	10.7.1 VPN的一些考虑	182
8.2.2 IP转发的考虑	128	10.7.2 网关到网关VPN	184
8.2.3 FireWall-1组件的连通性	130	10.7.3 SecuRemote	187
8.3 在Windows平台上安装FireWall-1	130	第11章 Check Point Next Generation	191
8.3.1 最小系统要求	130	11.1 新特征和功能增强概述	191
8.3.2 安装过程	130	11.1.1 NG的策略管理器	191
		11.1.2 增强的日志功能	192
		11.1.3 审计	193

11.1.4 TCP 服务属性	193	13.3.1 接口配置	225
11.1.5 增强的网络地址转换	194	13.3.2 电缆连接	226
11.1.6 NG对象数据库	194	13.3.3 初始PIX输入	226
11.1.7 进程监视	194	13.3.4 配置PIX	227
11.1.8 可视化策略编辑器	195	13.4 使用TFTP升级你的IOS	234
11.1.9 安全内部通信 (SIC)	195	第14章 Cisco PIX配置	237
11.1.10 SecureUpdate	196	14.1 路由选择	237
11.1.11 管理高可用性	196	14.1.1 静态	237
11.2 升级考虑	198	14.1.2 路由信息协议 (RIP)	238
11.3 在Windows上安装Check Point NG 防火墙	198	14.2 流量过滤和地址转换	239
11.4 在Unix上安装Check Point NG防火墙	201	14.2.1 管道 (conduit)	239
11.5 NG策略管理器的操作	203	14.2.2 静态 (static)	241
11.5.1 创建时间对象	203	14.2.3 Outbound/Apply命令	242
11.5.2 创建基本管理模块对象	205	14.2.4 NAT/Global	244
11.5.3 创建防火墙模块对象	206	14.2.5 访问表	245
11.6 使用SecureUpdate	207	第15章 Cisco PIX 高级功能	249
11.6.1 应用SecureUpdate进行产品管理	207	15.1 用户访问管理	249
11.6.2 许可证管理	208	15.1.1 访问PIX	249
第12章 Cisco PIX防火墙	210	15.1.2 通过PIX的流量	250
12.1 产品背景	210	15.2 流量管理	252
12.2 PIX的特征与功能	210	15.2.1 包管理	252
12.2.1 PIX模型	212	15.2.2 协议管理	254
12.2.2 PIX性能	214	15.3 冗余度	256
12.3 软件版本	215	15.4 PIX监控	258
12.3.1 PIX版本6.X	215	第16章 Cisco安全策略管理器	263
12.3.2 PIX 6.X版可以做的事与不 可以做的事	216	16.1 背景	263
12.3.3 PIX 版本5.3	216	16.1.1 应用区	263
12.4 自适应安全算法	216	16.1.2 操作流	264
第13章 Cisco PIX安装	221	16.2 安装	264
13.1 为PIX安装制定计划	221	16.3 拓扑图	267
13.2 安装前	222	16.3.1 创建拓扑图	267
13.2.1 选择许可证	222	16.3.2 查看拓扑图	272
13.2.2 选择PIX型号	223	16.4 策略设计	275
13.2.3 物理位置	224	16.4.1 网络对象组	276
13.3 安装	225	16.4.2 网络服务组	277
		16.4.3 创建规则集	278
		16.5 PIX命令	283

16.5.1 策略前的分发	284	18.3.5 允许IPSec VPN通过的防火墙	327
16.5.2 分发策略	288	18.3.6 实现服务类型 (TOS) 标记	328
16.6 报告	290	18.4 通过日志实现故障诊断	328
16.6.1 监控报告	291	18.5 防火墙实用工具	329
16.6.2 系统报告	291	18.5.1 Mason	329
第17章 Cisco IOS 防火墙特征集	293	18.5.2 Iptables-save和Iptables-restore	329
17.1 产品背景	293	18.5.3 Knetfilter	329
17.2 IOS防火墙的特征和功能	293	第19章 Symantec防火墙企业版的背景 与安装	330
17.2.1 IOS FFS阶段1的特征	293	19.1 Symantec/Raptor 6.5 的历史	330
17.2.2 IOS FFS阶段2的特征	294	19.1.1 对标准服务的支持	331
17.3 计划安装IOS防火墙的特征集	294	19.1.2 支持的验证类型	331
17.3.1 选择硬件平台	294	19.1.3 关于Symantec防火墙企业版6.5	332
17.3.2 选择软件特征集	295	19.1.4 Symantec防火墙企业版6.5的 重要特性	332
17.3.3 选择软件版本	296	19.1.5 代理	337
17.4 IOS防火墙设计考虑	296	19.2 安装	339
17.4.1 IOS 防火墙的强度	296	19.2.1 安装准备	339
17.4.2 警告	297	19.2.2 网络设置	340
17.4.3 IOS FFS设计示例	297	19.2.3 测试网络配置	346
17.5 安装和配置防火墙	298	19.2.4 测试TCP/IP的连通性	346
17.5.1 Cisco IOS的命令行界面	298	19.2.5 检查名称解析 (DNS)	346
17.5.2 记录IP和端口信息	300	19.2.6 ping主机	346
17.5.3 安装软件	300	19.2.7 理解网络如何处理名称解析	346
17.6 配置IOS FFS	302	19.2.8 提前约见Internet服务 提供商 (ISP)	347
17.7 配置CBAC	307	19.2.9 知道哪些服务需要通过安全网关	347
17.7.1 理解CBAC的工作原理	307	19.2.10 安装Symantec防火墙企业版6.5	347
17.7.2 配置访问控制表	308	19.2.11 安装Symantec Raptor管理控制台	348
17.7.3 配置检查规则	309	19.2.12 连接到Symantec防火墙企业版	349
17.7.4 打开告警和审计跟踪	311	19.2.13 安装远程日志记录	349
17.7.5 配置PAM	311	19.2.14 Vulture: 未授权的服务	349
第18章 Linux 内核防火墙—Iptables	312	第20章 Symantec防火墙企业版的配置	350
18.1 Linux 内核防火墙的发展	312	20.1 网络接口的配置	350
18.2 安装Iptables	317	20.2 配置网络实体	353
18.3 构建Iptables防火墙	317	20.3 用户和用户组的配置	357
18.3.1 独立主机	318		
18.3.2 简单的NAT 防火墙	320		
18.3.3 端口转发防火墙	322		
18.3.4 具有DMZ和透明Web代理 的防火墙	324		

20.3.1 定义用户组	358	22.2.1 多层防火墙	406
20.3.2 定义用户	358	22.2.2 基于策略的访问控制	407
20.4 配置Symantec和代理服务	365	22.3 ISA组件	408
20.4.1 Symantec 服务	365	22.3.1 服务器软件	408
20.4.2 代理服务	370	22.3.2 客户端软件	408
20.5 授权规则的填写	372	22.4 ISA操作模式	409
20.6 地址转换的配置	377	22.5 ISA管理	410
20.6.1 地址转换	378	22.5.1 本地管理	410
20.6.2 虚拟客户机	381	22.5.2 远程管理	411
第21章 Symantec防火墙企业版		22.6 报警	412
高级功能	383	22.6.1 条件	412
21.1 使用客户协议和服务	383	22.6.2 动作	414
21.1.1 定义一个GSP服务	383	22.7 日志	415
21.1.2 为过滤器中的应用定义协议	386	22.7.1 数据包过滤器日志	416
21.2 拒绝服务(DoS)	387	22.7.2 防火墙服务和Web代理日志	417
21.3 配置代理以支持第三方软件	388	22.7.3 方法	418
21.3.1 使用SQL*Net V2 代理	389	22.8 报表	420
21.3.2 代理连接小结	390	22.8.1 报表的产生	420
21.3.3 配置SQL*Net V2客户机	390	22.8.2 报表的日程安排	422
21.3.4 创建客户配置文件	390	第23章 微软ISA Server 2000的安装和	
21.3.5 H.323标准	391	配置	424
21.4 设定证书验证	396	23.1 微软ISA Server 2000安装准备	424
21.4.1 在主机上生成证书	396	23.2 软件安装	425
21.4.2 在Entrust CA服务器上生		23.2.1 初始安装	425
成一个证书	397	23.2.2 安全服务器向导	429
21.5 配置服务重新定向	399	23.2.3 从微软Proxy Server 2升级	432
21.5.1 使用服务重新定向	399	23.3 启动向导	433
21.5.2 给所支持的重新定向添加一个规则	400	23.3.1 创建日程表	434
21.6 通告方式的配置	400	23.3.2 创建客户端集	436
21.6.1 音频通告的配置	401	23.3.3 创建协议规则	437
21.6.2 邮件通告功能的配置	402	23.3.4 创建目标集	439
21.6.3 呼叫通告功能的配置	403	23.3.5 创建站点和内容规则	440
21.6.4 客户端程序通告的配置	404	23.3.6 为防火墙和SecureNAT客户端	
21.6.5 SNMP通告的配置	404	配置路由	441
第22章 微软ISA Server 2000综述	405	第24章 微软ISA Server 2000的高级功能	443
22.1 产品背景	405	24.1 包过滤器和入侵检测	443
22.2 ISA特征	406	24.2 报警管理	444

24.3 创建协议定义	445	28.5 Intranet防火墙	492
24.4 虚拟专用网络	446	28.6 DMZ地址	493
24.4.1 远程访问	446	28.7 高级NAT	494
24.4.2 站点到站点的VPN	447	28.8 以太网设置	495
24.5 应用程序过滤器	450	28.9 过滤	496
24.5.1 SMTP过滤器	451	28.9.1 种类标签	496
24.5.2 SMTP的体系结构	453	28.9.2 列表升级标签	497
24.6 高可用性	455	28.9.3 自定义标签	498
第25章 SonicWALL防火墙的 背景和管理	457	28.9.4 关键词标签	499
25.1 产品	457	28.9.5 赞同标签	500
25.2 6.2版的软件特征	459	28.10 VPN	501
25.3 SonicWALL的包处理	461	28.10.1 配置组VPN	501
25.4 SonicWALL的管理	461	28.10.2 客户端配置	502
第26章 安装SonicWALL	466	28.10.3 测试VPN客户端配置	503
26.1 物理安装	466	28.10.4 在两个SonicWALL设备之间 配置IKE	504
26.1.1 安装硬件	466	28.11 高可用性	507
26.1.2 物理安装过程	466	28.12 反病毒	511
26.2 初始化配置信息	467	28.12.1 反病毒小结	513
26.3 基于Web的配置向导	468	28.12.2 E-Mail过滤器	513
26.3.1 管理控制台配置	468	第29章 NetScreen防火墙的背景和管理	515
26.3.2 安装向导	468	29.1 背景	515
第27章 SonicWALL配置	474	29.1.1 产品和性能	515
27.1 安全策略示例	474	29.1.2 NetScreen应用产品	515
27.2 网络访问规则	475	29.1.3 NetScreen安全系统	518
27.3 网络访问规则类型和等级	475	29.2 ScreenOS操作系统	520
27.3.1 增加服务	476	29.2.1 ScreenOS的规则处理	521
27.3.2 通过服务确定的网络访问规则	477	29.2.2 ScreenOS特征集	523
27.3.3 创建和编辑规则	480	29.2.3 ScreenOS管理接口	523
27.3.4 增加和编辑用户	483	第30章 安装NetScreen	525
27.3.5 配置SNMP	485	30.1 NetScreen设备的安装	525
27.3.6 安全的远程管理	486	30.1.1 安装NetScreen-5XP	525
第28章 SonicWALL高级配置	487	30.1.2 安装NetScreen-25/50	527
28.1 日志	487	30.1.3 安装NetScreen-100	529
28.2 代理中继	488	30.2 NetScreen安全系统的安装	531
28.3 静态路由	489	30.2.1 安装NetScreen-500	531
28.4 DHCP服务器	490	30.2.2 架设NetScreen-500	532

30.2.3 在基本的单独配置下连接 NetScreen-500	533	第32章 NetScreen的高级配置	555
30.2.4 在冗余(HA)配置下连接 NetScreen-500	534	32.1 虚拟专用网	555
30.2.5 安装NetScreen-1000	535	32.1.1 手工密钥站点到站点的VPN配置	555
30.2.6 架设NetScreen-1000	536	32.1.2 高可用性配置	561
30.2.7 在独立配置下连接NetScreen-1000	536	32.1.3 用VIP进行负载平衡	562
30.2.8 在冗余配置下连接NetScreen-1000	536	32.1.4 带宽整形和优先化	564
第31章 NetScreen的配置	537	32.1.5 监控NetScreen设备	565
31.1 控制台初始化配置	537	32.1.6 ScreenOS的调试命令	565
31.2 用GUI进行NetScreen配置	540	32.2 NetScreen-1000设备的一个配置 文件示例	566

几乎与Internet一样众所周知的,还有那些费尽心机闯入他人计算机系统搞“黑客”(hacker)及其不怀好意的同党“骇客”(cracker)。不幸的是现如今闯入一个系统已不需要什么高深的计算机技巧,现在网上甚至有一个新词汇叫“脚本玩家”(script kiddie)。“脚本玩家”并没有什么神奇的计算机能力,而只是拥有一段专为发现和闯入他人系统而编写的程序。“脚本玩家”并不了解那些程序是如何进行攻击他人的,他们只知道如何去使用。甚至那些“脚本玩家”也随着在整个攻击过程中失去了作用,因为程序已经变得非常智能化,不用人参与就能完成对系统的扫描和破坏。这种情况使得近几年来攻击的频率、密度和受破坏市的资源发生了显著的增长。

Internet用户必须认识到这些地下活动是Internet的一个部分,而且这些地下活动最终会破坏你们的系统。Internet遍布了全球,而在这类机构却没有办法把哪怕只是一小撮黑客等阻挡之以外。但好在事情没有完全无望,我们可以使用很多工具来保护系统安全,其中防火墙是威力最大和最牢靠的武器,它使用那些技术能力只能在信息高速公路上网外游荡而不敢靠近。

本书可以作为设计、建造和维护当今最流行的火墙的重要指南。这个指南不仅适用于哪个供货商,同时既可用于指导新防火墙的实施,也可作为对正在使用的防火墙进行管理的参考。它涵盖了适合所有规模用户的有用信息,这些用户既包括大公司的防火墙管理员,也包括小办公室的网管、个人用户及普通爱好者。

1.1 防火墙的定义

防火墙的基本功能是对网络通信进行筛选过滤以防止未经授权的访问进出计算机网络。防火墙可以有不同的结构和规模,通常防火墙是由几台计算机组成的。在本书中,防火墙指的是位于可信网络(例如,内联网)和不可信网络(例如,Internet)之间并定期通过一定的网络流量进行筛查的一台或多台计算机。防火墙具有以下特性。

- 所有的通信都经过防火墙。

- 防火墙只放行经过授权的通信流量。

- 防火墙能够抵御针对其本身的攻击。

简而言之,防火墙就是可信网络和不可信网络之间的一个屏障。“防火墙”这个词实际是从物理上一种技术衍生而来的,这种技术通过用一堵由耐火材料筑成的墙体来阻止或延缓火蔓延蔓延。它本质上是一种障碍物。在网络中,防火墙是一个防范从其他网络发起的攻击的屏障。

防火墙既可以是一台服务器,一台个人电脑或一台主机,也可以是由多台主机组成的体系,它们被配置

第1章 简介

Internet确实已经成为了人类所构建的最丰富多彩的虚拟世界。其绝对用户的数目正成百上千地在世界各地增长,而且这种增长将一直持续下去。Internet这个虚拟世界欢迎每一个人前来做生意、相互沟通、研究信息或仅仅是享受网上冲浪的乐趣,其庞大的规模连同其使用者的互异性一起创建出了一个绝无仅有的融合体。此外,它也存在被误用、滥用和用来实施犯罪的可能性,而这种会导致危害的可能性使得用来保护Internet资源的安全措施和设备变得不可或缺。

几乎与Internet一样众所周知的,还有那些费尽心机闯入他人计算机系统的“黑客”(hacker)及其不怀好意的同党“破解者”(cracker)。不幸的是现如今闯入一个系统已不再需要什么高深的计算机技巧,现在词汇表里有一个新词儿叫“脚本玩家(script kiddie)”,“脚本玩家”其实没有什么神奇的计算机魔力,而只是拥有一段专为发现和闯入别人系统而编写的程序。“脚本玩家”并不了解那段程序是如何进行攻击闯入的,他仅仅知道如何去使用。甚至那些“脚本玩家”也逐渐在整个攻击过程中丧失了作用,因为程序已经变得非常智能化,不用人参与就能完成对系统的扫描和破坏。这种情况使得近几年来攻击的频率、密度和实施攻击的资源发生了显著的增长。

Internet用户必须认识到这些地下活动是Internet的一个部分,而且这些地下活动最终会发现你们的系统。Internet遍布于全球,而法律实施机构却没有办法把哪怕只是一小撮网络罪犯绳之以法。但好在事态没有完全失控,我们可以使用很多工具来保护系统安全。其中防火墙是威力最大和效果最好的武器,它使得那些邪恶势力只能在信息高速公路上到处游荡而不能得逞。

本书可以作为设计、构建和维护当今最流行防火墙的参考指南。这本指南不特定局限于哪个供货商,因而既可用于指导新防火墙的实施,也可作为对正在使用的防火墙进行管理的案头参考。它涵盖了适合所有类型用户的有用信息,这些用户既包括大公司的防火墙管理员,也包括小办公室的网管、个人用户及普通的爱好者。

1.1 防火墙的定义

防火墙的基本功能是对网络通信进行筛选屏蔽以防未经授权的访问进出计算机网络。防火墙可以有不同的结构和规模,通常防火墙是由几台计算机构成的。在本书中,防火墙指的是位于可信网络(例如,内部网)和不可信网络(例如,Internet)之间并对经过其间的网络流量进行检查的一台或多台计算机。防火墙有如下特性:

- 所有的通信都经过防火墙。
- 防火墙只放行经过授权的网络流量。
- 防火墙能经受得起对其本身的攻击。

简而言之,防火墙就是在可信网络和不可信网络之间的一个缓冲。“防火墙”这个词实际是从建筑上一种技术派生而来的,这种技术通过用一堵由防火材料建成的墙体来阻止或减缓火势的蔓延。它实质上是一种障碍物。在网络中,防火墙是一个防范从其他网络发起的攻击的屏障。

防火墙既可以是一台路由器、一台个人电脑或一台主机,也可以是由多台主机构成的体系,它们被配置

为专门保护一个私有网络，使其免受那些被处于可信网络之外的主机滥用的某些协议和服务的影响。一套防火墙系统通常位于一段网络的边界，例如某站点与Internet的连接处。然而，防火墙也能够而且应该被置于网络边界之内，因为这样可为一小批特定主机提供额外的、特殊的保护。

防火墙保护可信网络的办法在于它本身及其使用的策略/规则。下面是现今四类主要的防火墙技术：

- 包过滤器
- 应用级网关
- 电路级网关
- 状态包检查引擎

同所有的技术解决方案一样，防火墙技术也面临着其他产品和技术所面对的技术进步和生命周期的问题。第4章和第5章提供了更多关于不同防火墙类型和技术的详细信息。

1.2 为什么使用防火墙

人们要提的第一个问题可能是为什么要使用防火墙？把每个单独的系统配置好能经受住攻击不就行了吗？对此问题最简单的回答是：防火墙只专注于一件事——在已授权和未授权通信之间作出决断，这就避免了在安全性、可用性和功能上进行权衡和妥协。

如果没有防火墙，系统就只能依靠他们自己的安全设备和配置。这些系统可能正在运行升级功能或方便管理的服务，但这些服务可能并不十分安全，或不可信任，或者仅应从一个特定的位置才能被访问。防火墙可用于这种层次的访问控制。

如果周围没有防火墙，安全就完全仰仗主机自身了。而整个系统的安全将由系统中安全性最差的主机所决定。网络越大，把网络内所有主机维护至同样高的安全水平就越复杂。若一时粗心（例如只给15台Web服务器的14台打了关系安全的补丁），则因为简单的配置错误或未能修补所有漏洞就会导致闯入的发生。

防火墙成为了与不可信网络进行联络的惟一纽带，于是管理员就不用再确保多台机器要尽可能的安全了，他只要集中关注防火墙就行了。但这并不是说躲在防火墙里面的系统就不再需要严格的安全措施了，防火墙只是提供了一层避免错误的额外保护而已。

防火墙是一个优秀的审计员。因为所有的网络流量都经过它，那些包含在其日志中的信息可以用来重新构建新的事件以防安全出现缺口。

总之，防火墙减轻了系统被用于非法和恶意目的的风险（例如，被非法攻击者黑掉）。那么这些系统面临的被防火墙所防范的风险又是什么呢？企业的系统和数据有以下三个主要方面受到防火墙保护：

- **机密性的风险** 包括某方未经授权就访问敏感数据或数据的过早泄漏。一个商业公司很容易仅仅是因为泄漏了他们的商业计划、公司交易秘密或财务状况就损失数百万元。
- **数据完整性的风险** 包括未经授权就对数据进行修改，例如财务信息、产品特性或某网站上商品的价格。商业公司的成长和兴旺依赖于其信息系统提供信息的准确性，如果系统信息是不可靠的，那又怎能作出最好的决策（比如销售水平如何？哪一个可用账户是准确的）？
- **可用性的风险** 系统可用性保证系统可以适时地为用户服务（就是说用户需要用它的时候）。那些不可用的系统导致公司损失了大量的财政收入和雇员的生产效率，同时也无形中挫伤了消费者对公司的信心并损坏了公司的公众形象。

1.3 常见攻击类型

前面的几节介绍了为什么个人和团体要使用防火墙。现在的问题是，到底那些攻击是怎样未经授权就获

取了系统访问权？关于攻击的动机不胜枚举，从“看看是否能行得通”到使用一个已被侵害的系统进攻另一个系统，再到协作刺探，甚至仅仅是想把系统搞垮和破坏掉这样简单的恶意动机。

见诸文字的有几十种不同的方法可以使闯入者获取系统的访问权。第6章提供了一些补充的关于对防火墙进行攻击的常见方法的信息。本章在这里只是简要列出了最常见的攻击方法：

- **社交工程** 攻击者哄骗系统管理员或其他授权用户，让他们透露出其登录信息或系统操作的细节。
- **软件错误** 攻击者钻研出了程序的漏洞并能使一个应用程序或服务未经授权就强制运行，他还可以强制运行一些恶意命令。这种攻击在程序运行时带有其他权限或管理权限的情况下尤为危险。这种漏洞通常是指“缓冲区溢出攻击”或“格式化字符串攻击”。

注意 想了解更多关于“缓冲区溢出攻击”或“格式化字符串攻击”的信息，请参考以下网址：

<http://www.insecure.org/stf/smashstack.txt>

http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html

<http://julianor.tripod.com/teso-fs1-1.pdf>

- **病毒和特洛伊木马** 攻击者诱骗一个合法用户执行某个攻击程序。最常用的做法是把攻击程序伪装成一个看起来没什么问题的电子邮件或藏在某个病毒里面。一旦被执行，攻击程序就会执行一系列恶意操作，包括安装后门程序、盗取文件和机密甚至删除文件。
- **脆弱的系统配置** 攻击者能够通过其可获得的服务和账户研究出系统的错误。通常这些错误包括没有改变默认账户的密码（既有系统级的也有应用级的）、未限制对应用管理程序的访问或是没有禁止多余的和未用的服务。

除了试图进行未授权系统访问之外，一些恶意的人可能只是想把系统搞垮。对于那些重要的而又被广泛关注的系统应用，由此造成的商业损失将会非常惨重。这些攻击被称为拒绝服务（denial of service, DoS）攻击，它是指某个用户、网络或组织被剥夺了他们通常享有的资源和服务。而某些服务的丧失通常也意味着有关个体网络服务的失效，例如电子邮件和Web服务，有时还会造成网络连接的暂时丢失。

1.4 防火墙的部署

尽管第3章还将对网络设计和防火墙部署有一个更深入地探讨，在这里我们先引出几个话题。防火墙可以并应该安装于两个有不同安全要求的网络互联之处，最常见的是被置于本地网和Internet相连的地方。而其他常见的防火墙应用还包括保护与第三方的连接，比如与市场数据提供商的连接，以及保护网络内部的与敏感数据的连接。

在讨论网络的时候，本书使用了“网络边界”（network perimeter）这个概念，这个概念是指一个本地网络的整个边界。本地网络通过输入点和输出点与其他网络（例如Internet）相连，这些连接点几乎都装有防火墙。

表面看起来“网络边界”的定义是很简单的，但是随着虚拟专用网络（Virtual Private Network, VPN）的出现，原来很确切的边界变得模糊了。虚拟专用网络技术允许一个远端用户通过防火墙连入一个网络就好像他在网络内部一样。这已经成为一种公司网络的扩展，但是那些外面的主机无法再受到公司防火墙的保护了。那些恶意的攻击者可以先攻破那些外面的用户并通过这种渠道穿过公司的防火墙。管理员应该考虑为那些外面的系统安装个人防火墙以期达到获得一致安全水平的目的。

1.5 防火墙的优势和弱点

防火墙仅仅是整体安全构架的一个部分。然而作为一个比较独立的部分，防火墙的设计应该满足整体设

计中的至关重要的安全需求。和其他事物一样，防火墙也有它的优势和弱点。

1.5.1 优势

一般防火墙有以下优势：

- 防火墙可以出色地完成执行公司整体安全策略的任务。经过适当配置，防火墙应能把通信约束在管理决策所能接受的范围之内。
- 防火墙可用于限制对某些特殊服务的访问。举例来说，防火墙可以允许公众访问Web服务器但禁止他们访问Telnet端口和其他非公开的域。大多数防火墙可以提供在授权机制下的有选择性访问服务。
- 防火墙功能专一。因此，不必在安全性和可用性之间进行什么权衡妥协。
- 防火墙有出色的审计功能。若有足够的磁盘空间或远程记录功能，防火墙能够存录所有经过的网络流量。
- 防火墙可以向相关人员发出警告信息。

1.5.2 弱点

一般来说防火墙有如下弱点：

- 防火墙不能防范经过授权的东西。你可能会奇怪这是什么意思，这就是说防火墙允许其所保护的系统应用的正常通信流量通过防火墙——否则就不对了。如果一个应用程序自身就有错误，那么防火墙也不会阻止由此引起的攻击，因为对于防火墙来说，这是经过授权的。
- 防火墙只是按对其配置的规则进行有效的工作。一个过于随意的规则配置可能会减弱防火墙的功效。
- 防火墙对于社交工程类型的攻击或一个授权用户利用合法访问进行的恶意攻击不起作用。
- 防火墙不能修复脆弱的管理措施或设计有问题的安全策略。
- 防火墙不能阻止那些不经过它的攻击。

1.6 完善的安全措施

虽然关于如何最有效地配置和管理防火墙的完整讨论已经超出本书范围（关于这个话题可以找到很多书），但对一些能够提高防火墙整体安全性能的重要概念作些介绍还是很有益处的。这些概念既可用于防火墙也可用于被防火墙保护的系统。同时请注意，以下介绍的概念和措施相互间并非是排斥的，如果能适当地综合应用，将会获得更高的安全保障水平。

1.6.1 完善系统本身

除了在一些非常罕见的场合，一般系统和其应用程序并非是按最安全的要求安装的。往往会有一些对你系统的功能而言额外的服务被安装上并默认为激活状态，一种好的习惯是只开放系统所提供的服务和最必须的账户。很多闯入的发生都是由于那些对系统而言多余的服务和账户被攻破。这种禁止多余服务和为提高安全性而进行重新配置的措施经常被称作“主机加固”（host hardening）。下面是进行主机加固时可用的一个较小的检查列表：

- 禁止所有的不需要的或不必须的服务。
- 删除不需要的账户和组。更改默认的应用程序和系统账户的密码或干脆禁止它们。禁止那些不需要交互式登录的账户。
- 重新配置剩余的服务以提高安全性。
- 保证所有的管理功能的安全。

- 使用强健的密码。强健的密码是指由多于7个字符并有大写字母、小写字母、数字和其他字符混合构成的密码。

注意 SANS（系统管理监测与网络安全研究所，www.sans.org）出版了一些关于操作系统最佳安全措施指南。

1.6.2 补丁

如今连绵不绝出现的各种补丁可能会使人们感到不安而且经常会被遗忘。新的攻击很快就会被发现，一个一分钟前还算安全的系统转眼就会变得无比脆弱。若想让系统总是处于最安全状态，就应订阅多份错误提醒邮件列表和软件供货商的邮件列表。比较流行的漏洞提醒服务由以下组织进行维护：

- 由ISS（Internet Security Systems）维护的xforce数据库及邮件列表。

其网址为<http://www.iss.net/xforce>。

- 由SecurityFocus维护的Bugtraq（一个黑客组织的邮件组）存档的拷贝及邮件列表。

其网址为<http://www.securityfocus.com>。

- CERT（Computer Incident Emergency Response Team，计算机事故紧急响应小组）的网址为<http://www.cert.org>。

- CVE（Common Vulnerabilities and Exposures，常见弱点曝光）数据库的网址为<http://www.cve.mitre.org>。

注意 打了补丁之后，应该确认系统安全性没有被削弱。例如Sun就曾经因为他们发布的Solaris操作系统的补丁把已经禁止的服务重新启用而坏了他们的名声。

1.6.3 硬件与操作系统

早些时候防火墙都是运行于通用操作系统如Windows NT和Unix之上的软件，它们通过修改系统的内核和TCP/IP协议栈来监测流量。所以防火墙的性能就与其所运行的操作系统所存在的问题休戚相关。要想获得较高的安全性，就必须对操作系统进行加固、修补和维护（如前几节所述）。如果没有足够的专业人士或时间来维护一个操作系统的功能，那么这些工作将是既费时又困难的。然而，现在已经有很多防火墙供货商把他们的产品作成硬件了。

硬件防火墙集成了操作系统和防火墙软件的功能，形成了一个整体牢固、功能专一的设备。在集成的过程中，那些对于筛选屏蔽数据包不必要的功能被删除掉了。此外，这种产品提供了功能完善的管理接口，使得防火墙的配置和维护得到了进一步的简化。硬件防火墙在使用时不需要作很多主机加固的工作（当然改变默认密码还是必要的）。管理员不用再费心于重新配置和修补通用操作系统，而是可以集中注意力构思防火墙规则，同原来基于操作系统的软件防火墙相比，硬件防火墙显著地减少了操作和维护的费用。本书将探讨很多硬件防火墙，其中包括Cisco PIX、Netscreen、SonicWall以及运行于Nokia IPSO平台上的CheckPoint FireWall-1。

1.6.4 层次防御

虽然防火墙本身是一个出色的安全工具，但我们并不能完全依靠它。前面曾经提到，防火墙不能防范那些拥有授权的通信。当一个人侵者绕过防火墙又会怎样呢？可以设想如下情况：一个人侵者通过HTTP访问Web服务器并获取了系统shell访问权限。由于通过HTTP访问Web服务器是合法的所以防火墙允许这种访问通过，攻击者可以利用这一点并通过这个渠道去攻击网络上其他的服务器和系统，而这时已没有了防火墙