

<<Cisco安全PIX防火墙>>

图书基本信息

书名：<<Cisco安全PIX防火墙>>

13位ISBN编号：9787115103888

10位ISBN编号：7115103887

出版时间：2002-8

出版时间：第1版 (2002年1月1日)

作者：Chapman

页数：285

译者：刘兴初

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<Cisco安全PIX防火墙>>

内容概要

本书详细介绍了配置、验证并管理PIX防火墙产品系列的相关知识，内容包括黑客的常见攻击手段，网络内部和外部的安全威胁；不同型号PIX防火墙的特点等内容。

<<Cisco安全PIX防火墙>>

书籍目录

第1章 网络安全介绍

- 1.1 为什么网络安全是必需的
- 1.2 定义安全的网络设计
- 1.3 网络安全威胁分类
- 1.4 网络安全是如何被破坏的
 - 1.4.1 侦察攻击
 - 1.4.2 访问攻击
 - 1.4.3 DoS攻击
- 1.5 网络安全策略和安全轮图
- 1.6 小结
- 1.7 复习题

第2章 Cisco PIX防火墙软件和硬件

- 2.1 防火墙的类型
 - 2.1.1 数据包过滤器
 - 2.1.2 代理过滤器
 - 2.1.3 状态型数据包过滤器
- 2.2 PIX防火墙逻辑
- 2.3 PIX防火墙的型号
- 2.4 复习题

第3章 使用并升级Cisco PIX防火墙软件映像

- 3.1 PIX命令行接口
- 3.2 维护并测试PIX防火墙
- 3.3 在PIX防火墙上安装一个新的OS
 - 3.3.1 升级到PIX防火墙的一个不同版本
 - 3.3.2 使用监视模式升级到一个不同的PIX OS
 - 3.3.3 安装PIX OS 5.0和更早的版本
 - 3.3.4 安装PIX OS 5.1和更新的版本
 - 3.3.5 用Windows PC创建一张启动帮助(Boothelper)磁盘
 - 3.3.6 用UNIX、Solaris或Linux工作站创建一张启动帮助磁盘
 - 3.3.7 为具有软盘驱动器的PIX防火墙安装并使用启动帮助程序
- 3.4 口令恢复
 - 3.4.1 对于PIX Classic、PIX 10000、510和520的软盘口令恢复
 - 3.4.2 对于PIX 506、515、525和535的TFTP口令恢复
- 3.5 复习题

第4章 配置Cisco PIX 防火墙

- 4.1 ASA安全级别
- 4.2 配置Cisco PIX防火墙的6个基本命令
 - 4.2.1 nameif命令
 - 4.2.2 interface命令
 - 4.2.3 ip address命令
 - 4.2.4 nat命令
 - 4.2.5 global命令
 - 4.2.6 route命令
- 4.3 复习题

第5章 Cisco PIX防火墙翻译

<<Cisco安全PIX防火墙>>

5.1 传输协议

5.1.1 传输控制协议

5.1.2 用户数据报协议

5.2 PIX防火墙翻译

5.2.1 静态地址翻译

5.2.2 动态地址翻译

5.2.3 翻译和连接

5.3 复习题

第6章 配置通过Cisco PIX 防火墙的访问

6.1 配置通过PIX防火墙的访问

6.2 理解静态翻译和管道命令

6.2.1 static命令

6.2.2 conduit命令

6.3 穿过PIX进行访问的其他方法

6.3.1 配置PAT

6.3.2 配置nat 0

6.3.3 配置FIXUP协议

6.3.4 多媒体支持

6.4 配置多个接口

6.5 复习题

第7章 系统日志

7.1 系统日志消息

7.2 系统日志配置

7.2.1 logging host命令

7.2.2 logging trap命令

7.2.3 logging buffered命令

7.2.4 logging console命令

7.2.5 logging facility命令

7.2.6 logging monitor命令

7.2.7 logging standby命令

7.2.8 logging timestamps命令

7.2.9 (no)logging message命令

7.2.10 show logging命令

7.2.11 clear logging命令

7.3 依据不同版本的、新的系统日志消息

7.4 复习题

第8章 Cisco PIX防火墙上的AAA配置

8.1 定义AAA

8.2 直通式代理的操作运行

8.3 支持的AAA服务器

8.4 安装用于Windows NT的CSACS

8.5 配置认证

8.5.1 其他服务的认证

8.5.2 虚拟Telnet

8.5.3 虚拟HTTP

8.5.4 控制台访问的认证

8.5.5 改变认证超时时间

<<Cisco安全PIX防火墙>>

8.5.6 改变认证提示

8.6 配置授权

8.6.1 为CSACS-NT增加授权规则

8.6.2 其他服务的授权

8.7 配置审计

8.7.1 用CSACS-NT查看审计记录

8.7.2 其他服务的审计

8.8 检验配置

8.9 复习题

第9章 Cisco PIX防火墙高级协议处理和攻击防卫

9.1 对高级协议处理的需求

9.1.1 标准模式的FTP

9.1.2 被动模式的FTP

9.1.3 fixup protocol FTP命令

9.1.4 远程命令解释程序(rsh)

9.1.5 SQL*Net

9.2 多媒体支持

9.2.1 实时流协议(RTSP)

9.2.2 H.323

9.3 攻击防卫

9.3.1 邮件防卫

9.3.2 DNS防卫

9.3.3 碎片攻击防卫

9.3.4 AAA风暴攻击防卫

9.3.5 SYN风暴攻击防卫

9.4 总结

9.5 复习题

第10章 Cisco PIX防火墙故障切换

10.1 故障切换操作

10.1.1 故障切换电缆

10.1.2 配置复制

10.1.3 故障切换监视

10.1.4 故障恢复

10.2 配置故障切换

10.3 实验练习

10.3.1 任务1：配置主PIX防火墙，使它可以在发生故障时切换到PIX防火墙

10.3.2 任务2：强制让主PIX防火墙再次回到活跃状态

10.3.3 任务3：为主PIX防火墙配置状态型故障切换

10.4 复习题

第11章 为Cisco PIX防火墙配置IPSec

11.1 Cisco安全PIX防火墙支持安全的VPN

11.1.1 PIX、VPN和IPSec

11.1.2 IPSec

11.1.3 IKE

11.1.4 SA

11.1.5 DES

11.1.6 3DES

<<Cisco安全PIX防火墙>>

- 11.1.7 D-H
- 11.1.8 MD5
- 11.1.9 SHA-1
- 11.1.10 RSA签名
- 11.1.11 CA
- 11.2 配置PIX防火墙的IPSec支持
 - 11.2.1 任务1：为IPSec做准备
 - 11.2.2 任务2：为预共享密钥配置IKE
 - 11.2.3 任务3：配置IPSec
 - 11.2.4 任务4：测试并检验IPSec的总体配置
- 11.3 扩展PIX防火墙VPN
 - 11.3.1 PIX防火墙的CA注册
- 11.4 案例学习1：使用预共享密钥为点对点主机配置PIX防火墙IPSec
 - 11.4.1 网络安全策略
 - 11.4.2 PIX 1防火墙的配置实例
 - 11.4.3 PIX 2防火墙的配置实例
- 11.5 案例学习2：使用预共享密钥的三个站点完全网状连接IPSec隧道
 - 11.5.1 网络安全策略
 - 11.5.2 Portland、Seattle和San Jose PIX防火墙的配置实例
- 11.6 总结
- 11.7 复习题
- 11.8 参考文献
- 第12章 Cisco IOS防火墙基于上下文的访问控制
 - 12.1 Cisco IOS防火墙简介
 - 12.1.1 基于上下文的访问控制
 - 12.1.2 认证代理
 - 12.1.3 入侵检测
 - 12.2 基于上下文的访问控制的操作运行
 - 12.2.1 配置CBAC
 - 12.2.2 配置CBAC
 - 12.2.3 将检查规则和ACL应用到路由器接口上
 - 12.2.4 测试、检验并监视CBAC
 - 12.3 复习题
- 第13章 Cisco IOS防火墙认证代理配置
 - 13.1 IOS认证代理简介
 - 13.2 认证代理配置任务
 - 13.2.1 AAA服务器配置
 - 13.2.2 AAA配置
 - 13.2.3 认证代理配置
 - 13.2.4 测试并检验配置
 - 13.2.5 认证代理服务配置实例
 - 13.3 复习题
- 附录A 为入侵检测配置PIX
 - A.1 PIX入侵检测简介
 - A.2 入侵检测配置要素
 - A.2.1 以接口为单位配置审计策略
 - A.2.2 从审计策略中选择性地禁用IDS特征

<<Cisco安全PIX防火墙>>

- A.3 PIX IDS配置实例
- A.4 PIX IDS特征
- A.5 常见问题的问答
- A.6 推荐读物列表
- 附录B 在PIX防火墙上配置SNMP协议
 - B.1 理解PIX对SNMP的支持
 - B.2 从PIX上检索SNMP数据
 - B.2.1 MIB浏览
 - B.2.2 SNMP陷阱
 - B.2.3 配置PIX来允许浏览MIB并发送系统日志陷阱
 - B.3 SNMP v1 MIB-II目录
 - B.4 网络上的SNMP资源
- 附录C 在PIX防火墙上配置动态主机配置协议(DHCP)
 - C.1 DHCP基础
 - C.2 DHCP服务器
 - C.3 DHCP客户端
 - C.4 配置实例
 - C.4.1 PIX 506作为DHCP服务器：静态外部地址
 - C.4.2 PIX 506作为DHCP客户端：动态获取的外部地址
 - C.5 互联网上的DHCP资源
- 附录D 在PIX防火墙上配置安全Shell(SSH)
 - D.1 安全Shell(SSH)简介
 - D.2 为SSH访问配置PIX
 - D.2.1 配置PIX来接受SSH连接
 - D.2.2 配置SSH客户端来连接到PIX
 - D.3 SSH客户端连接的故障诊断
 - D.4 为我们的平台获取一个SSH客户端软件
- 附录E 安全资源
- 附录F 复习题答案

<<Cisco安全PIX防火墙>>

媒体关注与评论

本书详细介绍了配置、验证并管理PIX防火墙产品系列的相关知识，内容包括黑客的常见攻击手段，网络内部和外部的安全威胁；不同型号PIX防火墙的特点，升级所需要完成的任务；基本的安装细节，以及如何启用更高级的特性和访问控制；采用PIX系统日志服务和PIX AAA子系统的管理和监测；配置PIX故障切换机制，PIX上的IPSec，以及Cisco IOS防火墙特性集。

附录提供了一些很有帮助的参考，包括配置PIX入侵检测特性、SNMP管理支持、DHCP客户端和服务器的安全Shell协议(SSH)连接，以及许多与安全相关的资源。

本书适合那些准备参加Cisco Security Specialist 1认证考试的人员。
本书还适合那些想理解并更有效地使用PIX防火墙的网络管理人员。

<<Cisco安全PIX防火墙>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>