

<<管理CISCO网络安全>>

图书基本信息

书名：<<管理CISCO网络安全>>

13位ISBN编号：9787115097187

10位ISBN编号：7115097186

出版时间：2001-11-1

出版时间：人民邮电出版社

作者：MichaelWenstrom

页数：602

字数：948000

译者：李逢天

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>

## <<管理CISCO网络安全>>

### 内容概要

基于同名的培训课程，《管理Cisco网络安全》一书集中介绍了如何实施IP网络的安全。

本书分为六个部分。

第一部分教给读者如何建立网络安全策略和保护网络基础设施方面的信息。

第二部分描述用CiscoSecure ACS和Cisco IOS软件AAA安全特性来保护远程拨号访问安全的方法。

第三部分集中讲述通过识别边界安全系统的基本组件和配置边界路由器及Cisco防火墙特性集来保护Internet访问安全。

第四部分向读者介绍PIX防火墙的特性和组件，提供了有关如何配置基本PIX防火墙特性的详细信息。

第五部分剖析Cisco加密技术（CET），并教给读者如何配置CET来确保数据私密性。

在第六部分中，读者将学习如何用IP安全（IPSec）特性来实施一个安全的虚拟专用网络（VPN）解决方案，以及如何使用入侵检测和网络统计工具。

本书是MCNS培训课程的正式教材，同时也适合作为广大网络管理人员的参考书，用以设置、维护网络安全。

## <<管理CISCO网络安全>>

### 作者简介

Michael Wenstrom是Cisco Systems公司的培训专员，他设计、开发和交付关于Cisco虚拟专用网络和网络安全产品方面的培训。

Mike在技术培训方面有18年以上的经验，他做过指导设计人、课程开发人，技术指导人和项目经理。

## &lt;&lt;管理CISCO网络安全&gt;&gt;

## 书籍目录

第一部分 建立网络安全策略 第1章 评估网络安全威胁 1.1 我们为什么需要网络安全 1.2 我们为什么会有安全问题 1.2.1 安全问题的三个主要原因 1.2.2 了解敌人：入侵者在想什么 1.3 安全威胁类型 1.3.1 侦察 1.3.2 非授权访问 1.3.3 拒绝服务 (Denial of Service) 1.3.4 数据操纵 (Data Manipulation) 1.4 安全机会 1.5 小结 1.6 复习题 1.7 参考文献 1.7.1 网络安全和商务 1.7.2 攻击 (hacking) 和黑客 (hacker) 工具 1.7.3 安全Web站点 1.7.4 安全调研与报告 1.7.5 网络入侵者报导 第2章 评估网络安全策略 2.1 保护网络的重要性 2.2 安全状况评估过程 2.2.1 评估网络安全策略 2.2.2 XYZ公司的网络安全策略 2.2.3 保护网络的安全 2.2.4 监视网络安全 2.2.5 通过安全审计测试网络安全 2.3 改善网络安全状况 2.4 网络安全案例研究 2.4.1 案例研究1：开放的安全策略 2.4.2 案例研究2：有限的安全策略 2.4.3 案例研究3：严密的安全策略 2.4.4 案例研究小结 2.5 小结 2.6 案例学习：评估XYZ公司的网络安全策略 2.6.1 案例学习背景介绍 2.6.2 案例学习背景问题的答案 2.7 复习题 2.8 参考文献 2.8.1 开发安全策略 2.8.2 安全策略示例和指导原则 2.8.3 对安全事件报告有用的事件响应中心 2.8.4 其他安全Web站点 第3章 保护网络基础设施的安全 3.1 园区网安全问题和解决方案 3.2 保护设备的物理安全 3.3 保护管理接口的安全 3.3.1 保护控制台 (console) 端口访问安全 3.3.2 使用口令加密 3.3.3 细调线路参数 3.3.4 设置多个特权级别 3.3.5 设置设备标识 (banner) 消息 3.3.6 控制Telnet访问 3.3.7 控制SNMP访问 3.4 保护路由器到路由器的通信安全 3.4.1 路由协议认证 3.4.2 保护路由器配置文件的安全 3.4.3 用过滤器控制数据流 3.4.4 抑制从路由更新中收到的路由 3.4.5 进入网络过滤器 3.4.6 用安全策略控制数据流的一个简单例子 3.4.7 控制对路由器的HTTP访问 3.5 保护以太网交换机的安全 3.5.1 控制以太网交换机的管理访问 3.5.2 以太网交换机的端口安全 3.5.3 以太网交换机的访问安全 3.6 小结 3.7 案例学习：配置基本的网络安全 3.7.1 案例学习背景介绍 3.7.2 拓扑结构 3.7.3 网络安全策略 3.7.4 路由器R2的配置样例 3.8 复习题 3.9 参考文献 3.9.1 通用路由器安全配置 3.9.2 标准和扩展访问列表 3.9.3 SNMP 3.9.4 相邻路由器认证 3.9.5 以太网交换机安全 第二部分 拨号(Dialup)安全 第4章 分析Cisco AAA安全技术 第5章 配置网络接入服务器使用AAA安全特性 第6章 配置Cisco Secure ACS和TACACS+/RADIUS 第三部分 保护Internet连接安全 第7章 配置Cisco边界路由器 第8章 配置Cisco IOS防火墙 第四部分 配置Cisco Secure PIX防火墙 第9章 PIX防火墙基础 第10章 配置通过PIX防火墙访问 第11章 在PIX防火墙上配置多个接口和AAA 第12章 配置PIX防火墙高级特性 第五部分 配置Cisco加密技术 第13章 Cisco加密技术概览 第14章 配置Cisco加密技术 第六部分 用IPSec配置VPN 第15章 理解Cisco对IPSec的支持 第16章 配置Cisco IOS IPSec 第17章 配置PIX防火墙对IPSec的支持 第18章 扩展Cisco IPSec网络 第七部分 附录

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>