

图书基本信息

书名：<<思科网络技术学院教程 CCNA安全>>

13位ISBN编号：9787115301123

10位ISBN编号：7115301123

出版时间：2013-1

出版时间：人民邮电出版社

作者：Cisco Networking Academy

页数：338

字数：643000

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>

内容概要

《思科网络技术学院教程 CCNA安全(第2版)》所介绍的内容是针对思科网络技术学院最新的认证项目之一——

CCNA安全课程，作为思科网络学院的指定教材，该书面向的读者群需要具备CCNA水平的知识。

《思科网络技术学院教程

CCNA安全(第2版)》共分10章，第1章介绍了现代网络安全威胁相关的知识，让大家了解网络安全发展的历史和现状，以及病毒、蠕虫和木马为典型代表的各种攻击的特点和防范。

随后的三章主要侧重于如何防止外部网络对内部网络的攻击，比如如何加强对路由器的保护、AAA认证以及防火墙技术和部署。

第5章介绍了如何对内部网络自身的保护，强调了网络入侵防御系统(IPS)的特点和在思科设备上的实现。

第6章是针对局域网的安全防护，主要侧重于对于交换网络的安全部署及配置。

第7章介绍了加密算法，普及了加密技术的基本知识。

第8章是本书的重要环节，介绍了使用路由器来实现虚拟专用网(VPN)技术，特别是IPSec技术的概念和配置。

第9章综合了前面的内容，介绍了如何设计和部署一个安全网络的全面解决方案，以及如何制定有效的安全策略等。

第10章对Cisco

ASA防火墙配置和VPN配置的实施进行了详细介绍。

《思科网络技术学院教程 CCNA安全(第2版)》所介绍的内容涵盖了思科认证考试——CCNA安全(IINS

640-554)要求的全部知识，因此适合准备该认证考试的读者阅读。

对网络安全感兴趣的读者也可以从中获益。

作者简介

思科网络技术学院 (Cisco Networking Academy Program) 是由思科公司联合世界范围内的教育机构、公司、政府和国际组织一起努力推广的以网络技术为主要内容的教育项目。其目的就是为了让更多的年轻人学习最先进的网络技术知识，帮助教育机构克服资金和技术两大瓶颈，为互联网时代做准备。

书籍目录

第1章 现代网络安全威胁

- 1.1 一个安全网络的基本原则
 - 1.1.1 网络安全的演进
 - 1.1.2 网络安全的驱动者
 - 1.1.3 网络安全组织
 - 1.1.4 网络安全领域
 - 1.1.5 网络安全策略
- 1.2 病毒、蠕虫和特洛伊木马
 - 1.2.1 病毒
 - 1.2.2 蠕虫
 - 1.2.3 特洛伊木马
 - 1.2.4 缓解病毒、蠕虫和特洛伊木马
- 1.3 攻击方法
 - 1.3.1 侦查攻击
 - 1.3.2 接入攻击
 - 1.3.3 拒绝服务攻击
 - 1.3.4 缓解网络攻击
- 1.4 Cisco网络基础保护框架

第2章 保护网络设备

- 2.1 保护对设备的访问
 - 2.1.1 保护边界路由器
 - 2.1.2 配置安全的管理访问
 - 2.1.3 为虚拟登录配置增强的安全性
 - 2.1.4 配置SSH
- 2.2 分配管理角色
 - 2.2.1 配置特权级别
 - 2.2.2 配置基于角色的CLI访问
- 2.3 监控和管理设备
 - 2.3.1 保证Cisco IOS和配置文件的安全
 - 2.3.2 安全管理和报告
 - 2.3.3 使用系统日志
 - 2.3.4 使用SNMP实现网络安全
 - 2.3.5 使用NTP
- 2.4 使用自动安全特性
 - 2.4.1 执行安全审计
 - 2.4.2 使用AutoSecure锁定路由器
 - 2.4.3 用CCP锁定路由器

第3章 认证、授权和记账

- 3.1 使用AAA的目的
 - 3.1.1 AAA概述
 - 3.1.2 AAA的特点
- 3.2 本地AAA认证
 - 3.2.1 使用CLI配置本地AAA认证
 - 3.2.2 使用CCP配置本地AAA认证
 - 3.2.3 本地AAA认证故障处理

3.3 基于服务器的AAA

3.3.1 基于服务器AAA的特点

3.3.2 基于服务器AAA通信协议

3.3.3 Cisco安全ACS

3.3.4 配置Cisco安全ACS

3.3.5 配置Cisco安全ACS用户和组

3.4 基于服务器的AAA认证

3.4.1 使用CLI配置基于服务器的AAA认证

3.4.2 使用CCP配置基于服务器的AAA认证

3.4.3 基于服务器的AAA认证故障处理

3.5 基于服务器的AAA授权和记账

3.5.1 配置基于服务器的AAA授权

3.5.2 配置基于服务器的AAA记账

第4章 实现防火墙技术

4.1 访问控制列表

4.1.1 用CLI配置标准和扩展IP ACL

4.1.2 使用标准和扩展IP ACL

4.1.3 ACL的拓扑和流向

4.1.4 用CCP配置标准和扩展ACL

4.1.5 配置TCP的Established和自反ACL

4.1.6 配置动态ACL

4.1.7 配置基于时间的ACL

4.1.8 复杂ACL实现的排错

4.1.9 使用ACL缓解攻击

4.1.10 IPv6 ACL

4.1.11 在ACE中使用对象组

4.2 防火墙技术

4.2.1 使用防火墙构建安全网络

4.2.2 防火墙类型

4.2.3 网络设计中的防火墙

4.3 基于上下文的访问控制

4.3.1 CBAC特性

4.3.2 CBAC运行

4.3.3 配置CBAC

4.3.4 CBAC排错

4.4 区域策略防火墙

4.4.1 基于策略防火墙的特点

4.4.2 基于区域策略的防火墙运行

4.4.3 用CLI配置区域策略防火墙

4.4.4 用CCP向导配置区域策略防火墙

4.4.5 使用CCP手动配置基于区域的策略防火墙

4.4.6 区域策略防火墙排错

第5章 执行入侵防御

5.1 IPS技术

5.1.1 IDS和IPS特性

5.1.2 基于网络的IPS执行

5.2 IPS特征

- 5.2.1 IPS特征特性
- 5.2.2 IPS特征警报
- 5.2.3 调整IPS特征报警
- 5.2.4 IPS特征行动
- 5.2.5 管理和监视IPS
- 5.2.6 IPS全局关联
- 5.3 执行IPS
- 5.3.1 使用CLI配置Cisco IOS IPS
- 5.3.2 使用CCP配置Cisco IOS IPS
- 5.3.3 修改Cisco IOS IPS特征
- 5.4 检验和监测IPS
- 5.4.1 检验Cisco IOS IPS
- 5.4.2 监测Cisco IOS IPS
- 第6章 保护局域网
- 6.1 终端安全
- 6.1.1 终端安全概述
- 6.1.2 使用IronPort的终端安全
- 6.1.3 使用网络准入控制的端点安全
- 6.2 第二层安全考虑
- 6.2.1 第二层安全概述
- 6.2.2 MAC地址欺骗攻击
- 6.2.3 MAC地址表溢出攻击
- 6.2.4 STP操纵攻击
- 6.2.5 LAN风暴攻击
- 6.2.6 VLAN攻击
- 6.3 配置第二层安全
- 6.3.1 配置端口安全
- 6.3.2 检验端口安全
- 6.3.3 配置BPDU保护、BPDU过滤器和根保护
- 6.3.4 配置风暴控制
- 6.3.5 配置VLAN中继(Trunk)安全
- 6.3.6 配置Cisco 交换端口分析器
- 6.3.7 配置PVLAN边缘
- 6.3.8 对于第二层建议的实践
- 6.4 无线、VoIP和SAN安全
- 6.4.1 企业高级技术安全考虑
- 6.4.2 无线安全考虑
- 6.4.3 无线安全解决方案
- 6.4.4 VoIP安全考虑
- 6.4.5 VoIP安全解决方案
- 6.4.6 SAN安全考虑
- 6.4.7 SAN安全解决方案
- 第7章 密码系统
- 7.1 密码服务
- 7.1.1 保护通信安全
- 7.1.2 密码术
- 7.1.3 密码分析

7.1.4 密码学

7.2 基本完整性和真实性

7.2.1 密码散列

7.2.2 MD5和SHA-1的完整性

7.2.3 HMAC的真实性

7.2.4 密钥管理

7.3 机密性

7.3.1 加密

7.3.2 数据加密标准

7.3.3 3DES

7.3.4 高级加密标准

7.3.5 替代加密算法

7.3.6 Diffie-Hellman密钥交换

7.4 公钥密码术

7.4.1 对称加密与非对称加密

7.4.2 数字特征

7.4.3 Rivest、Shamir和Alderman

7.4.4 公共密钥基础架构

7.4.5 PKI标准

7.4.6 认证授权

7.4.7 数字证书和CA

第8章 实现虚拟专用网络

8.1 VPN

8.1.1 VPN概述

8.1.2 VPN拓扑

8.1.3 VPN解决方案

8.2 GRE VPN

8.3 IPSec VPN组件和操作

8.3.1 IPSec介绍

8.3.2 IPSec安全协议

8.3.3 Internet密钥交换

8.4 使用CLI实现站点到站点的IPSec VPN

8.4.1 配置一个站点到站点的IPSec VPN

8.4.2 任务1——配置兼容ACL

8.4.3 任务2——配置IKE

8.4.4 任务3——配置变换集

8.4.5 任务4——配置加密ACL

8.4.6 任务5——应用加密映射

8.4.7 验证IPSec配置和故障排除

8.5 使用CCP实现站点到站点的IPSec VPN

8.5.1 使用CCP配置IPSec

8.5.2 VPN向导——快速安装

8.5.3 VPN向导——逐步安装

8.5.4 验证、监控VPN和VPN故障排除

8.6 实现远程访问VPN

8.6.1 向远程办公的转变

8.6.2 远程访问VPN介绍

8.6.3 SSL VPN

8.6.4 Cisco Easy VPN

8.6.5 使用CCP配置一台VPN服务器

8.6.6 连接VPN客户端

第9章 管理一个安全的网络

9.1 安全网络设计的原则

9.1.1 确保网络是安全的

9.1.2 威胁识别和风险分析

9.1.3 风险管理和风险避免

9.2 安全架构

9.2.1 Cisco SecureX架构简介

9.2.2 Cisco SecureX架构的解决方案

9.2.3 网络安全的未来趋势

9.3 运行安全

9.3.1 运行安全介绍

9.3.2 运行安全的原则

9.4 网络安全测试

9.4.1 网络安全测试介绍

9.4.2 网络安全测试工具

9.5 业务连续性规划和灾难恢复

9.5.1 连续性规划和灾难恢复

9.5.2 中断和备份

9.5.3 安全复制

9.6 系统开发生命周期

9.6.1 SDLC介绍

9.6.2 SDLC的各阶段

9.7 开发一个全面的安全策略

9.7.1 安全策略概述

9.7.2 安全策略的结构

9.7.3 标准、指南、规程

9.7.4 角色和职责

9.7.5 安全意识和培训

9.7.6 法律与道德

9.7.7 对安全违规的响应

第10章 实施Cisco自适应安全设备(ASA)

10.1 介绍ASA

10.1.1 ASA概述

10.1.2 基本ASA配置

10.2 ASA防火墙配置

10.2.1 ASA防火墙配置介绍

10.2.2 配置管理设置和服务

10.2.3 介绍ASDM

10.2.4 ASDM向导

10.2.5 对象组

10.2.6 ACL

10.2.7 ASA上的NAT服务

10.2.8 ASA上的访问控制

10.2.9 ASA上的服务策略

10.3 ASA VPN配置

10.3.1 ASA远程访问(Remote-Access)VPN选项

10.3.2 无客户端SSL VPN

10.3.3 配置无客户端SSL VPN

10.3.4 AnyConnect SSL VPN

10.3.5 配置AnyConnect SSL VPN

术语表

章节摘录

版权页： 密码散列函数被设计用来验证和确保数据完整性。

它也可以被用来验证身份。

这一过程取用数据的一个可变块，返回一个被称为散列值或消息摘要的固定长度的比特串。

散列类似于计算循环冗余校验码（cyclic redundancy check，CRC）的校验和，但它的加密强度要大很多。

例如，给定一个CRC值，使用相同的CRC生成数据很容易。

使用散列函数，要让两组不同的数据得到相同的散列输出在计算上是不可行的。

每次数据变化或更改，散列值也会变化。

由于这一原因，密码散列值经常被称为数字指纹，它们可被用来探测复制的数据文件、文件版本变化以及类似的应用程序。

这些值被用于防范对数据的无意或有意变更以及偶然的数据损坏。

密码散列函数被应用于很多不同的情况。

当与对称安全认证密钥（例如IPSec或路由协议认证）一起使用时提供真实性（authenticity）证据。

通过在如PPP挑战握手认证协议（Challenge Handshake Authentication Protocol，CHAP）这类认证协议中对挑战生成一次性的单向响应来提供认证（authentication）。

提供消息完整性检查证据（例如那些在数字特征合同中使用的）和公共密钥基础架构（PublicKey Infrastructure，PKI）证书（例如使用浏览器访问安全站点时被接受的证书）。

在数学上，一个散列函数是这样一个过程，它获得一个输入，返回一个被称为散列值的定长串。

计算公式是 $h=H(x)$ 。

一个密码散列函数应具备以下特征。

输入可以是任意长度。

输出的长度固定。

对于任意给定的 X ， $H(x)$ 相对易于计算。

$H(x)$ 是单向的，不可逆。

$H(x)$ 不会发生冲突，这意味着两个不同的输入值将得到不同的散列结果。

如果一个散列函数很难反转，它被认为是一个单向散列。

难以反转意味着给定一个散列值 h ，要找到一个输入使得 $H(x)=h$ 在计算上是不可行的。

当要保护数据不被意外改变时散列函数很有用，但它们不能保证数据未被精心改动。

例如，发送方想要确保消息在被送往接收方的路途中不被改变。

发送设备将消息输入到一个散列算法计算出它的定长摘要或指纹。

消息和散列都是明文。

指纹随后被附在消息上发给接收方。

接收设备从消息上移除，指纹，把消息输入相同的散列算法。

如果接收设备计算出的散列与被附在消息上的散列相等，则消息在传输过程中未被篡改。

编辑推荐

思科网络技术学院教程 CCNA安全最新升级版本，完成本课程的学习，你将能够掌握以下技能：描述现代网络基础架构中的安全威胁。

了解cisco安全路由器，在cisco路由器上使用本地路由器和网络的安全威胁。

实现安全的网络管理和报告，缓解常见的二层攻击，实现cisco ios 防火墙特性集，实现cisco ios ips特性集，实现站点到站点的IPSec VPN

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>