

<<网络安全原理与实践>>

图书基本信息

书名：<<网络安全原理与实践>>

13位ISBN编号：9787115182739

10位ISBN编号：7115182736

出版时间：2008-8

出版单位：人民邮电出版社

作者：马里克

页数：607

字数：989000

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>

<<网络安全原理与实践>>

内容概要

本书为广大读者提供了安全网络设施和VPN的专家级解决方案。

全书共分9个部分，分别介绍了网络安全介绍、定义安全区、设备安全、安全路由、安全LAN交换、网络地址转换与安全、防火墙基础、PIX防火墙、IOS防火墙、VPN的概念、GRE、L2TP、IPSec、入侵检测、Cisco安全入侵检测、AAA、TACACS+、RADIUS、使用AAA实现安全特性的特殊实例、服务提供商安全的利益和挑战、高效使用访问控制列表、使用NBAR识别和控制攻击、使用CAR控制攻击、网络安全实施疑难解析等。

附录中包括各章复习题答案和企业网络安全蓝图白皮书。

本书适合准备参加CCIE网络安全认证工作的人员，也适合那些想增强关于网络安全核心概念知识的网络安全专业人员。

<<网络安全原理与实践>>

书籍目录

第一部分 网络安全介绍	第1章 网络安全介绍	1.1 网络安全目标	1.2 资产确定
1.3 威胁评估	1.4 风险评估	1.5 构建网络安全策略	1.6 网络安全策略的要素
1.7 实现网络安全策略	1.8 网络安全体系结构的实现	1.9 审计和改进	1.10 实例研究
1.10.1 资产确定	1.10.2 威胁确定	1.10.3 风险分析	
1.10.4 定义安全策略	1.11 小结	1.12 复习题	第二部分 构建网络安全
定义安全区	2.1 安全区介绍	2.2 设计一个DMZ	第2章 定义安全区
2.1 安全区介绍	2.2 设计一个DMZ	2.2.1 使用一个三脚防火墙创建DMZ	2.2.2 DMZ置于防火墙之外, 公共网络和防火墙之间
2.2.2 DMZ置于防火墙之外, 公共网络和防火墙之间	2.2.3 DMZ置于防火墙之外, 但不在公共网络和防火墙之间的通道上	2.2.4 在层叠的防火墙之间创建DMZ	
2.3 实例研究: 使用PIX防火墙创建区	2.4 小结	2.5 复习题	第3章 设备安全
3.1 物理安全	3.1.1 冗余位置	3.1.2 网络拓扑设计	3.1.3 网络的安全位置
3.1.4 选择安全介质	3.1.5 电力供应	3.1.6 环境因素	3.2 设备冗余
3.2.1 路由冗余	3.2.2 HSRP	3.2.3 虚拟路由器冗余协议 (VRRP)	
3.3 路由器安全	3.3.1 配置管理	3.3.2 控制对路由器的访问	3.3.3 对路由器的安全访问
3.3.4 密码管理	3.3.5 记录路由器事件	3.3.6 禁用不需要的服务	3.3.7 使用回环接口
3.3.8 控制SNMP作为一个管理协议	3.3.9 控制HTTP作为一个管理协议	3.3.10 将CEF作为一种交换机制使用	3.3.11 从安全的角度来建立调度表
3.3.12 使用NTP	3.3.13 登录标志	3.3.14 捕获存储器信息转存	3.3.15 在CPU高负载期间使用nagle服务以提高Telnet访问
3.4.1 配置管理	3.4.2 控制对PIX的访问	3.4.3 安全访问PIX	3.4.4 密码管理
3.4.5 记录PIX事件	3.5 交换机安全	3.5.1 配置管理	3.5.2 控制对交换机的访问
3.5.3 对交换机的安全访问	3.5.4 记录交换机事件	3.5.5 控制管理协议 (基于SNMP的管理)
第4章 安全路由	第5章 安全LAN交换	第6章 网络地址转换与安全	第三部分 防火墙
第7章 什么是防火墙	第8章 PIX防火墙	第9章 IOS防火墙	第四部分 VPN
第10章 VPN的概念	第11章 GRE	第12章 L2TP	第13章 IPsec
第五部分 入侵检测	第14章 什么是入侵检测	第15章 Cisco安全入侵检测	第六部分 网络访问控制
第16章 AAA	第17章 TACACS+	第18章 RADIUS	第19章 使用AAA实现安全特性的特殊实例
第七部分 服务提供商安全	第20章 服务提供商安全的利益和挑战	第21章 有效使用访问控制列表	第22章 使用NBAR识别和控制攻击
第23章 使用CAR控制攻击	第八部分 疑难解析	第24章 网络安全实施疑难解析	第九部分 附录

章节摘录

第一部分 网络安全介绍 第1章 网络安全介绍 1.6 网络安全策略的要素 为了透彻了解什么是网络安全策略，需要对网络安全策略最重要的元素进行分析以帮助理解。

RFC 2196列出以下内容作为一个安全策略的要素： 1.计算机技术购买准则，指明了需要的或者涉及到的安全特性。

这些应该是对现有的购买策略和准则的补充。

2.保密策略，定义例如监控电子邮件、记录键盘输入和访问用户文件等与保密相关的合理的期望值。

3.访问策略，用于定义访问权力和特权，指定用户、工作团体和管理者可接受的使用准则，以便从失败或者泄密中保护资产。

它应该提供指导原则，用以指导外部连接、数据通信、向网络中连接设备和向系统中添加新的软件。它还应该指明任何需要通知的信息（例如，连接信息应提供关于授权使用的警告信息和在线监控信息，而不是只简单地说“欢迎”）。

4.职责策略，用于定义用户、工作团体和管理者的职责。

它应该规定审计能力并且提供事故处理准则（也就是说，如果检测到一个可能的入侵的话，应该做什么以及和联系谁）。

5.认证策略，通过一个有效的密码策略，为远程认证和认证设备使用设置准则（例如一次性密码和产生一次性密码的设备），从而建立信任机制。

6.可用性声明，用以设置用户对资源可用性的期望值。

它应该有地址冗余和恢复问题，也指明操作时间和维护停机时间。

它还应包括报告系统和网络故障的联系信息。

7.信息技术系统 & 网络维护策略，描述如何允许内部和外部维护人员处理和访问网络中用到的技术。

这里提出的一个重要议题，是否允许远程维护以及怎样控制这样的访问。

需要考虑的另一个领域是外部采办以及怎样管理它。

8.侵犯报告策略，用以指明哪种类型的侵犯（例如，保密和安全，内部的和外部的）是必须汇报的，以及报告生成后向谁汇报。

在一个非危急的环境中，如果侦测到入侵并且需要报告的话，那么使用匿名报告的可能性较大。

9.支持信息，它是为每种类型的策略侵犯而提供给用户、团队和管理者的联系信息；如何处理关于一个安全事故的外部询问，或者哪个应被考虑成保密或是专有的指导方针；以及安全程序的交叉引用和相关信息，比如公司策略和政府的法律和法规。

<<网络安全原理与实践>>

编辑推荐

通过定义区、实施安全路由协议设计、构建安全的LAN交换环境实现网络安全。
理解Cisco PIX防火墙的内部工作原理，深入剖析Cisco PIX防火墙和Cisco IOS防火墙的特性和概念。

理解什么是VPN以及如何与诸如GRE、L2TP和IPSec等协议一起实施VPN。
获取对IPSec协议套、相关的封装和哈希函数、认证技术分组级的理解。
学习如何对网络攻击进行分类，以及如何设计和配置CiscoIDS以抵御网络攻击。
通过学习AAA如何嵌入Cisco安全模块和实施RADIUS及TACACS+协议控制对网络的访问。
使用ACL、NBAR和CAR来标识和控制攻击，为服务提供商提供安全保障。
通过评价一些实际的疑难解析场景来识别和解决常见的失败实施。
随着各种组织的核心商业活动对网络的依赖性逐渐增强。
以及通过虚拟专用网（VPN）对远程站点和移动办公员工访问的增加。
网络安全变得越来越重要。
在今天的网络时代，信息是一个组织最为重要的资源。
如果客户、合作伙伴以及员工不能有效地访问电子商务和数据服务器。
将影响收益和生产能力。
即使如此。
很多网络也没有适当的安全措施。
本书提供了对相关策略、产品和企业的深入介绍。
它们能够把这个非常复杂的话题很好地组织起来。
并使你对网络系统和服务的性能及完整性更有信心。
本书作者是CCIE T工程师，他参与编写了CCIE安全考试的试题。
本书是第一本备考CCIE安全考试的参考书。

<<网络安全原理与实践>>

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>