

《网络安全体系结构》

图书基本信息

书名：《网络安全体系结构》

13位ISBN编号：9787115298188

10位ISBN编号：7115298181

出版时间：2013-1

出版社：人民邮电出版社

作者：Sean Convery

页数：670

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《网络安全体系结构》

内容概要

《网络安全体系结构》共分为4个部分和3个附录。第一部分介绍了设计安全网络的一些基础概念，提供了设计安全网络的先决条件以及进行安全网络设计所需的基本元素，为后续章节打下基础。第二部分全面讨论了可供安全设计人员使用的各类技术，以及使用不同技术来设计网络安全解决方案时需要予以考虑的因素。第三部分针对不同的网络环境，介绍了它们各自的设计方式。第四部分介绍了如何保障网络管理的安全性，同时对一些设计案例进行了研究，最后对全书做了总结。附录A对书中使用过的一些术语进行了介绍。附录B提供了各章测试题的参考答案。附录C则提供了安全网络设计中，一些设计文档的起草范例。

《网络安全体系结构》

作者简介

Sean Convery, CCIE

#4232, 是Cisco公司的一名安全架构师。他在Cisco工作了6年, 其中最为引人瞩目的工作是担任了最初的Cisco

SAFE安全蓝图的首席架构师, 并且还是其中数个白皮书的作者。在Cisco工作期间, Sean曾为全球数以千计的Cisco客户进行了网络安全设计, 并为很多不同网络规模的客户提供了安全设计方面的咨询。

书籍目录

第一部分 网络安全基础

第1章 网络安全公理

- 1.1 网络安全是一个系统
- 1.2 必须首先考虑业务的优先级
- 1.3 网络安全催生良好的网络设计
- 1.4 一切皆为目标
- 1.5 一切皆为武器
- 1.6 设法简化操作
- 1.7 良好的网络安全策略是具有预见性的
- 1.8 不要通过隐匿来提高系统的安全性
- 1.9 机密性不等同于安全
- 1.10 总结
- 1.11 参考资料
- 1.12 应用知识问题

第2章 安全策略与运行生命周期

- 2.1 网络安全千金难买
- 2.2 什么是安全策略
 - 2.2.1 实施安全策略需要考虑的事项
- 2.3 安全系统的开发与运行概述
 - 2.3.1 安全系统的开发
 - 2.3.2 安全系统运作的生命周期
- 2.4 总结
- 2.5 参考资料
- 2.6 应用知识问题

第3章 安全联网的威胁

- 3.1 攻击过程
- 3.2 攻击者的类型
 - 3.2.1 脚本小子
 - 3.2.2 解密者
 - 3.2.3 精英
- 3.3 弱点类型
 - 3.3.1 软件弱点
 - 3.3.2 硬件弱点
 - 3.3.3 配置弱点
 - 3.3.4 策略弱点
 - 3.3.5 使用弱点
- 3.4 攻击结果
 - 3.4.1 信息泄密
 - 3.4.2 信息损坏
 - 3.4.3 拒绝服务
 - 3.4.4 服务被盗
 - 3.4.5 访问权增大
- 3.5 攻击分类
 - 3.5.1 读取攻击
 - 3.5.2 操纵攻击
 - 3.5.3 欺骗攻击
 - 3.5.4 泛洪

- 3.5.5 重定向
- 3.5.6 混合型攻击
- 3.6 总结
- 3.7 参考资料
- 3.8 应用知识问题
- 第4章 网络安全技术
 - 4.1 实现网络安全的难点
 - 4.2 安全技术
 - 4.2.1 身份识别技术
 - 4.2.2 主机和应用安全
 - 4.2.3 网络防火墙
 - 4.2.4 内容过滤
 - 4.2.5 网络入侵检测系统
 - 4.2.6 加密技术
 - 4.3 新兴安全技术
 - 4.3.1 混合主机解决方案
 - 4.3.2 在线 (inline) NIDS
 - 4.3.3 应用防火墙
 - 4.4 总结
 - 4.5 参考资料
 - 4.6 应用知识问题
- 第二部分 设计安全网络
- 第5章 设备安全强化
 - 5.1 安全强化战略的组成
 - 5.1.1 安全策略
 - 5.1.2 设备位置
 - 5.1.3 威胁配置文件
 - 5.1.4 功能需求
 - 5.1.5 管理需求
 - 5.2 网络设备
 - 5.2.1 路由器
 - 5.2.2 交换机
 - 5.2.3 防火墙
 - 5.2.4 NIDS
 - 5.3 主机操作系统
 - 5.3.1 分区磁盘空间
 - 5.3.2 关闭不需要的服务
 - 5.3.3 为需要的服务打补丁
 - 5.3.4 记录关键事件
 - 5.4 应用程序
 - 5.5 基于设备的网络服务
 - 5.6 无赖设备检测
 - 5.7 总结
 - 5.8 参考资料
 - 5.9 应用知识问题
- 第6章 常规设计考虑
 - 6.1 物理安全问题
 - 6.1.1 控制对设施的物理访问
 - 6.1.2 控制对数据中心的物理访问

- 6.1.3 用于非安全位置的隔离身份识别机制
 - 6.1.4 防止非安全位置的密码恢复机制
 - 6.1.5 清楚线缆线路问题
 - 6.1.6 清楚电磁辐射问题
 - 6.1.7 清楚物理PC安全威胁
 - 6.2 第2层安全考虑
 - 6.2.1 L2控制协议
 - 6.2.2 MAC泛洪考虑
 - 6.2.3 VLAN跳转考虑
 - 6.2.4 ARP考虑
 - 6.2.5 DHCP考虑
 - 6.2.6 私有VLAN
 - 6.2.7 L2最佳做法推荐
 - 6.3 IP寻址设计考虑
 - 6.3.1 通用最佳做法和路由汇总
 - 6.3.2 入站/出站过滤
 - 6.3.3 NAT
 - 6.4 ICMP设计考虑
 - 6.4.1 ICMP消息类型过滤
 - 6.5 路由选择考虑
 - 6.5.1 路由选择协议安全
 - 6.5.2 非对称路由与可感知状态的安全技术
 - 6.6 传输协议设计考虑
 - 6.7 DoS设计考虑
 - 6.7.1 网络泛洪设计考虑
 - 6.7.2 TCP SYN泛洪设计考虑
 - 6.7.3 ICMP不可达DoS考虑
 - 6.8 总结
 - 6.9 参考资料
 - 6.9 应用知识问题
- 第7章 网络安全平台选项和最佳做法
- 7.1 网络安全平台的选择
 - 7.1.1 通用操作系统安全设备
 - 7.1.2 专业安全设备
 - 7.1.3 将安全技术集成到网络中
 - 7.1.4 网络安全平台选择的建议
 - 7.2 网络安全设备的最佳做法
 - 7.2.1 防火墙
 - 7.2.2 代理服务器/内容过滤
 - 7.2.3 NIDS
 - 7.3 总结
 - 7.4 参考资料
 - 7.5 应用知识问题
- 第8章 常用应用设计考虑
- 8.1 电子邮件
 - 8.1.1 基本的两层(Two-Tier)电子邮件设计
 - 8.1.2 分布式两层电子邮件设计
 - 8.1.3 访问控制实例
 - 8.1.4 邮件应用设计推荐

8.2 DNS

- 8.2.1 不要将你的DNS服务器放在同一处
- 8.2.2 拥有多台权威DNS服务器
- 8.2.3 让你的外部DNS服务器仅响应非递归查询请求
- 8.2.4 提供受保护的内部DNS服务器
- 8.2.5 分隔外部和内部DNS服务器提供的信息
- 8.2.6 限制权威服务器的区域传输
- 8.2.7 DNS过滤案例学习

8.3 HTTP/HTTPS

- 8.3.1 简单Web设计
- 8.3.2 两层Web设计
- 8.3.3 三层Web设计

8.4 FTP

- 8.4.1 主动模式
- 8.4.2 被动模式

8.5 即时消息

8.6 应用评估

8.7 总结

8.8 参考资料

8.9 应用知识问题

第9章 身份识别设计考虑

9.1 基本身份识别概念

- 9.1.1 设备身份识别与用户身份识别
- 9.1.2 网络身份识别与应用身份识别
- 9.1.3 你信任谁
- 9.1.4 身份识别与认证、授权与审计
- 9.1.5 共享的身份识别
- 9.1.6 加密身份识别考虑

9.2 身份识别类型

- 9.2.1 物理访问
- 9.2.2 MAC地址
- 9.2.3 IP地址
- 9.2.4 第4层信息
- 9.2.5 用户名
- 9.2.6 数字证书
- 9.2.7 生物特征识别

9.3 身份识别要素

9.4 身份识别在网络安全中的角色

9.5 身份识别技术指导方针

- 9.5.1 AAA服务器设计指导方针
- 9.5.2 802.1x/EAP身份识别设计指导方针
- 9.5.3 基于网关的网络认证
- 9.5.4 PKI使用基础

9.6 身份识别部署推荐

- 9.6.1 设备到网络
- 9.6.2 用户到网络
- 9.6.3 用户到应用

9.7 总结

9.8 参考资料

9.9 应用知识问题

第10章 IPSec VPN设计考虑

10.1 VPN基础

10.2 IPSec VPN类型

10.2.1 站点到站点VPN

10.2.2 远程用户VPN

10.3 IPSec运行模式与安全选项

10.3.1 IPSec的三个要素

10.3.2 传输模式和隧道模式

10.3.3 IPSec SA建立

10.3.4 其他安全选项

10.4 拓扑考虑

10.4.1 分割隧道

10.4.2 拓扑选择

10.5 设计考虑

10.5.1 平台选项

10.5.2 身份识别和IPSec访问控制

10.5.3 第3层IPSec考虑

10.5.4 分片和路径最大传输单元

10.5.5 VPN的防火墙和NIDS放置

10.5.6 高可用性

10.5.7 QoS

10.5.8 IPSec厂商互操作性

10.6 站点到站点部署实例

10.6.1 基本IPSec

10.6.2 GRE + IPSec

10.6.3 动态多点VPN

10.7 IPSec外包

10.7.1 基于网络管理的IPSec

10.7.2 CPE管理的IPSec

10.8 总结

10.9 参考资料

10.10 应用知识问题

第11章 支持技术设计考虑

11.1 内容

11.1.1 缓存

11.1.2 内容传播与路由选择

11.2 负载均衡

11.2.1 安全考虑

11.2.2 服务器负载均衡

11.2.3 安全设备负载均衡

11.3 无线局域网

11.3.1 一般考虑

11.3.2 技术选项

11.3.3 独特的部署选项

11.3.4 WLAN结论

11.4 IP电话通讯

11.4.1 安全考虑

11.4.2 部署选项

11.4.3 IP电话推荐

11.5 总结

11.6 参考资料

11.7 应用知识问题

第12章 设计安全系统

12.1 网络设计进阶

12.1.1 核心层、分布层、接入层/边界

12.1.2 管理

12.2 安全系统概念

12.2.1 信任域

12.2.2 安全控制点

12.2.3 安全角色：接入/边界、分布、核心

12.3 网络安全对整个设计的影响

12.3.1 路由选择与IP寻址

12.3.2 易管理性

12.3.3 扩展性和性能

12.4 设计安全系统的10个步骤

12.4.1 第1步：回顾已完成的安全策略文档

12.4.2 第2步：对照安全策略分析当前网络

12.4.3 第3步：选择技术并评估产品能力

12.4.4 第4步：设计一个安全系统的理想草案

12.4.5 第5步：在实验中测试关键组件

12.4.6 第6步：评估并修正设计/策略

12.4.7 第7步：设计定案

12.4.8 第8步：在一个关键区域实现安全系统

12.4.9 第9步：推广到其他区域

12.4.10 第10步：验证设计/策略

12.4.11 两步骤评估清单

12.5 总结

12.6 应用知识问题

第三部分 安全网络设计

第13章 边界安全设计

13.1 什么是边界

13.2 预计威胁

13.3 威胁缓解

13.4 身份识别考虑

13.5 网络设计考虑

13.5.1 ISP路由器

13.5.2 公共服务器数量

13.5.3 分支与总部设计考虑

13.5.4 远程访问替代

13.6 小型网络边界安全设计

13.6.1 设计需求

13.6.2 设计概述

13.6.3 边界设备和安全角色

13.6.4 VPN

13.6.5 设计评估

13.6.6 设计替代选项

13.7 中型网络边界安全设计

- 13.7.1 设计需求
- 13.7.2 设计概述
- 13.7.3 Internet边界
- 13.7.4 远程访问边界
- 13.7.5 设计评估
- 13.7.6 设计替代选项
- 13.8 高端弹性边界安全设计
 - 13.8.1 设计需求
 - 13.8.2 设计概述
 - 13.8.3 Internet边界
 - 13.8.4 远程访问边界
 - 13.8.5 设计评估
 - 13.8.6 设计替代
- 13.9 电子商务和外部网设计防护措施
 - 13.9.1 电子商务
 - 13.9.2 外部网
- 13.10 总结
- 13.11 参考资料
- 13.12 应用知识问题

第14章 园区网络安全设计

- 14.1 什么是园区
- 14.2 园区信任模型
- 14.3 预计威胁
- 14.4 威胁缓解
- 14.5 身份识别考虑
- 14.6 网络设计考虑
 - 14.6.1 第2层考虑
 - 14.6.2 状态化与无状态ACL对比和L3与L4过滤对比
 - 14.6.3 入侵检测系统
 - 14.6.4 WLAN考虑
 - 14.6.5 网络管理
 - 14.6.6 无赖设备
- 14.7 小型网络园区安全设计
 - 14.7.1 设计需求
 - 14.7.2 设计概述
 - 14.7.3 园区设备和安全角色
 - 14.7.4 设计评估
 - 14.7.5 设计替代选项
 - 14.7.6 增加安全性的替代选项
 - 14.7.7 降低安全性的替代选项
- 14.8 中型网络园区安全设计
 - 14.8.1 设计需求
 - 14.8.2 设计概述
 - 14.8.3 园区设备和安全角色
 - 14.8.4 设计评估
 - 14.8.5 设计替代
 - 14.8.6 增加安全性的替代选项
 - 14.8.7 降低安全性的替代选项
- 14.9 高端弹性园区安全设计

- 14.9.1 设计需求
- 14.9.2 设计概述
- 14.9.3 园区设备与安全角色
- 14.9.4 设计评估
- 14.9.5 设计替代选项
- 14.10 总结
- 14.11 参考资料
- 14.12 应用知识问题
- 第15章 远程工作者安全设计
 - 15.1 定义远程工作者环境
 - 15.2 预计威胁
 - 15.3 威胁缓解
 - 15.4 身份考虑
 - 15.5 网络设计考虑
 - 15.5.1 主机保护
 - 15.5.2 网络传输保护
 - 15.6 基于软件的远程工作者设计
 - 15.6.1 设计需求
 - 15.6.2 设计概述
 - 15.7 基于硬件的远程工作者设计
 - 15.7.1 设计要求
 - 15.7.2 设计概述
 - 15.7.3 物理安全考虑
 - 15.8 设计评估
 - 15.9 总结
 - 15.10 参考资料
 - 15.11 应用知识问题
- 第四部分 网络管理、案例分析和结束语
- 第16章 安全网络管理和网络安全管理
 - 16.1 乌托邦管理目标
 - 16.2 组织现实
 - 16.3 协议能力
 - 16.3.1 Telnet/安全Shell
 - 16.3.2 HTTP/HTTPS
 - 16.3.3 简单网络管理协议
 - 16.3.4 TFTP/FTP/SFTP/SCP
 - 16.3.5 syslog
 - 16.3.6 NetFlow
 - 16.3.7 其他
 - 16.4 工具功能
 - 16.4.1 网络安全管理工具
 - 16.4.2 安全网络管理工具
 - 16.5 安全管理设计选项
 - 16.5.1 带内明文
 - 16.5.2 带内加密保护（会话和应用层）
 - 16.5.3 带内加密保护（网络层）
 - 16.5.4 混合管理设计
 - 16.5.5 安全网络管理可选组成部分
 - 16.6 网络安全管理最佳做法

- 16.6.1 24 × 7 × 365监控关键安全事件
- 16.6.2 从关键通知中分离历史事件数据
- 16.6.3 选择敏感日志级别
- 16.6.4 分离网络管理和网络安全管理
- 16.6.5 关注操作需求
- 16.6.6 考虑外包
- 16.7 总结
- 16.8 参考资料
- 16.9 应用知识问题

第17章 案例研究

- 17.1 引言
- 17.2 现实世界适应性
- 17.3 组织
 - 17.3.1 组织概况
 - 17.3.2 当前设计
 - 17.3.3 安全需求
 - 17.3.4 设计选择
 - 17.3.5 迁移战略
 - 17.3.6 攻击案例
- 17.4 NetGamesRUs.com
 - 17.4.1 组织概况
 - 17.4.2 当前设计
 - 17.4.3 安全需求
 - 17.4.4 设计选择
 - 17.4.5 迁移战略
 - 17.4.6 攻击案例
- 17.5 不安全大学
 - 17.5.1 组织概况
 - 17.5.2 当前设计
 - 17.5.3 安全需求
 - 17.5.4 设计选择
 - 17.5.5 迁移战略
 - 17.5.6 攻击案例
- 17.6 黑色直升机研究有限公司
 - 17.6.1 组织概况
 - 17.6.2 当前设计
 - 17.6.3 安全需求
 - 17.6.4 设计选择
 - 17.6.5 迁移战略
 - 17.6.6 攻击案例
- 17.7 总结
- 17.8 参考资料
- 17.9 应用知识问题

第18章 结束语

- 18.1 引言
- 18.2 管理问题仍在继续发生
- 18.3 安全计算开销将降低
- 18.4 同构和异构网络
- 18.5 应严肃考虑立法

18.6 IPv6改变规则

18.7 网络安全是一个体系

18.8 总结

18.9 参考资料

附录A 术语表

附录B

第1章

第2章

第3章

第4章

第5章

第6章

第7章

第8章

第9章

第10章

第11章

第12章

第13章

第14章

第15章

第16章

附录C 安全策略示例

C.1 INFOSEC可接受使用策略

C.1.1 1.0概述

C.1.2 2.0目的

C.1.3 3.0范围

C.1.4 4.0策略

C.1.5 5.0强制措施

C.1.6 6.0定义

C.1.7 7.0修订历史

C.2 密码策略

C.2.1 1.0概述

C.2.2 2.0目的

C.2.3 4.0范围

C.2.4 5.0强制措施

C.2.5 6.0定义

C.2.6 7.0修订历史

C.3 防病毒过程指导方针

章节摘录

版权页：插图：实施认证、授权和审计（AAA）旨在对身份进行验证。AAA是网络安全中的一个重要概念。其中，认证指的是你是谁，授权指的是允许你干什么，审计指的是对你所做事情进行记录。将它们缩写为AAA仿佛是在暗示它们的关系是密不可分的，更何况它们也可以仅通过一台专门的AAA服务器进行提供。但实际上，情况正好相反。在当今现代的网络中，AAA可能由许多位于不同地方的系统执行。我们仅以下列一系列事件为例进行解释。用户启动笔记本电脑——第一次需要认证是在输入基本输入/输出系统（BIOS）的启动密码时，由于在BIOS启动级别上无法区分访问计算机的用户，所以不必独立进行授权。如果你提供了BIOS密码，系统就会启动。在OS启动后，现代OS会再次提示用户输入认证信息。这里也会执行授权操作。一个只有访客登录权限的用户在系统中的权限要远远少于具有root密码的用户权限。这些访问权限可以在操作系统内部调整。此外，这里还会执行审计：现代OS会在特定用户访问系统时进行日志记录，同时当用户在系统上执行重要操作时也常常会将这些行为另行记录下来。用户建立到公司办公室的VPN连接——在这里，VPN网关会再次对用户进行认证。根据用户所属的成员组，VPN网关能够授权用户执行一些网络行为，同时阻止用户执行其他网络行为。在一些情形下，这仍然是由防火墙处的另一台设备完成的。在这里会再次执行审计。用户下载电子邮件——这是当用户登录时用户AAA的另一关键步骤，AAA会根据用户ID来授予用户访问特定文件的权限，并让邮件服务器将这次访问记录下来。当发送邮件时，在邮件服务器接受邮件消息之前，用户的IP地址最有可能被用来进行用户身份的识别。用户将一个项目文件移动到基于网络存储的设备——此处同样存在AAA，这次是在文件服务器上。用户浏览Internet - 假定没有代理服务器，那么AAA只会发生在IP层，即访问控制列表（ACL）控制用户访问Internet的行为，同时防火墙对行为进行记录。

《网络安全体系结构》

编辑推荐

一本网络安全的设计指南帮助读者设计出符合可满足不同安全需求的网络环境

《网络安全体系结构》

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:www.tushu000.com