

<<Cisco路由器防火墙安全>>

图书基本信息

书名：<<Cisco路由器防火墙安全>>

13位ISBN编号：9787115136954

10位ISBN编号：7115136955

出版时间：2006-1

出版时间：人民邮电出版社

作者：迪尔

页数：668

字数：1056000

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路由器防火墙安全>>

内容概要

本书全面系统地介绍基于Cisco IOS软件操作系统的各种防火墙特性。使用这些特性可以加固Cisco边界路由器和其他路由器，在保护已有投资的情况下，保护我们的网络免受各种安全威胁和攻击。

本书共有21章，分成9个部分。

第一部分是安全问题和防火墙的概述。

第二部分通过基本的访问设置、关闭不必要的服务和实施AAA来保护到路由器本身的访问安全。

第三部分介绍Cisco的无状态流量过滤技术，包括基本的、扩展的、命名的、定时的、有序的和编译的ACL。

第四部分介绍Cisco的有状态的流量过滤技术，包括反射ACL、CBAC、URL过滤和NBAR等特征。

第五部分介绍地址转换和地址转换所引起的问题以及相应的解决方法。

第六部分分别介绍锁和密钥ACL、认证代理和对路由选择协议的保护，锁和密钥以及认证代理用来实现在允许用户访问资源之前首先对他们进行认证的功能。

第七部分主要介绍入侵检测系统、DoS防护和记录日志事件。

第八部分介绍站到站的IPSec连接和远程接入IPSec连接。

第九部分介绍一个综合的案例学习，结合本书中介绍的重要安全组件，讲述如何保护一个实际环境中的网络安全。

本书是一本关于“如何做”的书，堪称是一部关于Cisco路由器防火墙安全的参考大全。

作者Richard是一位有多年计算机网络业工作经验的专家，本书融入了作者网络安全实践的很多体会和提示，使读者能更好地掌握重要特征和关键问题。

本书中提供的许多例子都很典型，可以方便地应用到我们的网络环境中。

本书文笔流畅、内容翔实、覆盖面很广，是广大网络安全从业人员和网络管理人员的案头必备用书。

本书也可以有效地帮助您通过Cisco的CCSP SECUR认证考试。

<<Cisco路由器防火墙安全>>

作者简介

Richard A.Deal拥有CCSP, CCNP和CCNA证书, 曾经就读于GROVE市立学院, 他主修数学、计算机和英语, 并获得科学学士学位。

在过去的7年里, 他经营自己的公司, 该公司提供咨询和技术培训。

他在计算机和网络业(包括网络、培训、系统管理和编程)有17年的工作经验。

除了

<<Cisco路由器防火墙安全>>

书籍目录

第一部分 安全概述和防火墙第1章 安全威胁	31.1 安全计划	41.1.1 不同的平台	41.1.2 安全目标	51.2 安全问题的起因	51.2.1 策略定义	61.2.2 计算机技术	91.2.3 设备配置	111.3 安全威胁的类型	111.3.1 外部和内部威胁	121.3.2 无组织的和有组织的威胁	121.4 威胁的分类	131.4.1 勘测攻击	131.4.2 访问攻击	161.4.3 拒绝服务攻击	231.5 安全解决方案	251.5.1 设计安全解决方案	251.5.2 Cisco安全轮形图	261.5.3 安全检查列表	271.5.4 附加信息	281.6 小结	28																																													
第2章 防火墙概述	312.1 防火墙简介	312.1.1 防火墙定义	322.1.2 防火墙保护	322.2 流量控制和OSI参考模型	342.2.1 OSI参考模型概要	342.2.2 防火墙和OSI参考模型	352.3 防火墙种类	352.3.1 包过滤防火墙	362.3.2 状态防火墙	402.3.3 应用网关防火墙	482.3.4 地址转换防火墙	542.3.5 基于主机的防火墙	572.3.6 混合防火墙	592.3.7 防火墙和其他服务	602.4 防火墙设计	612.4.1 设计准则	612.4.2 DMZ	642.4.3 组件	682.4.4 组件布局	712.4.5 防火墙实施	742.4.6 防火墙管理	762.5 Cisco IOS安全	762.5.1 Cisco IOS的使用	772.5.2 Cisco IOS的安全特性	772.5.3 Cisco IOS设备及其使用	782.5.4 何时使用Cisco IOS防火墙	792.6 小结	80																																						
第二部分 管理到路由器的访问第3章 访问路由器	853.1 认证类型	853.1.1 没有口令认证	863.1.2 静态口令认证	863.1.3 时效口令认证	873.1.4 一次性口令认证	873.1.5 令牌卡服务	883.2 用户级EXEC访问方法	903.2.1 本地访问：控制台和辅助线路	913.2.2 远程访问	933.3 特权级EXEC访问	1123.3.1 口令	1123.3.2 权限级别	1123.4 其他访问问题	1163.4.1 加密口令	1163.4.2 标识	1173.5 配置实例	1193.6 小结	121	第4章 关闭不必要的服务	1234.1 关闭全局服务	1234.1.1 Cisco发现协议	1244.1.2 TCP和UDP低端口服务	1254.1.3 Finger	1264.1.4 IdentD	1264.1.5 IP源路由	1274.1.6 FTP和TFTP	1284.1.7 HTTP	1284.1.8 SNMP	1294.1.9 域名解析	1304.1.10 BootP	1314.1.11 DHCP	1314.1.12 PAD	1324.1.13 配置自动加载	1324.2 关闭接口服务	1334.2.1 不安全接口上的CDP	1334.2.2 ARP代理	1344.2.3 定向广播	1354.2.4 ICMP消息	1364.2.5 维护操作协议	1394.2.6 VTY	1404.2.7 未使用的接口	1414.3 在边界路由器上手动关闭服务的配置例子	1414.4 AutoSecure	1424.4.1 安全平面	1424.4.2 AutoSecure配置	1444.5 小结	154																			
第5章 认证、授权和记账	1575.1 AAA概述	1575.1.1 AAA工作原理	1585.1.2 打开AAA	1585.1.3 安全协议	1595.2 认证	1665.2.1 认证方法	1675.2.2 认证配置	1685.2.3 认证排错	1715.2.4 认证例子	1715.3 授权	1725.3.1 授权方法	1735.3.2 授权配置	1735.3.3 授权排错	1745.3.4 授权例子	1755.4 记账	1755.4.1 记账方法	1765.4.2 记账配置	1765.4.3 记账排错	1785.4.4 记账例子	1795.5 安全复制	1795.5.1 SCP准备	1805.5.2 SCP配置	1805.5.3 SCP排错	1805.5.4 SCP例子	1815.6 小结	181	第三部分 无状态的过滤技术第6章 访问列表概述	1856.1 访问列表简介	1856.1.1 ACL和过滤	1866.1.2 ACL类型	1876.1.3 处理ACL	1886.2 基本ACL的配置	1946.2.1 建立ACL	1956.2.2 激活ACL	1966.2.3 编辑ACL	1976.3 通配符掩码	1986.3.1 将子网掩码转换成通配符掩码	1996.3.2 通配符掩码错误	2006.4 小结	200	第7章 基本访问列表	2037.1 ACL的类型	2037.1.1 标准ACL	2047.1.2 扩展ACL	2077.1.3 ACL验证	2187.1.4 分片和扩展ACL	2197.1.5 定时ACL	2237.2 其他的ACL特性	2267.2.1 ACL注释	2267.2.2 日志记录更新	2287.2.3 IP统计和ACL	2287.2.4 Turbo ACL	2307.2.5 有序的ACL	2327.3 受攻击时的保护	2357.3.1 Bogon阻塞和欺骗	2357.3.2 DoS和分布式DoS攻击	2407.3.3 简单勘查攻击	2467.3.4 分布式DoS攻击	2487.3.5 特洛伊木马	2547.3.6 蠕虫	2567.4 阻塞不必要的服务	2607.4.1 一场艰难的战斗	2607.4.2 即时消息产品	2617.4.3 文件共享：端到端产品	2657.5 小结	272
第四部分 有状态的和高级的过滤技术第8章 反射访问列表	2778.1 反射ACL概述	2778.1.1 扩展的ACL相比反射ACL	2788.1.2 反射ACL的工作原理	2828.1.3 反射ACL的局限性	2858.2 配置反射ACL	2888.2.1 接口选择	2888.2.2 配置命令	2918.3 反射ACL举例	2958.3.1 简单的RAACL例子	2958.3.2 两个接口的RAACL例子	2958.3.3 三个接口的RAACL例子	2968.4 小结	299	第9章 基于上下文的访问控制	3019.1 Cisco IOS防火墙特性	3019.2 CBAC的功能	3029.2.1 过滤流量	3029.2.2 审查流量	3039.2.3 检测入侵	3039.2.4 生成警告和审计信息	3039.3 CBAC的操作	3039.3.1 基本操作	3039.3.2 CBAC相对RAACL的增强	3059.4 CBAC支持																																										

<<Cisco路由器防火墙安全>>

的协议 3089.4.1 RTSP应用 3099.4.2 H.323应用 3109.4.3 Skinny支持 3109.4.4 SIP支持 3119.5
 CBAC的性能 3129.5.1 吞吐量改进特性 3139.5.2 每秒连接改进特性 3139.5.3 CPU使用率改进
 特性 3139.6 CBAC的局限性 3149.7 CBAC的配置 3149.7.1 步骤1:接口选择 3159.7.2 步骤2
 :ACL配置 3159.7.3 步骤3:全局超时值 3169.7.4 步骤4:端口应用映射 3179.7.5 步骤5:审查
 规则 3209.7.6 步骤6:激活审查 3249.7.7 步骤7:CBAC排错 3249.7.8 删除CBAC 3289.8
 CBAC例子 3289.8.1 简单例子 3289.8.2 两个接口的CBAC例子 3309.8.3 三接口的CBAC例子
 3319.9 小结 334第10章 过滤Web和应用流量 33710.1 Java小程序 33710.1.1 Java审查
 33810.1.2 Java阻塞 33810.1.3 Java阻塞例子 33810.2 URL过滤 34010.2.1 URL过滤操作
 34010.2.2 URL过滤的优点和局限性 34110.2.3 URL过滤实施 34310.2.4 URL过滤验证
 34910.2.5 URL过滤例子 35110.3 基于网络的应用识别 35210.3.1 QoS的组件 35210.3.2
 NBAR和分类 35310.3.3 NBAR的限制和局限性 35710.3.4 基本的NBAR配置 35810.3.5 NBAR
 验证 36410.3.6 NBAR例子 36710.4 小结 372第五部分 地址转换和防火墙第11章 地址转换
 37711.1 地址转换概述 37711.1.1 私有地址 37711.1.2 地址转换 37811.2 地址转换的工作原
 理 37911.2.1 用于地址转换的术语 38011.2.2 执行地址转换 38011.2.3 地址转换的局限性
 38511.3 地址转换配置 38611.3.1 NAT配置 38611.3.2 PAT配置 38911.3.3 端口地址重定向配
 置 39111.3.4 处理重叠的地址 39311.3.5 流量分配配置 39611.3.6 配置转换限制 39811.3.7 地
 址转换的验证和排错 39811.4 NAT和CBAC的例子 40111.5 小结 403第12章 地址转换问题
 40512.1 嵌入的地址信息 40512.1.1 嵌入地址信息问题 40612.1.2 支持的协议和应用 40712.1.3
 非标准的端口号 40812.2 控制地址转换 40912.2.1 使用ACL 40912.2.2 使用路由映射:动态转
 换 41012.2.3 使用路由映射:静态转换 41312.3 地址转换和冗余 41512.3.1 使用HSRP的静
 态NAT冗余 41512.3.2 有状态的地址转换失败切换 41912.4 使用服务器负载均衡来分配流量
 42612.4.1 SLB过程 42612.4.2 SLB的优点和局限性 42912.4.3 SLB的配置 42912.4.4 SLB验证
 43212.4.5 SLB例子 43312.5 小结 434第六部分 管理通过路由器的访问第13章 锁和密钥访问
 列表 43913.1 锁和密钥概述 43913.1.1 锁和密钥与普通ACL 43913.1.2 何时使用锁和密钥
 44013.1.3 锁和密钥的好处 44013.1.4 锁和密钥的处理过程 44113.2 锁和密钥配置 44213.2.1
 配置步骤 44213.2.2 允许远程管理访问 44613.2.3 验证和排错 44713.3 锁和钥匙举例 44813.4
 小结 449第14章 认证代理 45114.1 AP简介 45114.1.1 AP特性 45214.1.2 AP过程 45314.1.3
 AP的使用 45514.1.4 AP的局限性 45614.2 AP的配置 45714.2.1 在路由器上配置AAA
 45714.2.2 在服务器上配置AAA 45814.2.3 为HTTP或HTTPS作准备 46014.2.4 配置AP策略
 46114.2.5 调整AP 46214.2.6 防止访问攻击 46314.3 AP验证和排错 46414.3.1 show命令
 46414.3.2 clear命令 46514.3.3 debug命令 46614.4 AP举例 46614.4.1 简单的AP例子
 46614.4.2 复杂的AP例子:CBAC和NAT 46914.5 小结 472第15章 路由选择协议保护 47515.1
 静态和黑洞路由选择 47515.1.1 静态路由 47615.1.2 Null路由 47615.1.3 基于策略的路由选择
 47815.2 内部网关协议安全 48015.2.1 认证 48115.2.2 RIPv2 48215.2.3 EIGRP 48315.2.4
 OSPF 48415.2.5 IS-IS 48415.2.6 其他工具 48615.2.7 HSRP 48815.3 BGP安全 49015.3.1 认
 证 49015.3.2 路由翻动阻尼 49115.3.3 BGP路由选择例子 49215.4 逆向路径转发(单播流量)
 49615.4.1 RPF过程 49615.4.2 RPF的使用 49815.4.3 RPF局限性 49915.4.4 RPF配置 49915.4.5
 RPF验证 50015.4.6 单播RPF例子 50115.5 小结 501第七部分 检测和防止攻击第16章 入侵检
 测系统 50516.1 IDS简介 50516.1.1 IDS的实现 50616.1.2 IDS解决方案 50716.1.3 IDS要点
 50916.2 IDS签名 51016.2.1 签名实现 51016.2.2 签名结构 51116.2.3 基本分类 51116.2.4
 Cisco签名类型 51116.3 Cisco路由器IDS解决方案 51216.3.1 签名支持 51216.3.2 路由器IDS过
 程 51516.3.3 内存和性能问题 51616.4 IDS配置 51716.4.1 步骤1:初始化配置 51716.4.2 步
 骤2:日志和邮局配置 51716.4.3 步骤3:审查规则配置和激活 51816.4.4 IDS验证 52016.5 IDS举
 例 52116.6 小结 522第17章 DoS防护 52517.1 检测DoS攻击 52517.1.1 常见的攻击 52517.1.2
 检查CPU使用率来检测DoS攻击 52617.1.3 使用ACL检测DoS攻击 52817.1.4 使用NetFlow来检
 测DoS攻击 53317.2 CEF交换 53817.3 TCP截取 53917.3.1 TCP SYN洪水攻击 53917.3.2 TCP
 截取模式 53917.3.3 TCP截取的配置和验证 54017.3.4 TCP截取举例 54417.4 CBAC和DoS攻击

<<Cisco路由器防火墙安全>>

54517.4.1 超时和阈值 54517.4.2 CBAC DoS阻止验证 54717.4.3 CBAC配置举例 54717.5 速率限制 54817.5.1 ICMP速率限制 54917.5.2 CAR 55017.5.3 NBAR 55417.6 小结 557第18章 记录日志事件 55918.1 基本日志记录 55918.1.1 日志消息格式 56018.1.2 基本日志记录配置 56018.1.3 日志记录目的地 56118.1.4 其他日志命令 56618.1.5 日志记录验证 56718.1.6 日志记录和错误计数 56918.2 时间和日期与Cisco IOS 57018.2.1 路由器时间源 57018.2.2 时间和日期的手动配置 57118.2.3 网络时间协议简介 57318.2.4 为NTP配置路由器客户端 57318.2.5 为NTP配置路由器服务器 57518.2.6 NTP安全 57618.2.7 其他NTP命令 57818.2.8 NTP验证 57818.2.9 NTP配置举例 58018.3 内置的系统日志管理器 58018.3.1 ESM简介 58118.3.2 ESM过滤模块 58118.3.3 ESM的建立和配置介绍 58418.4 其他日志记录信息 58618.4.1 要寻找什么 58618.4.2 其他工具 58718.5 小结 589第八部分 虚拟专用网第19章 站到站的IPSec连接 59319.1 IPSec准备 59319.1.1 基本任务 59319.1.2 外部ACL 59419.2 IKE阶段1:管理连接 59519.2.1 打开ISAKMP/IKE 59619.2.2 定义IKE阶段1策略 59619.3 IKE阶段1对等体认证 59819.3.1 身份类型 59819.3.2 使用预共享密钥的认证 59919.3.3 使用RSA加密Nonce的认证 59919.3.4 使用证书认证 60119.4 IKE阶段2:数据连接 60719.4.1 步骤1:建立一个加密映射 60719.4.2 步骤2:建立变换集 60819.4.3 步骤3:建立加密映射 61019.4.4 步骤4:激活加密映射 61319.4.5 步骤5:验证加密映射配置 61319.5 IPSec连接排错 61419.5.1 检查SA 61419.5.2 使用debug命令 61619.5.3 清除连接 61819.6 L2L举例 61819.7 小结 620第20章 IPSec远程接入连接 62320.1 远程接入概述 62320.1.1 EasyVPN介绍 62420.1.2 EasyVPN IPSec支持 62520.1.3 EasyVPN特性 62520.2 IPSec远程接入连接过程 62620.2.1 步骤1:EVC发起IPSec连接 62720.2.2 步骤2:EVC发送IKE阶段1策略 62720.2.3 步骤3:EVS接受IKE阶段1策略 62720.2.4 步骤4:EVS认证用户 62720.2.5 步骤5:EVS执行IKE模式配置 62820.2.6 步骤6:EVS使用RRI处理路由 62820.2.7 步骤7:IPSec设备建立数据连接 62920.3 IPSec远程接入EVS设置 62920.3.1 配置过程 63020.3.2 任务1:认证策略 63020.3.3 任务2:组策略 63120.3.4 任务3:IKE阶段1策略 63220.3.5 任务4:动态加密映射 63320.3.6 任务5:静态加密映射 63520.3.7 任务6:远程接入验证 63620.4 IPSec远程接入举例 63720.5 小结 639第九部分 案例学习第21章 案例学习 64321.1 公司简介 64321.1.1 公司总部 64321.1.2 分支机构 64521.1.3 远程接入用户 64521.2 提议 64621.3 案例学习配置 64721.3.1 基本配置 64721.3.2 不必要的服务和SSH 64821.3.3 AAA 65021.3.4 访问控制列表 65221.3.5 CBAC和Web过滤 65621.3.6 地址转换 65721.3.7 路由选择 65921.3.8 入侵检测系统 66021.3.9 连接攻击和CBAC 66121.3.10 速率限制 66121.3.11 NTP和系统日志 66321.3.12 站到站VPN 66421.3.13 远程接入VPN 66621.4 小结 668

<<Cisco路由器防火墙安全>>

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>