第一图书网, tushu007.com

# <<Cisco IOS网络安全>>

## 图书基本信息

书名：<<Cisco IOS网络安全>>

13位ISBN编号：9787115090362

10位ISBN编号：711509036X

出版时间：2001-1

出版时间：人民邮电出版社

作者：信达工作室译

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

第一图书网, tushu007.com

# <<Cisco IOS网络安全>>

## 内容概要

本书全面介绍了在Cisco网络设备上如何配置Cisco IOS安全特性，以确保网络安全的方法、技巧和命令。
全书包括五部分：身份认证、授权和统计，安全服务器协议，流量过滤，网络数据加密以及其他安全特性。
第一部分详细介绍了配置身份认证、授权和统计的方法以及命令；第二部分讲述了配置RUDIUS、TACACS+、TACACS、扩展TACAC以及Kerberos的方法和命令；第三部分讨论了配置动态访问列表、反射访问列表和TCP截取的方法和命令；第四部分详细介绍了配置网络数据加密的方法和命令；第五部分介绍了配置口令、权限、IP安全选项的方法以及使用的命令。

本书内容丰富，阐述详细，可作为网络管理人员的参考书或相关领域的培训教材。

第一图书网, tushu007.com

# <<Cisco IOS网络安全>>

## 书籍目录

第1章 安全性概述1.1 本书内容简介1.1.1 身份认证、授权和统计1.1.2 安全服务器协议1.1.3 数据流过滤1.1.4 网络数据加密1.1.5 其他安全特性1.2 创建有效的安全策略1.2.1 安全策略的性质1.2.2 安全策略的两个级别1.2.3 开发有效的安全策略的技巧1.3 认识安全危险和Cisco IOS 解决方案1.3.1 防止对网络设备的未经授权的访问1.3.2 防止对网络的未经授权的访问1.3.3 防止网络数据窃听1.3.4 防止欺骗性路由更新1.4 使用Cisco IOS软件创建防火墙1.4.1 防火墙概述1.4.2 创建防火墙1.4.3 配置防火墙的其他指导原则第一部分 身份认证、授权和统计（AAA）第2章 AAA概述2.1 AAA安全服务2.1.1 使用AAA的益处2.1.2 AAA基本原理2.1.3 方法列表2.2 从何处开始2.2.1 AAA配置过程概述2.2.2 启用AAA2.2.3 停用AAA2.3 下一步工作第3章 配置认证3.1 AAA身份认证方法列表3.1.1 方法列表举例3.1.2 配置AAA身份认证的通用步骤3.2 AAA身份认证方法3.2.1 使用AAA配置登录身份认证3.2.2 使用AAA配置PPP身份认证3.2.3 使用AAA配置ARA身份认证3.2.4 使用AAA配置NASI身份认证3.2.5 启用特权级口令保护3.2.6 启用身份认证覆盖（override）3.2.7 启用双重身份认证3.3 非AAA身份认证方法3.3.1 配置线路口令保护3.3.2 建立用户名身份认证3.3.3 启用CHAP或PAP身份认证3.3.4 配置TACACS和扩展TACACS口令保护3.4 身份认证示例3.4.1 RADIUS身份认证示例3.4.2 TACACS+身份认证示例3.4.3 TACACS和扩展TACACS身份认证示例3.4.4 Kerberos身份认证示例3.4.5 双重身份认证配置示例第4章 身份认证命令4.1 aaa authentication arap4.2 aaa authentication enable default4.3 aaa authentication local-override4.4 aaa authentication login4.5 aaa authentication nasi4.6 aaa authentication password-prompt4.7 aaa authentication ppp4.8 aaa authentication username-prompt4.9 aaa new-model4.10 access-profile4.11 arap authentication4.12 login authentication4.13 login tacacs4.14 nasi authentication4.15 ppp authetication4.16 ppp chap hostname4.17 ppp chap password4.18 ppp chap refuse4.19 ppp chap wait4.20 ppp pap sent-username4.21 ppp use-tacacs第5章 配置授权5.1 AAA授权类型5.2 AAA授权方法5.3 AAA授权前的准备工作5.4 AAA授权配置任务列表5.5 配置授权5.6 关闭全局配置命令授权5.7 授权属性-值对（Attribute-Value Pair）5.8 授权配置示例5.8.1 TACACS+授权示例5.8.2 RADIUS授权示例5.8.3 Kerberos实例映射示例第6章 授权命令6.1 aaa authorization6.2 aaa authorization config-commands6.3 aaa new-model第7章 配置统计7.1 AAA统计类型7.1.1 网络统计7.1.2 连接统计7.1.3 EXEC统计7.1.4 系统统计7.1.5 命令统计7.2 AAA统的准备工作7.3 AAA统计配置任务列表7.4 启用AAA统计7.4.1 禁止为用户名字符串为空的用户会话生成统计记录 7.4.2 生成临时统计记录7.5 监视统计7.6 统计属性-值对7.7 统计配置示例第8章 统计命令8.1 aaa accounting8.2 aaa accounting suppress null-username8.3 aaa accounting update8.4 show accounting第二部分 安全服务器协议第9章 配置RADIUS9.1 RADIUS概述9.2 RADIUS操作9.3 RADIUS配置任务列表9.4 为RADIUS服务器通信配置路由器9.5 为厂商专用的RADIUS服务器通信配置路由器9.6 配置路由器以便向RADIUS服务器 查询静态路由和IP地址 9.7 指定RADIUS身份验证9.8 指定RADIUS授权9.9 指定RADIUS统计9.10 RADIUS属性9.11 厂商专用的RADIUS属性9.12 RADIUS配置示例9.12.1 RADIUS身份验证和授权示例9.12.2 RADIUS AAA示例9.12.3 厂商专用的RADIUS配置示例第10章 RADIUS命令10.1 ip radius source-interface10.2 radius-server configure-nas10.3 radius-server dead-time10.4 radius-server host10.5 radius-server host non-standard10.6 radius-server key10.7 radius-server retransmit10.8 radius-server timeout第11章 配置TACACS+11.1 TACACS+概述11.2 TACACS+操作11.3 TACACS+配置任务列表11.4 指定TACACS+服务器主机11.5 设置TACACS+身份验证密匙11.6 指定TACACS+身份验证11.7 指定TACACS+授权11.8 指定TACACS+统计11.9 TACACS+ AV对11.10 TACACS+配置示例11.10.1 TACACS+身份验证示例11.10.2 TACACS+授权示例11.10.3 TACACS+统计示例11.10.4 TACACS+后台程序配置示例第12章 配置TACACS和扩展TACACS12.1 TACACS协议描述12.2 TACACS和扩展TACACS配置任务列表12.3 设置用户级TACACS口令保护12.4 关闭用户级口令核查12.5 设置可选的口令验证12.6 设置特权级TACACS口令保护12.7 关闭特权级口令核查12.8 设置用户操作通知12.9 设置用户操作身份验证12.10 建立TACACS服务器主机12.11 限制尝试登录的次数12.12 指定登录输入时间12.13 启用扩展TACACS模式12.14 为PPP身份验证启用扩展TACACS12.15 为ARA身份验证启用标准TACACS12.16 为ARA身份验证启用扩展TACACS12.17 启用TACACS，以使用特定的IP地址12.18 TACACS配置示例第13章 TACACS、扩展TACACS和TACACS+命令13.1 TACACS命令比较13.2 arap use-tacacs13.3 enable last-resort13.4 enable use-tacacs13.5 ip tacacs source-interface13.6 tacacs-server attempts13.7

第一图书网, tushu007.com


tacacs-server authenticate13.8 tacacs-server directed-request13.9 tacacs-server extended13.10 tacacs-server host13.11 tacacs-server key13.12 tacacs-server last-resort13.13 tacacs-server login-timeout13.14 tacacs-server notify13.15 tacacs-server optional-passwords13.16 tacacs-server retransmit13.17 tacacs-server timeout第14章 配置Kerberos14.1 Kerberos概述14.2 Kerberos客户支持操作14.2.1 向边界路由器证明身份14.2.2 从KDC取得TGT14.2.3 向网络服务证明身份14.3 Kerberos配置任务列表14.4 使用Kerberos命令配置KDC14.4.1 将用户加入到KDC数据库中14.4.2 在KDC中创建SRVTAB14.4.3 提取SRVTAB14.5 配置路由器，使之使用Kerberos协议14.5.1 定义Kerberos域14.5.2 复制SRVTAB文件14.5.3 指定Kerberos身份验证14.5.4 启用证书转发功能14.5.5 用Telnet登录到路由器14.5.6 建立加密的Kerberized Telnet会话14.5.7 启用强制性Kerberos身份验证14.5.8 启用Kerberos实例映射14.6 监视并维护Kerberos14.7 Kerberos配置示例14.7.1 定义Kerberos域示例14.7.2 复制SRVTAB文件示例14.7.3 Kerberos配置示例14.7.4 指定加密Telnet会话示例第15章 Kerberos命令15.1 clear kerberos creds15.2 connect15.3 kerberos clients mandatory15.4 kerberos credentials forward15.5 kerberos instance map15.6 kerberos local-realm15.7 kerberos preauth15.8 kerberos realm15.9 kerberos server15.10 kerberos srvtab entry15.11 kerberos srvtab remote15.12 key config-key15.13 show kerberos creds15.14 telnet第三部分 数据流过滤第16章 访问控制列表：概述和指南16.1 本章内容16.2 关于访问控制列表16.2.1 访问列表的功能16.2.2 为什么要配置访问列表16.2.3 何时配置访问列表16.2.4 基本访问控制列表与高级访问控制列表16.3 访问列表配置概述16.3.1 创建访问列表16.3.2 给每个访问列表指定一个唯一的名称或编号16.3.3 定义转发包或阻断分组的准则16.3.4 在TFTP服务器上创建和编辑访问列表语句16.3.5 将访问列表用于接口16.4 查找访问列表的完整配置和命令信息第17章 配置锁定和密钥安全性（动态访问列表）17.1 本章内容17.2 关于锁定和密钥17.2.1 锁定和密钥优点17.2.2 何时使用锁定和密钥17.2.3 锁定和密钥的工作原理17.3 Cisco IOS Release 11.1与早期版本的兼容性17.4 电子欺骗对锁定和密钥的威胁17.5 锁定和密钥对路由器性能的影响17.6 配置锁定和密钥前的准备工作17.7 配置锁定和密钥17.7.1 锁定和密钥配置的注意事项17.8 验证锁定和密钥配置17.9 锁定和密钥的维护17.9.1 显示动态访问列表条目17.9.2 手工删除动态访问列表条目17.10 锁定和密钥配置示例17.10.1 使用本地身份验证的锁定和密钥示例17.10.2 使用TACACS+身份验证的锁定和密钥示例第18章 锁定和密钥命令18.1 access-enable18.2 access-template18.3 clear access-template18.4 show ip accounting第19章 配置IP会话过滤（反射访问列表）19.1 本章的内容19.2 关于反射访问列表19.2.1 反射访问列表的优点19.2.2 什么是反射访问列表19.2.3 反射访问列表如何实现会话过滤19.2.4 在何处配置反射访问列表19.2.5 反射访问列表的工作原理19.2.6 使用反射访问列表的限制19.3 配置反射访问列表前的准备工作19.3.1 选择内部接口还是外部接口19.4 配置反射访问列表19.4.1 外部接口配置任务列表19.4.2 内部接口配置任务列表19.4.3 定义反射访问列表19.4.4 嵌套反射访问列表19.4.5 设置全局超时值（可选）19.5 反射访问列表配置示例19.5.1 外部接口配置示例19.5.2 内部接口配置示例第20章 反射访问列表命令20.1 evaluate20.2 ip reflexive-list timeout20.3 permit (reflexive)第21章 配置TCP截取（防止拒绝服务攻击）21.1 本章内容21.2 关于TCP截取21.3 TCP截取配置任务列表21.4 启用TCP截取21.5 设置TCP截取模式21.6 设置TCP截取删除模式21.7 更改TCP截取定时器21.8 更改TCP截取主动阈值21.9 监视和维护TCP截取21.10 TCP截取配置范例第22章 TCP截取命令22.1 ip tcp intercept connection-timeout22.2 ip tcp intercept drop-mode22.3 ip tcp intercept finrst-timeout22.4 ip tcp intercept list22.5 ip tcp intercept max-incomplete high22.6 ip tcp intercept max-incomplete low22.7 ip tcp intercept mode22.8 ip tcp intercept one-minute high22.9 ip tcp intercept one-minute low22.10 ip tcp intercept watch-timeout22.11 show tcp intercept connections22.12 show tcp intercept statistics第四部分 网络数据加密第23章 配置网络数据加密23.1 为什么要加密23.2 Cisco的加密实现23.2.1 什么被加密了23.2.2 分组在网络的什么地方被加密和解密23.2.3 加密分组何时被交换23.2.4 加密路由器如何识别其他对等加密路由器23.2.5 Cisco加密实现了哪些标准23.2.6 Cisco加密如何工作23.3 配置加密前的准备工作23.3.1 确定对等路由器23.3.2 考虑网络拓扑结构23.3.3 确定每个对等路由器中的加密引擎23.3.4 理解实现要点和局限性23.4 配置加密23.4.1 生成DSS公钥/私钥23.4.2 交换DSS公钥23.4.3 启用DES加密算法23.4.4 定义加密映射表，并将它们指定给接口23.4.5 备份配置23.5 GRE隧道加密配置23.5.1 只对GRE隧道通信进行加密23.5.2 对GRE隧道通信和其他通信都进行加密23.6 VIP2中ESA加密配置23.6.1 重置ESA23.6.2 执行其他的加密配置23.7 对Cisco 7200系列路由器上的ESA 进行加密配置23.7.1 必须完成的任务23.7.2 可选任务23.7.3 重置ESA23.7.4 执行其他加密配置23.7.5 启用ESA23.7.6 选择加密引擎23.7.7

第一图书网, tushu007.com


删除DSS密钥23.8 定制加密（配置选项）23.8.1 定义加密会话的持续时间23.8.2 通过预先生成DH编号缩短会话的建立时间23.8.3 修改加密访问列表的限制23.9 关闭加密23.10 加密测试和故障排除23.10.1 测试加密配置23.10.2 诊断连接故障23.10.3 使用调试命令23.11 加密配置示例23.11.1 生成DSS公钥/私钥示例23.11.2 交换DSS密钥示例23.11.3 启用DES加密算法示例23.11.4 建立加密访问列表、定义加密映射表并将它用于接口的示例 23.11.5 修改加密访问列表限制示例23.11.6 GRE隧道加密配置示例23.11.7 ESA特有加密配置任务示例23.11.8 删除DSS密钥示例23.11.9 测试加密连接示例第24章 网络数据加密命令24.1 access-list（encryption）24.2 clear crypto connection24.3 crypto algorithm 40-bit-des24.4 crypto algorithm des24.5 crypto clear-latch24.6 crypto esa24.7 crypto gen-signature-keys24.8 crypto key-exchange24.9 crypto key-exchange passive24.10 crypto key-timeout24.11 crypto map(global configuration)24.12 crypto map(interface configuration)24.13 crypto pregen-dh-pairs24.14 crypto public-key24.15 crypto sdu connections24.16 crypto sdu entities24.17 crypto zeroize24.18 deny24.19 ip access-list extended(encryption)24.20 match address24.21 permit24.22 set algorithm 40-bit-des24.23 set algorithm des24.24 set peer24.25 show crypto algorithms24.26 show crypto card24.27 show crypto connections24.28 show crypto engine brief24.29 show crypto engine configuration24.30 show crypto engine connections active24.31 show crypto engine connections dropped-packets24.32 show crypto key-timeout24.33 show crypto map24.34 show crypto map interface24.35 show crypto map tag24.36 show crypto mypubkey24.37 show crypto pregen-dh-pairs24.38 show crypto pubkey24.39 show crypto pubkey name24.40 show crypto pubkey serial24.41 test crypto initiate-session第五部分 其他安全特性第25章 配置口令和权限25.1 保护对特权EXEC 命令的访问25.1.1 设置或修改静态有效口令25.1.2 使用有效口令和有效密钥保护口令25.1.3 设置或修改线路口令25.1.4 为特权EXEC模式设置TACACS口令保护25.2 加密口令25.3 配置多重权限级别25.3.1 设置命令的权限级别25.3.2 修改线路的默认权限级别25.3.3 显示当前的权限级别25.3.4 登录到某个权限级别25.4 恢复丢失的有效口令25.4.1 恢复口令的步骤25.4.2 第一种口令恢复方法25.4.3 第二种口令恢复方法25.5 恢复丢失的线路口令25.6 配置标识支持25.7 口令和权限配置示例25.7.1 多重权限级别示例25.7.2 用户名示例第26章 口令和权限命令26.1 enable26.2 enable password26.3 enable secret26.4 ip identd26.5 password26.6 privilege level (global)26.7 privilege level (line)26.8 service password-encryption26.9 show privilege26.10 username第27章 邻接路由器身份认证--概述和指南27.1 本章内容27.2 邻接身份认证的优点27.3 使用邻接身份认证的协议27.4 何时配置邻接身份认证27.5 邻接身份认证的工作原理27.5.2 明文身份认证27.5.2 MD5身份认证27.6 密钥管理（密钥链）第28章 配置IP安全选项邻28.1 本章的内容28.2 配置基本IP安全选项28.2.1 启用IPSO并设置安全机密级别28.2.2 指定如何处理IP安全选项28.3 配置扩展IP安全选项28.3.1 配置全局默认设置28.3.2 将ESO附加到接口28.3.3 将AESO附加到接口28.4 配置DNSIX审计跟踪功能28.4.1 启用DNSIX审计跟踪功能28.4.2 指定接收审计跟踪消息的主机28.4.3 指定传输参数28.5 IPSO配置示例28.5.1 示例128.5.2 示例2第29章 IP安全选项命令29.1 dnsix-dmdp retries29.2 dnsix-nat authorized-redirection29.3 dnsix-nat primary29.4 dnsix-nat secondary29.5 dnsix-nat source29.6 dnsix-nat transmit-count29.7 ip security add29.8 ip security aeso29.9 ip security dedicated29.10 ip security eso-info29.11 ip security eso-max29.12 ip security eso-min29.13 ip security extended-allowed29.14 ip security first29.15 ip security ignore-authorities29.16 ip security implicit-labelling29.17 ip security multilevel29.18 ip security reserved-allowed29.19 ip security strip29.20 show dnsix附录A RADIUS属性A.1 支持的RADIUS属性A.2 RADIUS统计属性A.3 RADIUS厂商专用特性附录B TACACS+属性-值对B.1 TACACS+属性-值对B.2 TACACS+统计AV对

第一图书网, tushu007.com

# <<Cisco IOS网络安全>>

## 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