CiscoIOS配置SSH详解 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/245/2021_2022_CiscoIOS_E9_85_c101_245619.htm 使用telnet进行远程设备维护的时候，由于密码和通讯都是明文的，易受sniffer侦听，所以应采用SSH替代telnet.SSH （Secure Shell）服务使用tcp 22 端口，客户端软件发起连接请求后从服务器接受公钥，协商加密方法，成功后所有的通讯都是加密的。Cisco 设备目前只支持SSH v1，不支持v2.Cisco实现 SSH的目的在于提供较安全的设备管理连接，不适用于主机到主机的通讯加密。Cisco推荐使用IPSEC作为端对端的通讯加密解决方案。 1.IOS设备（如6500 MSFC、8500、7500）的配置： a） 软件需求 IOS版本12.0.（10）S以上 含IPSEC 56 Feature 推荐使用 IOS 12.2 IP PLUS IPSEC 56C以上版本 基本上Cisco全系列路由器都已支持，但为运行指定版本的软件您可能需要相应地进行硬件升级 b） 定义用户 user mize pass nnwh@163.net user sense secret ssn d） 定义域名 ip domain-name mize.myrice.com //配置SSH必需 e） 生成密钥 crypto key generate rsa modulus 2048 执行结果：The name for the keys will be: 6509-mize.myrice.com % The key modulus size is 2048 bits Generating RSA keys ... [OK] f）指定可以用SSH登录系统的主机的源IP地址access-list 90 remark Hosts allowed to SSH in //低版本可能不支持remark关键字 access-list 90 permit 10.10.1.100 access-list 90 permit 10.10.1.101 g） 限制登录line con 0 login local line vty 0 4 login local //使用本地定义的用户名和密码登录 transport input SSH //只允许用SSH登录(注意：禁止telnet和从交换引擎session!) access-class 90 in //只允许指定源主机登录

2.CatOS（如6500/4000交换引擎）的配置： a） 软件需求 运行CatOS的6500/4000交换引擎提供SSH服务需要一个6.1以上“ k9 ”版本的软件，如： cat6000-sup2cvk9.7-4-3.bin 和 cat4000-k9.6-3-3a.bin. 8540/8510交换机支持SSH需要以上12.1（12c）EY版本软件。 3550交换机支持SSH需要12.1（11）EA1以上版本软件。 其他交换机可能不支持SSH. b） 生成密钥 set crypto key rsa 2048 密钥的生成需要1-2分钟，执行完毕后可用命令show crypto key查看生成的密钥。 c） 限制管理工作站地址set ip permit 10.10.1.100 ssh //只允许使用SSH登录的工作站 set ip permit 10.10.1.101 ssh set ip permit enable ssh //检查SSH连接的源地址 set ip permit enable telnet //检查telnet连接的源地址 set ip permit enable snmp //检查snmp请求的源地址 如果服务的ip permit 处于disable状态，所有的连接将被允许（当然服务如telnet本身可能包含用户认证机制）。如果指定服务的ip permit 处于enable状态，则管理工作站的地址必须事先用set ip permit [可选的子网掩码] [允许使用的服务类型（ssh/telnet/snmp）]来定义 可用命令 show ip permit 来检查ip permit 的配置 某些服务可能存在安全漏洞（如http）或协议本身设计就是比较不安全的（如snmp、telnet）。如果服务不是必要的，可以将之关闭；如果服务是必须的，应采取措施保证这些服务仅向合法用户提供： 6500/4000交换引擎：set ip http server disable //关闭http服务 set ip permit enable snmp //限制SNMP源地址 set snmp comm. read-only //清空预设的SNMP COMM字 set snmp comm. read-write set snmp comm. read-write-all 8500、7500、MSFC等IOS设备：no ip http server //关闭http服务 no snmp //关闭snmp服务 no service dhcp //关闭

dhcp 服务 no ip finger //关闭 finger 服务 no service tcp-small-server //关闭tcp基本服务 no service udp-small-server //关闭 udp基本服务 service password-encryption //启用明文密码加密服务 3.SSH 客户端 a） 从管理工作站登录 必须使用支持SSH v1协议的终端仿真程序才能使用SSH协议管理设备，推荐使用Secure CRT 3.3， 也可以使用免费软件putty.下面介绍使用Secure CRT登录SSH设备的方法： 运行Secure CRT程序，选择菜单File Quick Connect…设置以下参数：Protocol（协议）：ssh1 Hostname（主机名）：10.10.1.1 Port（端口）：22 Username（用户名）：mize Ciper（加密方法）：3DES Authentication（认证方式）assword 点击Connect，这时可能会提示您接受来自设备的加密公钥，选择Accept once（只用一次）或Accept &amp. Save （保存密钥以便下次使用）。由于协议实现的问题，可能会碰到SSH Buffer Overflow的问题，如果出现“ 收到大于16k的密钥 ”的提示，请重新连接。连接正常，输入密码即可登录到系统。 第二次登录点击File Connect 点击连接10.10.1.1即可。 b） 从IOS设备用SSH协议登录其他设备 IOS设备也可以发起SSH连接请求（作为SSH Client），从IOS设备登录支持3DES的IOS设备，使用以下命令（-l 指定用户名）：ssh l mize 10.10.3.3 从IOS设备登录支持 DES（56位）的IOS，使用以下命令（-c des指定1 des加密方式）：ssh c des l mize 10.10.5.5 从IOS设备登录支持 3DES的CatOS，如6509/4006的交换引擎，使用如下命令（无需指定用户名）：ssh 10.10.6.6 4.限制telnet源地址 对于未支持SSH 的设备，可采取限制telnet源地址的方法来加强安全性。为了不致于增加一个管理员地址就要把所有的设备配置修改一遍，可以采用

中继设备的方法，即受控设备只允许中继设备的telnet访问，中继设备则允许多个管理员以较安全的方法（如SSH）登录。 设置中继设备：inter lo 0 ip address 10.10.1.100 255.255.255.255 ip telnet source-interface Loopback0 //发起telnet的源地址 设置受控设备：access-list 91 remark Hosts allowed to TELNET in access-list 91 permit 10.10.1.100 access-list 91 permit 10.10.1.101 line con 0 password xxxxxxxx line vty 0 4 password xxxxxxxx access-class 91 in 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com