使用TACACS+，配置拨号认证的Cisco路由器

目录

简介

本文档介绍如何使用在UNIX上运行的TACACS+配置思科路由器以进行拨号身份验证。TACACS+提供的功能不如市售的Cisco Secure ACS for Windows或Cisco Secure ACS for UNIX提供的功能多。

Cisco Systems 以前提供的 TACACS+ 软件已停产并且不再受 Cisco Systems 支持。

今天，当您在您最喜爱的 Internet 搜索引擎上搜索“TACACS+ 免费软件”时，您可以找到许多可用的 TACACS+ 免费软件版本。Cisco 并不具体推荐任何特定的 TACACS+ 免费软件版本实施。

Cisco 安全访问控制服务器 (ACS) 可通过世界范围内的常规 Cisco 销售和分销渠道购买。Cisco Secure ACS for Windows 包括在 Microsoft Windows 工作站实施独立安装所需的全部必要组件。Cisco Secure ACS 解决方案引擎随附有预先安装的 Cisco Secure ACS 软件许可证。有关产品编号，请参阅Cisco Secure ACS 4.0产品公告。访问 Cisco 订购主页（仅限注册用户）下订单。

注意：您需要具有关联服务合同的CCO帐户才能获取Cisco Secure ACS for Windows的90天试用版(仅限注册客户)。

本文档中的路由器配置是在运行Cisco IOS®软件版本11.3.3的路由器上开发的。Cisco IOS软件版本12.0.5.T及更高版本使用**group tacacs+**而不**是tacacs+**。aaa authentication login default tacacs+ **enable等语句显示**为aaa authentication login default group tacacs+ **enable**。

您可以通过anonymous ftp将TACACS+免费软件和用户指南下载到/pub/tacacs目录中的ftp-

eng.cisco.com。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)查找有关本文档中使用的命令的其他信息。

本文档使用以下配置：

- 路由器配置
- 免费软件服务器上的 TACACS+ 配置文件

路由器配置

```
!
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication ppp default if-needed tacacs+
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-
authenticated
aaa authorization commands 15 default tacacs+ if-
authenticated
aaa authorization network default tacacs+
enable password ww
!
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
!
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!
 !--- Challenge Handshake Authentication Protocol !---
(CHAP/PPP) authentication user. interface Async1 ip
unnumbered Ethernet0 encapsulation ppp async mode
dedicated peer default ip address pool async no cdp
enable ppp authentication chap ! !--- Password
Authentication Protocol (PAP/PPP) authentication user.
interface Async2 ip unnumbered Ethernet0 encapsulation
```

```
ppp async mode dedicated peer default ip address pool
async no cdp enable ppp authentication pap ! !---
Authentication user with autocommand PPP. interface
Async3 ip unnumbered Ethernet0 encapsulation ppp async
mode interactive peer default ip address pool async no
cdp enable ! ip local pool async 10.6.100.101
10.6.100.103 tacacs-server host 171.68.118.101 tacacs-
server timeout 10 tacacs-server key cisco ! line 1
session-timeout 20 exec-timeout 120 0 autoselect during-
login script startup default script reset default modem
Dialin transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! line 2 session-
timeout 20 exec-timeout 120 0 autoselect during-login
script startup default script reset default modem Dialin
transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect
ppp script startup default script reset default modem
Dialin autocommand ppp transport input all stopbits 1
rxspeed 115200 txspeed 115200 flowcontrol hardware ! end
```

免费软件服务器上的 TACACS+ 配置文件

```
!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }
```

Microsoft Windows安装程序

用于用户 1 和 2 的 Microsoft Windows 设置

本部分提供有关如何配置本文档所述功能的信息。

逐步指导

完成下面这些步骤。

注意：PC配置可能因您使用的操作系统版本而略有不同。

1. 选择**开始 > 程序 > 附件 > 拨号网络**以打开“拨号网络”窗口。
2. 从“**连接”菜**单中选择“新建连接”，然后输入连接的名称。
3. 输入调制解调器特定信息，然后单击**Configure**。
4. 在“常规属性”页上，选择调制解调器的最高速度，但不要选中“**仅以此速度连**接.....”框。
5. 在“配置/连接属性”页上，使用8个数据位、无奇偶校验和1个停止位。要使用的呼叫首选项**是“在拨号前等待拨号音”**和**“如果200秒后未连接则取消呼叫”**。

6. 在“连接”(Connection)页面上，单击**“高级”**。在“高级连接设置”中，仅选择“硬**件流控制和调**制类型**标准”**。在“配置/选项”属性页上，除状态控制下的框外，不应选中任何内容。
7. 单击“**OK(确**定)”，然后单击“**Next(下一步**)”。
8. 输入目标的电话号码，再次单击“**Next”，然后单击“Finish”**。
9. 出现新连接图标后，右键单击该图标并选择“属性”**>“服务器类型”**。
10. 选**择PPP:WINDOWS 95、WINDOWS NT 3.5、Internet，**不选中任何高级选项。
11. 检查**Allowed Network Protocols(允许的网络协议)**下的TCP/IP。
12. 在TCP/IP Settings..（TCP/IP设置……）下，选择**Server assigned IP address**（服务器分配的名称服务器地址）**，然后选择Use default gateway on remote network（在远程网络上使用默认网关），然后单击OK**。
13. 当用户双击图标以显示“连接到”窗口以进行拨号时，用户必须填写“用户名”和“密码”字段，然后单击“连**接”**。

用于用户 3 的 Microsoft Windows 设置

用户3（使用autocommand PPP的身份验证用户）的配置与用户1和用户2的配置相同，但以下情况除外：

- 在“配置/选项”属性页（第6步）上，选中**拨号后打开终端窗口**。
- 当用户双击该图标以打开要拨号的“连接到”窗口（步骤13）时，用户不会填写“用户名”和“密码”字段。用户单击“**连接”**。在与路由器建立连接后，用户在显示的黑色窗口中键入用户名和密码。身份验证后，用户按**继续(F7)**。

验证

当前没有可用于此配置的验证过程。

故障排除

路由器

发出 debug 命令之前，请参阅有关 debug 命令的重要信息。

- **terminal monitor** — 显示**当**前终端和会话的debug命令输出和系统错误消息。
- **debug ppp negotiation** — 显示在PPP启动期间发送的PPP数据包，在此处协商PPP选项。
- **debug ppp packet** — 显示发送和接收的PPP数据包。（此命令显示低级数据包转储信息。）
- **debug ppp chap** — 显示有关客户端是否通过身份验证的信息（对于11.2之前的Cisco IOS软件版本）。
- **debug aaa authentication — 显示有关身份验证、授权和记帐 (AAA)/TACACS+ 身份验证的信息。**
- **debug aaa authorization - 显示有关 AAA/TACACS+ 授权的信息。**

服务器

注意： 这假设思科的TACACS+免费软件服务器代码。

```
tac_plus_executable -C config.file -d 16
  tail -f /var/tmp/tac_plus.log
```

相关信息

- TACACS+ 支持页
- IOS 文档中的 TACACS+
- 思科安全访问控制服务器
- 安装和调试 CiscoSecure 2.x TACACS+
- 技术支持和文档 - Cisco Systems