使用TACACS+配置思科路由器以進行撥號身份驗證

目錄

簡介

本檔案介紹如何使用UNIX上執行的TACACS+設定思科路由器以進行撥號驗證。TACACS+提供的功能不如市售的Cisco Secure ACS for Windows或Cisco Secure ACS for UNIX多。

Cisco Systems先前提供的TACACS+軟體已停產，且Cisco Systems不再支援。

現在，您在您喜愛的網際網路搜尋引擎上搜尋「TACACS+免費軟體」時，可以找到許多可用的TACACS+免費軟體版本。思科並不特別建議實施任何特定的TACACS+免費軟體。

思科安全存取控制伺服器(ACS)可透過世界各地的定期思科銷售和分銷管道購買。Cisco Secure ACS for Windows包含在Microsoft Windows工作站上進行獨立安裝所需的所有必要元件。Cisco Secure ACS解決方案引擎附帶預裝的Cisco Secure ACS軟體許可證。請參閱Cisco Secure ACS 4.0產品公告，瞭解產品編號。訪問思科訂購首頁(僅限註冊客戶)下訂單。

附註：您需要具有相關服務合約的CCO帳戶才能獲得Cisco Secure ACS for Windows的90天試用版(僅限註冊客戶)。

本檔案中的路由器組態是在執行Cisco IOS®軟體版本11.3.3的路由器上開發。Cisco IOS軟體版本12.0.5.T和更新版本使用**group tacacs+**而不是**tacacs+**。諸如**aaa authentication login default tacacs+ enable**之類的語句顯示為**aaa authentication login default group tacacs+ enable**。

您可以通過匿名ftp將TACACS+免費軟體和使用手冊下載到/pub/tacacs目錄中的ftp-eng.cisco.com。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

組態

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅供已註冊客戶使用)查詢有關本文檔中使用的命令的其他資訊。

本檔案會使用以下設定：

- 路由器配置
- 免費軟體伺服器上的TACACS+配置檔案

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
```

免費軟體伺服器上的TACACS+配置檔案

```
!--- 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安裝程式

使用者1和2的Microsoft Windows安裝程式

本節提供用於設定本文件中所述功能的資訊。

逐步說明

請完成以下步驟。

注意：PC配置可能因您使用的作業系統版本而略有不同。

1. 選擇**Start > Programs > Accessories > Dial-Up Networking**以開啟Dial-Up Networking視窗。
2. 從「連線」選單中選擇**新建連線**，然後輸入連線的名稱。
3. 輸入數據機特定的資訊，然後按一下**Configure**。
4. 在General Properties頁面上，選擇數據機的最高速度，但是不要選中**Only connect at this speed**...框。
5. 在「配置/連線屬性」頁上，使用8個資料位、無奇偶校驗位和1個停止位。要使用的呼叫首選

項是**Wait for dial tone before dialing**和**Cancel the call if not connected after 200 seconds**。
6. 在「連線」頁面上，按一下**高級**。在Advanced Connection Settings中，僅選擇**Hardware Flow Control**和**Modulation Type Standard**。在「配置/選項」屬性頁面上，除「狀態控制」下的框外，不應選中任何內容。
7. 按一下「**OK**」，然後按一下「**Next**」。
8. 輸入目標的電話號碼，再次按一下**Next**，然後按一下**Finish**。
9. 顯示新連線圖示後，按一下右鍵該圖示，然後選擇**「屬性」>「伺服器型別」**。
10. 選擇**PPP:WINDOWS 95、WINDOWS NT 3.5、Internet**，並且不選中任何高級選項。
11. 在Allowed Network Protocols下檢查**TCP/IP**。
12. 在「TCP/IP設定……」下，選擇**伺服器分配的IP地址**、**伺服器分配的名稱伺服器地址**和**在遠端網路上使用預設網關**，然後按一下**確定**。
13. 當使用者按兩下圖示以顯示「連線到」視窗以進行撥號時，使用者必須填寫「使用者名稱」和「密碼」欄位，然後按一下**連線**。

使用者3的Microsoft Windows安裝程式

使用者3（使用自動命令PPP進行身份驗證的使用者）的配置與使用者1和使用者2的配置相同，但以下情況例外：

- 在「Configure/Options properties（配置/選項屬性）」頁面（步驟6）上，選中**Bring up terminal window after dialing**。
- 當使用者按兩下該圖示以開啟「連線至」視窗進行撥號時（步驟13），使用者不會填寫「使用者名稱」和「密碼」欄位。使用者按一下**Connect**。連線到路由器後，使用者在出現的黑色視窗中鍵入使用者名稱和密碼。身份驗證後，使用者按**Continue(F7)**。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

路由器

發出**debug**指令之前，請先參閱有關Debug指令的重要資訊。

- **terminal monitor** — 顯示**debug**命令輸出以及目前終端和作業階段的系統錯誤訊息。
- **debug ppp negotiation** — 顯示在PPP啟動期間傳送的PPP資料包，其中協商了PPP選項。
- **debug ppp packet** — 顯示傳送和接收的PPP資料包。（此命令顯示低級資料包轉儲。）
- **debug ppp chap** — 顯示有關客戶端是否通過身份驗證（對於11.2版之前的Cisco IOS軟體版本）的資訊。
- **debug aaa authentication** — 顯示有關身份驗證、授權和記帳(AAA)/TACACS+身份驗證的資訊。
- **debug aaa authorization** — 顯示有關AAA/TACACS+授權的資訊。

伺服器

附註： 此假設使用思科的TACACS+免費軟體伺服器代碼。

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

相關資訊

- TACACS+支援頁面
- IOS 文件中的 TACACS+
- 思科安全存取控制伺服器
- 設定和調試CiscoSecure 2.x TACACS+
- 技術支援與文件 - Cisco Systems