設定和調試CiscoSecure 2.x TACACS+

目錄

簡介

本文檔旨在協助首次使用Cisco Secure 2.x的使用者設定和調試Cisco Secure TACACS+配置。它並非思科安全功能的詳盡說明。

有關伺服器軟體和使用者設定的詳細資訊，請參閱您的Cisco Secure文檔。有關路由器命令的詳細資訊，請參閱Cisco IOS軟體文檔以獲得相應版本。

必要條件

需求

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Secure ACS 2.x及更高版本
- Cisco IOS®軟體版本11.3.3及更新版本

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定Cisco Secure

請完成以下步驟：

1. 確保使用軟體附帶的說明在UNIX伺服器上安裝Cisco Secure代碼。
2. 若要確認產品停止和啟動，請將`cd/etc/rc0.d`，並以root使用者身份執行`/K80Cisco Secure`（停止守護程式）。將`cd/etc/rc2.d`，並作為root使用者執行`/S80Cisco Secure`（用於啟動守護程式）。啟動時，您應該會看到以下消息：
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   運行`$BASE/utils/psg`，以確保每個進程至少有一個運行，例如SQLAnywhere或其他資料庫引擎、Cisco Secure資料庫伺服器進程、Netscape Web Server、Netscape Web Admin、Acme Web Server、Cisco Secure AAA進程或自動重新啟動進程。
3. 為了確保您位於正確的目錄中，請在外殼環境中設定環境變數和路徑。此處使用c-shell。**$BASE是**安裝期間選擇的Cisco Secure的安裝目錄。它包含DOCS、DBServer、CSU等目錄。在此範例中，假設安裝在/opt/CSCOacs中，但您的系統可能有所不同：
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY是在安裝期間選擇安裝預設Cisco Secure資料庫的目錄。如果使用的是產品附帶的預設資料庫SQLAnywhere，則它包含資料庫、文檔等目錄。在此範例中，假設安裝在/opt/CSCOacs/SYBSsa50中，但您的系統可能有所不同。
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   將外殼環境中的路徑新增到：
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD到$BASE/config**CSU.cfg**是Cisco Secure Server控制檔案。製作此檔案的備份副本。在此檔案中，`LIST config_license_key`顯示您在購買軟體後通過許可流程接收的許可證金鑰；如果這是一個4埠試用許可證，則可以忽略此行。**NAS config_nas_config**部分可以包含預設的網路訪問伺服器(NAS)或路由器，或者您在安裝過程中輸入的NAS。在本例中，出於調試目的，您可以允許*任何*NAS與Cisco Secure Server進行通訊，而*無金鑰*。例如，從包含/* NAS名稱的行中刪除NAS的名稱和金鑰，可以轉到此處*/"和/*NAS/Cisco安全金鑰*/。該地區唯一*的*標準是：
   ```
   NAS config_nas_config = {
     {
       "",          /* NAS name can go here */
       "",              /* NAS/Cisco Secure secret key */
       "",                          /* message_catalogue_filename */
       1,                           /* username retries */
       2,                           /* password retries */
       1                            /* trusted NAS for SENDPASS */
     }
   };

   AUTHEN config_external_authen_symbols = {
   ```
   執行此操作時，您會告訴Cisco Secure它允許與所有NAS進行通訊，而無需交換金鑰。
5. 如果您希望調試資訊轉到/var/log/csuslog，則您需要在CSU.cfg的頂部有一行，它告訴伺服器要執行多少調試。0X7FFFFF增加了所有可能的調試。相應地新增或修改此行：
   ```
   NUMBER config_logging_configuration = 0x7FFFFFFF;
   ```
   此附加行將調試資訊傳送到local0:
   ```
   NUMBER config_system_logging_level = 0x80;
   ```

此外，請新增以下專案以修改/etc/syslog.conf檔案：

```
local0.debug /var/log/csuslog
```

然後回收syslogd以重新讀取：

```
kill -HUP `cat /etc/syslog.pid`
```

回收Cisco Secure伺服器：

```
/etc/rc0.d/K80Cisco Secure
/etc/rc2.d/S80Cisco Secure
```

應該還是要開始。

6. 您可能希望使用瀏覽器新增使用者、組等，或者使用CSimport實用程式。使用CSimport可以輕鬆地將本文檔末尾平面檔案中的示例使用者移動到資料庫中。這些使用者將用於測試用途，並且您可以在讓自己的使用者進入後將其刪除。匯入後，您可通過GUI檢視匯入的使用者。如果您決定使用CSimport:

   ```
   CD $BASE/utils
   ```

   將本文檔末尾的使用者和組配置檔案放在一個檔案中，如系統中的任何位置，然後從$BASE/utils目錄(後台守護程式正在運行，例如/etc/rc2.d/S80Cisco Secure)，並以使用者根使用者身份，使用測試(-t)選項運行CSimport:

   ```
   ./CSimport -t -p <path_to_file> -s <name_of_file>
   ```

   此指令會測試使用者的語法；您應該收到如下消息：

   ```
   Secure config home directory is: /opt/CSCOacs/config/CSConfig.ini
   hostname = berry and port = 9900 and clientid = 100
   /home/ddunlap/csecure/upgrade.log exists, do you want to write over 'yes' or 'no' ?
   yes
   Sorting profiles...
   Done sorting 21 profiles!
   Running the database import test...
   ```

   您不*應收*到以下消息：

   ```
   Error at line 2: password = "adminusr"
   Couldn't repair and continue parse
   ```

   無論是否有錯誤，請檢查upgrade.log以確保配置檔案已簽出。更正錯誤後，從$BASE/utils目錄，後台守護程式正在運行(/etc/rc2.d/S80Cisco Secure)，並以使用者根使用者身份運行CSimport with the commit(-c)選項，將使用者移動到資料庫中：

   ```
   ./CSimport -c -p <path_to_file> -s <name_of_file>
   ```

   同樣，螢幕上或upgrade.log中不應出現錯誤。
7. 思科安全相容性技術提示中列出支援的瀏覽器。在PC瀏覽器中，指向Cisco Secure/Solaris框**http://#.#.#.#/cs**，其中**#.#.#.#**是Cisco Secure/Solaris伺服器的IP。在顯示的螢幕上，使用者輸入**superuser**，密碼輸入**changeme**。此時請勿更改密碼。如果您在上一步中使用了CSimport，您應該會看到新增的使用者/組，或者您可以按一下**browse block off**並通過GUI手動新增使用者和組。

設定身份驗證

註：此路由器配置是在運行Cisco IOS軟體版本11.3.3的路由器上開發的。Cisco IOS軟體版本12.0.5.T及更高版本顯示group tacacs而不是tacacs。

此時，請配置路由器。

1. 配置路由器時終止Cisco Secure。

   ```
   /etc/rc0.d/K80Cisco Secure to stop the daemons.
   ```
2. 在路由器上，開始配置TACACS+。輸入啟用模式，並在命令集之前鍵入`conf t`。此語法可確保您在未運行*Cisco Secure*時不會鎖定在路由器之外。輸入`ps -ef | grep Secure`檢查以確保Cisco Secure未運行，如果是，則終止–9進程：

```
!--- Turn on TACACS+ aaa new-model enable password whatever !--- These are lists of
authentication methods, !--- that is, vtymethod and conmethod are !--- names of lists, and
the methods listed on the !--- same lines are the methods in the order to be !--- tried. As
used here, if authentication !--- fails due to Cisco Secure not being started, !--- the
enable password is accepted !--- because it is in each list. aaa authentication login
vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable !--- Point the
router to the server, that is, !--- #.#.#.# is the server IP address. tacacs-server host
#.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !---
during debugging. exec-timeout 0 0 login authentication conmethod line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0
0 login authentication vtymethod
```

3. 繼續進行之前，請進行測試，確保您仍可以通過Telnet和控制檯埠訪問路由器。由於Cisco Secure沒有運行，因此應該接受啟用密碼。**注意：**保持控制檯埠會話處於活動狀態並保持啟用模式；此會話不應超時。此時您開始限制對路由器的訪問，您需要能夠進行配置更改而不將自己鎖定。發出以下命令，以便檢視路由器上伺服器到路由器的互動：
   ```
   terminal monitor
   debug aaa authentication
   ```
4. 以root使用者身份在伺服器上啟動Cisco Secure:
   ```
   /etc/rc2.d/S80Cisco Secure
   ```
   這將啟動進程，但您希望啟用比S80Cisco Secure中配置的調試更多的調試，因此：
   ```
   ps -ef | grep Cisco Secure
   kill -9 <pid_of CS_process>

   CD $BASE/CSU
   ./Cisco Secure -cx -f $BASE/config/CSU.cfg to start the Cisco Secure process with debugging
   ```
   如果使用`-x`選項，Cisco Secure將在前台運行，以便觀察路由器與伺服器的互動。您不應看到錯誤消息。由於 — x選項，Cisco Secure進程應啟動並掛起。
5. 在另一個視窗中，檢查以確保Cisco Secure已啟動。輸入`ps -ef`並查詢Cisco Secure進程。
6. Telnet(vty)使用者現在必須通過Cisco Secure進行身份驗證。在路由器上進行偵錯時，從網路的另一部分Telnet至路由器。路由器應顯示使用者名稱和密碼提示。您應該可以使用以下使用者ID/密碼組合訪問路由器：
   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```
   觀察應檢視互動的伺服器和路由器，即傳送位置、響應和請求等。請更正所有問題，然後再繼續。
7. 如果您也希望使用者透過Cisco Secure進行驗證以進入啟用模式，請確保您的主控台連線埠作業階段仍處於作用中狀態，並將以下命令新增到路由器中：

   ```
   !--- For enable mode, list 'default' looks to Cisco Secure !--- then enable password if
   Cisco Secure is not running. aaa authentication enable default tacacs+ enable
   ```
8. 您現在必須通過**Cisco Secure**啟用。在路由器上進行偵錯時，從網路的另一部分Telnet至路由器。當路由器要求使用者名稱/密碼時，使用`operator/oper`響應。使用者操作員嘗試進入啟用模式（許可權級別15）時，需要密碼「cisco」。沒有許可權級別語句（或思科安全守護程式關閉），其他使用者將無法進入啟用模式。觀察伺服器和路由器，您應該從其中看到思科安全互動，例如，從何處傳送的內容、響應和請求等。在繼續之前更正所有問題。
9. 在連線到控制檯埠的同時關閉伺服器上的Cisco Secure進程，以確保您的使用者在Cisco Secure關閉時仍可以訪問路由器：
   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```
   重複上一步的Telnet和啟用。路由器應意識到Cisco Secure進程不會響應，允許使用者使用預設啟用密碼登入和啟用。
10. 再次啟動Cisco Secure伺服器並建立到路由器的Telnet會話（該會話應通過Cisco Secure進行身份驗證），使用userid/password **operator/oper**檢查通過Cisco Secure對控制檯埠使用者的

身份驗證。在確認可以通過控制檯埠登入到路由器之前，保持通過遠端登入到路由器並處於啟用模式。例如，通過控制檯埠註銷與路由器的原始連線，然後重新連線到控制檯埠。使用先前使用者ID/密碼組合登入的控制檯埠身份驗證現在應通過Cisco Secure。例如，必須先使用userid/password **operator/oper**和**cisco**密碼才能啟用。

設定

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(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

新增授權

新增授權是可選的。

預設情況下，路由器上有三個命令等級：

- 許可權級別0 — 包括禁用、啟用退出、幫助和註銷
- 許可權級別1 - Telnet上的正常級別和提示符為`router>`
- 許可權級別15 — 啟用級別並提示`router#`

由於可用命令取決於Cisco IOS功能集、Cisco IOS軟體版本、路由器型號等，因此沒有第1級和第15級所有命令的完整清單。例如，**show ipx route**不存在於僅IP功能集中，**show ip nat trans**不位於Cisco IOS軟體版本10.2.X代碼中，因為當時未引入NAT，並且沒有電源和溫度監控的路由器型號中沒有**show environment**。

可以找到特定路由器中特定級別的可用命令，可以輸入**?**處於該許可權級別時，在路由器中提示符處。

在實施CSCdi82030之前，未將控制檯埠授權新增為功能。預設情況下，控制檯埠授權處於關閉狀態，以減少路由器意外鎖定的可能性。如果使用者可以通過控制檯對路由器進行物理訪問，則控制檯埠授權不會非常有效。但是，可以在使用**authorization exec default|WORD**命令實施CSCdi82030的Cisco IOS映像中，在**line con 0**命令下開啟控制檯埠授權。

請完成以下步驟：

1. 路由器可以配置為在所有級別或某些級別通過Cisco Secure授權命令。此路由器配置允許所有使用者在伺服器上設定每個命令的授權。您可以通過Cisco Secure對所有命令進行授權，但是如果伺服器發生故障，則無需授權，因此`none`。在Cisco Secure Server關閉的情況下，輸入以下命令：輸入以下命令可移除必須透過Cisco Secure執行驗證的要求：
   ```
   no aaa authentication enable default tacacs+ none
   ```
   輸入以下命令可要求通過Cisco Secure進行命令授權：
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. 當Cisco Secure Server運行時，使用userid/password **loneusr/lonepwd**Telnet到路由器。此使用者應該不能執行除以下命令以外的任何命令：
   ```
   show version
   ping <anything>
   logout
   ```
   先前使用者**adminusr/adminusr**、**operator/oper**、**desusr/encrypt**仍憑藉其預設服務=permit有能力執行所有命令。如果進程出現問題，請進入路由器的啟用模式，然後使用以下命令開啟授

權調試：

```
terminal monitor
debug aaa authorization
```

觀察應看到思科安全互動的伺服器和路由器，例如，傳送內容、響應、請求等。請更正所有問題，然後再繼續。

3. 可以將路由器配置為通過Cisco Secure授權exec會話。**aaa authorization exec default tacacs+ none**命令為exec會話建立TACACS+授權。如果應用此項，則會影響使用者時間/時間、**telnet/telnet**、todam/todam、**todpm/todpm**和**somerouters/somerouters**。將此命令新增到路由器並以使用者**時間/時間**Telnet到路由器後，exec會話將保持開啟狀態一分鐘(set timeout = 1)。 使用者**telnet/telnet**會進入路由器，但會立即傳送到另一個位址(set autocmd = "telnet 171.68.118.102")。 **todam/todam**和**todpm/todpm**使用者可能無法訪問路由器，具體取決於測試期間路由器處於什麼時間。使用者**somerouters**只能從網路10.31.1.x通過Telnet連線到路由器koala.rtp.cisco.com。Cisco Secure會嘗試解析路由器的名稱。如果使用IP地址10.31.1.5，則解析未發生時有效；如果使用名稱koala，則解析為通過時有效。

新增記帳

新增記帳是可選操作。

1. 如果路由器運行的Cisco IOS軟體版本高於Cisco IOS軟體版本11.0，則除非在路由器中配置，否則不會進行記帳。您可以在路由器上啟用記帳：

```
aaa accounting exec default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
aaa accounting network default start-stop tacacs+
aaa accounting system default start-stop tacacs+
```

注意：Command-accounting has broken， in Cisco bug ID CSCdi44140，但是如果您使用修復了此問題的映像，也可以啟用命令記帳。

2. 在路由器上新增記帳記錄調試：

```
terminal monitor
debug aaa accounting
```

3. 控制檯上的調試應顯示使用者登入時進入伺服器的記帳記錄。
4. 為了以根使用者身份檢索記帳記錄：

```
CD $BASE/utils/bin
./AcctExport <filename> no_truncate
```

no_truncate表示資料保留在資料庫中。

新增撥號使用者

請完成以下步驟：

1. 在新增撥號使用者之前，請確保Cisco Secure的其他功能正常工作。如果Cisco Secure伺服器和數據機在此點之前無法正常工作，則它們在此點之後無法正常工作。
2. 將此命令新增到路由器配置：

```
aaa authentication ppp default if-needed tacacs+
aaa authentication login default tacacs+ enable
aaa authorization network default tacacs+
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
```

介面組態會有所不同，這取決於驗證的方式，但在本範例中，以下組態會使用撥入線路：

```
interface Ethernet 0
ip address 10.6.1.200 255.255.255.0
! !--- 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 ! !--- 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 ! !--- login 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
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 ! access-list 101 deny icmp any any
```

3. 在Cisco Secure的使用者檔案中：chapuser - CHAP/PPP — 使用者撥入第1行；地址由路由器上的**對等預設ip地址池非同步和ip local pool async 10.6.100.101 10.6.100**.103分配chapaddr - CHAP/PPP — 使用者撥入第1行；地址10.29.1.99由伺服器分配chapacl - CHAP/PPP — 使用者撥入第1行；地址10.29.1.100由伺服器分配，並應用入站訪問清單101（必須在路由器上定義）papuser - PAP/PPP — 使用者撥入第2行；地址由路由器**上的對等預設ip地址池非同步和ip local pool async 10.6.100.101 10.6.100**.103分配papaddr - PAP/PPP — 使用者撥入第2行；地址10.29.1.98由伺服器分配papacl - PAP/PPP — 使用者撥入第2行；地址10.29.1.100由伺服器分配，並且應用入站訪問清單101，該清單必須在路由器上定義loginauto — 使用者撥入第3行；使用autocommand on line的登入身份驗證強制使用者進行PPP連線並從池分配地址
4. 除使用者loginauto之外的所有使用者的Microsoft Windows安裝程式選擇**開始>程式>附件>撥號網路**。選擇**Connections > Make New Connection**。鍵入連線的名稱。輸入數據機特定的資訊。在**Configure > General**中，選擇數據機的最高速度，但不要選中此框下方的框。在**Configure > Connection**中，使用8個資料位、無奇偶校驗和1個停止位。呼叫首選項為**Wait for dial tone before dialing**和**Cancel the call if not connected after 200 seconds**。在高級中，僅選擇**硬體流控制**和**調制型別標準**。在**Configure > Options**中，除狀態控制下外，不檢查任何內容。按一下「**OK**」（確定）。在「下一步」視窗中，輸入目標的電話號碼，然後按一下**下一步**，然後按一下**完成**。顯示新連線圖示後，按一下右鍵該圖示並選擇**屬性**，然後按一下**伺服器型別**。選擇**PPP:WINDOWS 95、WINDOWS NT 3.5、Internet**，並且不檢查任何高級選項。在Allowed network protocols中，至少檢查**TCP/IP**。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「**使用遠端網路上的預設網關**」。按一下「**OK**」（確定）。按兩下圖示以開啟「連線到」視窗以進行撥號時，必須填寫「使用者名稱」和「密碼」欄位，然後按一下**連線**。
5. Microsoft Windows 95 Setup for User loginauto除**Configure > Options**視窗外，使用者loginauto（使用autocommand PPP進行身份驗證的使用者）的配置與其他使用者相同。選中**Bring up terminal window after dialing**。按兩下圖示以開啟「連線到」視窗進行撥號時，不會填寫「使用者名稱」和「密碼」欄位。按一下**Connect**，在連線到路由器後，在顯示的黑色視窗中鍵入使用者名稱和密碼。身份驗證後，按一下**Continue(F7)**。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

伺服器

```
./Cisco Secure -cx -f $BASE/CSU $BASE/config/CSU.cfg
```

路由器

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。有關特定命令的詳細資訊，請參閱Cisco IOS Debug命令參考。

- **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啟動期間傳輸的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。此命令顯示低級別資料包轉儲。
- **debug ppp chap** — 顯示有關實施質詢身份驗證協定(CHAP)的網際網路中的流量和交換的資訊。
- **debug aaa authentication** — 檢視正在使用哪些身份驗證方法，以及這些方法的結果。
- **debug aaa authorization** — 檢視正在使用的授權方法以及這些方法的結果。

思科安全使用者檔案

```
group = admin {
        password = clear "adminpwd"
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

group = oper {
        password = clear "oper"
        privilege = clear "cisco" 15
        service = shell {
                default cmd = permit
                default attribute = permit
        }
}

user = adminusr {
        password = clear "adminusr"
        default service = permit
        }

user = desusr {
        password = des "QjnXYd1kd7ePk"
        default service = permit
        }

user = operator {
        member = oper
        default service = permit
        }

user = time {
        default service = permit
        password = clear "time"
        service = shell  {
                set timeout = 1
```

```
                default cmd = permit
                default attribute = permit
        }
}

user = todam {
        password = clear "todam"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 0600 - 1200
        }
        }

user = todpm {
        password = clear "todpm"
        service = shell  {
                default cmd = permit
                default attribute = permit
                time = Any 1200 - 2359
        }
        }

user = telnet {
        password = clear "telnet"
        service = shell  {
                set autocmd = "telnet 171.68.118.102"
                        }
        }

user = limit_lifetime {
        password = clear "cisco" from
        "2 may 2001" until
        "4 may 2001"
        }

user = loneusr {
        password = clear "lonepwd"
        service = shell  {
                cmd = show {
                permit "ver"
                }
                cmd = ping {
                permit "."
                }
                cmd = logout {
                permit "."
                }
        }
}

user = chapuser {
        default service = permit
        password = chap "chapuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = chapaddr {
        password = chap "chapaddr"
```

```
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.99
                }
        }
}

user = chapacl {
        default service = permit
        password = chap "chapacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = papuser {
        default service = permit
        password = pap "papuser"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                }
        }
}

user = papaddr {
        default service = permit
        password = pap "papaddr"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set addr = 10.29.1.98
                }
        }
}

user = papacl {
        default service = permit
        password = chap "papacl"
        service = ppp {
                protocol = lcp {
                        }
                protocol = ip {
                        set inacl = 101
                        set addr = 10.29.1.100
                }
        }
}

user = loginauto {
        default service = permit
        password = clear "loginauto"
        service = ppp {
                protocol = lcp {
                        }
```

```
                protocol = ip {
                        }
        }
 }

user = somerouters {
   password = clear "somerouters"
   allow koala ".*" "10\.31\.1\.*"
   allow koala.rtp.cisco.com ".*" "10\.31\.1\.*"
   allow 10.31.1.5 ".*" "10\.31\.1\.*"
   refuse ".*" ".*" ".*"
   service=shell {
   default cmd=permit
   default attribute=permit
   }
   }
```

相關資訊

- Cisco Secure ACS for UNIX產品支援
- 安全產品現場通知（包括Cisco Secure UNIX）