安装和调试 CiscoSecure 2.x TACACS+

目录

简介

本文档旨在帮助首次使用Cisco Secure 2.x的用户设置和调试Cisco Secure TACACS+配置。它并非对思科安全功能的详尽描述。

有关服务器软件和用户设置的更完整信息，请参阅您的思科安全文档。有关路由器命令的详细信息，请参阅Cisco IOS软件文档以获取相应版本。

先决条件

要求

本文档中的信息基于以下软件和硬件版本：

- 思科安全ACS 2.x及更高版本
- Cisco IOS®软件版本11.3.3及更高版本

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

设置 Cisco Secure

请完成以下步骤：

1. 确保使用软件附带的说明在UNIX服务器上安装思科安全代码。
2. 要确认产品是否停止和启动，请将cd/etc/rc0.d，并作为root执行./K80Cisco Secure（以停止守护程序）。在/etc/rc2.d输入cd，作为根/S80Cisco Secure（启动守护程序）。启动时，您应看到如下消息：
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   运$BASE/utils/psg以确保每个进程至少运行一个，例如SQLAnywhere或另一个数据库引擎、Cisco Secure数据库服务器进程、Netscape Web Server、Netscape Web Admin、Acme Web Server、Cisco Secure AAA进程或Auto restart进程。
3. 为了确保您位于正确的目录中，请在外壳环境中设置环境变量和路径。此处使用c-shell。**$BASE**是安装Cisco Secure时选择的目录。它包含DOCS、DBServer、CSU等目录。在本例中，假设在/opt/CSCOacs中安装，但在您的系统中这可能有所不同：
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY是安装默认Cisco安全数据库的目录，在安装过程中选择。如果使用了产品附带的缺省数据库SQLAnywhere，则它包含数据库、文档等目录。在本示例中，假设在/opt/CSCOacs/SYBSsa50中安装，但这在您的系统上可能有所不同。
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   在外壳环境中添加路径到：
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD至$BASE/config**CSU.cfg**是Cisco Secure服务器控制文件。创建此文件的备份副本。在此文件中，LIST config_license_key显示您在购买软件时通过许可流程收到的许可证密钥；如果这是4端口试用许可证，则可忽略此线路。NAS config**_nas_config部**分可以包含默认网络接入服务器(NAS)或路由器，或在安装过程中输入的NAS。为了在本示例中进行调试，您可*以允*许任何NAS与Cisco Secure服务器通*信*，而无需密钥。例如，从包含/* NASNAS*/"和*/*NAS/Cisco Secure密钥*/*。该地区*唯*一的条件是：
   ```
   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 = {
   ```
   执行此操作时，您会告诉Cisco Secure，它允许与所有NAS进行对话，而不交换密钥。
5. 如果希望让调试信息转到/var/log/csuslog，则需要在CSU.cfg顶部的一行中显示，该行告知服务器要进行多少调试。0X7FFFFFF添加所有可能的调试。相应地添加或修改此行：
   ```
   NUMBER config_logging_configuration = 0x7FFFFFFF;
   ```
   此附加线路将调试信息发送到local0:
   ```
   NUMBER config_system_logging_level = 0x80;
   ```
   此外，添加此条目以修改/etc/syslog.conf文件：
   ```
   local0.debug /var/log/csuslog
   ```

然后，循环使用syslogd以重新读取：

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

回收Cisco Secure服务器：

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

它仍应该开始。

6. 您可能希望使用浏览器添加用户、组等，或CSimport实用程序。使用CSimport可以轻松地将本文档末尾平面文件中的示例用户移动到数据库中。这些用户将用于测试目的，在您让自己的用户进入后，您可以将其删除。导入后，您可以通过GUI查看导入的用户。如果您决定使用CSimport:

```
CD $BASE/utils
```

将用户和组配置文件放在本文档末尾的文件中，如系统上的任何位置，然后从$BASE/utils目录，运行守护程序，例如/etc/rc2.d/S80Cisco Secure，并作为用户根，使用test(-t)选项运行CSimport:

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

这将测试用户的语法；您应收到如下消息：

```
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...
```

您不应接收如下消息：

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

无论是否存在错误，请检查upgrade.log以确保已签出配置文件。纠正错误后，从$BASE/utils目录，运行守护程序(/etc/rc2.d/S80Cisco Secure)，并以用户根用户身份运行CSimport和commit(-c)选项，将用户移入数据库：

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

同样，屏幕或upgrade.log中不应出现错误。

7. 思科安全兼容性技术提示中列出了支持的浏览器。在PC浏览器中，指向Cisco Secure/Solaris框**http://#.#.#.#/cs**，其**中#.#.#.#**是Cisco Secure/Solaris服务器的IP。在显示的屏幕上，为用户输入超**级用**户，为密码输入**changeme**。此时请勿更改密码。如果在上一步中使用CSimport，或者可以单击浏览块关闭并通过GUI手动添加用户和组，则您应该看到添加的用户/组。

设置认证

注意：此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及更高版本显示了**group tacacs**而不**是tacacs**。

此时，请配置路由器。

1. 在配置路由器时终止Cisco Secure。

```
/etc/rc0.d/K80Cisco Secure to stop the daemons.
```

2. 在路由器上，开始配置TACACS+。进入启用模式，在命前键入conf t。此语法可确保在Cisco Secure未运行时，您不会*被锁*定在路由器之外。输入`ps -ef | grep secure`便检查以确保Cisco Secure未运行，并终止–9进程（如果是）：

```
!--- 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. 测试以确定您仍可在继续下一步前通过 Telnet 和控制台端口访问路由器。由于Cisco Secure未运行，因此应接受使能密码。**注意：**保持控制台端口会话处于活动状态并保持启用模式；此会话不应超时。此时您开始限制对路由器的访问，并且您需要能够在不将自己锁定的情况下更改配置。发出以下命令，以查看路由器上的服务器到路由器的交互：

   ```
   terminal monitor
   debug aaa authentication
   ```

4. 作为根用户，在服务器上启动Cisco Secure:

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

   这将启动进程，但您希望启用比S80Cisco Secure中配置的更多调试，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
   ```

   使用-x项，Cisco Secure在前台运行，因此可以观察路由器到服务器的交互。您不应看到错误消息。由于 — x选项，思科安全流程应启动并挂起。

5. 从另一个窗口，检查以确保Cisco Secure已启动。输入ps -ef并查找思科安全流程。
6. Telnet(vty)用户现在必须通过思科安全进行身份验证。在路由器上执行debug命令后，从网络的另一部分Telnet到路由器。路由器应生成用户名和密码提示。您应该能够使用以下用户ID/密码组合访问路由器：

   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```

   观察您应该在其中看到交互的服务器和路由器，即，在何处发送什么、响应和请求等。在您继续前，请更正所有问题。

7. 如果您还希望用户通过Cisco Secure进行身份验证以进入启用模式，请确保您的控制台端口会话仍处于活动状态并将此命令添加到路由器：

   ```
   !--- 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. 您现在必须通过Cisco Secure启用。在路由器上执行debug命令后，从网络的另一部分Telnet到路由器。当路由器要求输入用户名/口令时，会以操/应。当用户操作员尝试进入启用模式（权限级别15）时，需要密码“cisco”。如果没有权限级别语句（或Cisco安全守护程序关闭），其他用户将无法进入启用模式。观察服务器和路由器，您应该在其中看到思科安全交互，例如，发送内容、响应和请求等。在继续之前，请纠正任何问题。
9. 关闭服务器上的Cisco Secure进程，同时仍连接到控制台端口，以确保在Cisco Secure关闭时，您的用户仍可以访问路由器：

   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```

   重复前面的 Telnet 和启用步骤。路由器应该意识到Cisco Secure进程不响应，允许用户使用默认使能密码登录并启用。

10. 再次启动Cisco Secure服务器，并建立到路由器的Telnet会话，该会话应通过Cisco Secure进行身份验证，并使用用户ID/密码操作**员/操作**，以便通过Cisco Secure检查控制台端口用户的身份验证。保持telnet到路由器并处于启用模式，直到您确定可以通过控制台端口登录路由器，例如，通过控制台端口注销到路由器的原始连接，然后重新连接到控制台端口。使用之前

的用户ID/密码组合登录的控制台端口身份验证现在应通过Cisco Secure。例如，必须使用**userid/password operator/oper**，然**后使**用口令cisco才能启**用**。

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：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

增加授权

添加授权是可选的。

默认情况下，路由器上有三个命令级别：

- 权限级别0 — 包括禁用、启用退出、帮助和注销
- 权限级别1 - Telnet和提示符上的正常`>`
- 权限级别15 — 启用级别并提示`router#`

由于可用命令取决于Cisco IOS功能集、Cisco IOS软件版本、路由器型号等，因此没有1级和15级所有命令的综合列表。例如，**show ipx route**不存在于仅IP功能集中，**show ip nat trans** 不存在于Cisco IOS软件版本10.2中。X代码，因为当时未引入NAT，并且没有电源和温度监控的路由器型号中不存在**show environment**。

在特定级别的特定路由器中可用的命令是输入**?**即可获得。

在实施CSCdi82030之前，控制台端口授权未添加为功能。控制台端口授权默认关闭，以降低意外锁定路由器的可能性。如果用户通过控制台对路由器进行物理访问，则控制台端口授权并不十分有效。但是，在Cisco IOS映像中，**line con 0** 命令可以启用控制台端口授权，在该映像中，CSCdi82030是使用authorization exec default|**WORD命令实**现的。

请完成以下步骤：

1. 路由器可配置为通过Cisco Secure在所有或某些级别授权命令。此路由器配置允许所有用户在服务器上设置每个命令授权。您可以通过Cisco Secure对所有命令进行授权，但如果服务器关闭，则无需授权，因此无。当Cisco Secure服务器关闭时，输入以下命令：输入以下命令，以取消通过Cisco Secure执行启用身份验证的要求：
   ```
   no aaa authentication enable default tacacs+ none
   ```
   输入以下命令以要求通过Cisco Secure执行命令授权：
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. 当Cisco Secure服务器运行时，使用用户ID/密码loneusr/lonepwd通过Telnet连**接到路由器**。此用户除以下命令外，不能执行任何命令：
   ```
   show version
   ping <anything>
   logout
   ```
   以前的用户**adminusr/adminusr**、**operator/oper**、**desusr/encrypt**仍应能够通过其默认服务`=permit`执行所有命令。如果该过程有问题，请在路由器上进入启用模式，然后使用以下命令打开授权调试：
   ```
   terminal monitor
   debug aaa authorization
   ```

观察服务器和路由器，您应该在其中看到思科安全交互，例如，发送内容的位置、响应和请求等。在您继续前，请更正所有问题。

3. 路由器可配置为通过Cisco Secure授权执行会话。aaa authorization **exec default tacacs+ none命令**为执行会话启用TACACS+授权。如果应用此选项，它会影响用户的时间/时间、**telnet/telnet**、todam/todam、todpm/todpm和**somerouters/somerouters**。将此命令添加到路由器并以用户时间/时间形式Telnet到路由器后，**执行会话将保持打开一分钟**(set timeout = 1)。用户**telnet/telnet**进入路由器，但会立即发送到另一个地址(set autocmd = "telnet 171.68.118.102")。 用户todam/todam和**todpm/todpm**可能**是否能够访问路由器，这取决于测试期间路由器的时间。**用户**somerouters** 只能从网络10.31.1.x通过Telnet连接到路由器koala.rtp.cisco.com。Cisco Secure尝试解析路由器的名称。如果使用IP地址10.31.1.5，则解析无效；如果使用名称koala，则解析通过有效。

增加记账功能

添加记帐是可选的。

1. 如果路由器运行的Cisco IOS软件版本高于Cisco IOS软件版本11.0，则除非在路由器中进行配置，否则不会进行记帐。您可以在路由器上启用记帐：
```
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：在Cisco Bug ID CSCdi44140中，命令记帐已断开，但如果使用的映像中已修复，则命令记帐也可以启用。
2. 在路由器上添加记帐记录调试：
```
terminal monitor
debug aaa accounting
```
3. 控制台上的调试应显示在用户登录时输入服务器的记帐记录。
4. 要检索记帐记录，请以root身份：
```
CD $BASE/utils/bin
./AcctExport <filename> no_truncate
```
no_truncate表示数据保留在数据库中。

添加拨号用户

请完成以下步骤：

1. 在添加拨号用户之前，请确保Cisco Secure的其他功能正常工作。如果Cisco Secure服务器和调制解调器在此之前不工作，则在此之后它们不工作。
2. 将此命令添加到路由器配置：
```
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
```
接口配置不同，具体取决于身份验证的完成方式，但本例中使用拨入线路，其配置如下：
```
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. 从思科安全的用户文件：chapuser - CHAP/PPP — 用户在第1行拨号；地址由对等**默认ip address pool async和ip local pool async 10.6.100.101 10.6.100.103在路由器上**分配chapaddr - CHAP/PPP — 用户在第1行拨号；地址10.29.1.99由服务器分配chapacl - CHAP/PPP — 第1行中的用户拨号；地址10.29.1.100由服务器分配，并应用入站访问列表101（必须在路由器上定义）papuser - PAP/PPP — 用户在第2行拨号；地址由路由器**上的对等默认ip地址池异步和ip local pool async 10.6.100.101 10.6.100.103**分配papaddr - PAP/PPP — 用户在第2行拨号；地址10.29.1.98由服务器分配papacl - PAP/PPP — 用户在第2行拨号；地址10.29.1.100由服务器分配，入站访问列表101应用，必须在路由器上定义loginauto — 用户在第3行拨号；使用autocommand online的登录身份验证强制用户进行PPP连接并从池分配地址
4. 除用户登录自动外，所有用户的Microsoft Windows设置选择**开始>程序>附件>拨号网络**。选择**连接>新建连接**。键入连接的名称。输入调制解调器特定信息。在**Configure > General**中，选择调制解调器的最高速度，但不要选中下方的复选框。在**配置>连接**中，使用8个数据位、无奇偶校验和1个停止位。呼叫首选项**为"在拨号前等待拨号音"**和**"如果200秒后未连接则取消呼叫"**。在"高级"中，仅选**择硬件流控**制和调**制类型标准**。在**Configure > Options**中，除状态控制下外，不应检查任何内容。Click **OK**.在"Next（下一步）"窗口中，输入目标的电话号码，然后单击"Next（下一步）",**然后单击"Finish(完成)**"。出现新连接图标后，右键单击该图标并选择"属性"，**然后单击**"服务器类**型"**。选**择PPP:WINDOWS 95、WINDOWS NT 3.5、Internet，**不选中任何高级选项。在允许的网络协议中，至少检**查TCP/IP**。在"TCP/IP设置"下，选择**服务器分配的IP地址、服务器分配的名称服务器地址**和**使用远程网络上的默认网关**。Click **OK**.双击图标以打开"连接到"窗口进行拨号时，必须填写"用户名"和"密码"字段，然后单击"连**接"**。
5. Microsoft Windows 95用户登录自动设置除在"配置"(Configure)>"选项"(Options)窗口中外，用户登录自动（使用autocommand PPP的身份验证用户）的配置与其**他用户的配置**相同。选中**拨号后打开终端窗口**。双击图标以打开要拨号的"连接到"窗口时，不填写"用户名"和"密码"字段。单击**Connect**，在与路由器建立连接后，在显示的黑色窗口中键入用户名和密码。身份验证后，单**击继续(F7)**。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

服务器

```
./ — cx -f $BASE/CSU $BASE/config/CSU.cfg
```

路由器

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。有关特定命令的详细信息，请参阅Cisco IOS调试命令参考。

- **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启动期间传输的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。此指令显示低级数据包。
- **debug ppp chap** — 显示实施质询身份验证协议(CHAP)的网际网络中有关流量和交换的信息。
- **debug aaa authentication** — 查看正在使用哪些身份验证方法以及这些方法的结果。
- **debug aaa authorization** — 查看正在使用的授权方法以及这些方法的结果。

Cisco Secure Users 文件

```
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
}
}
```

相关信息

- Cisco Secure ACS for UNIX产品支持
- 安全产品现场通知（包括Cisco Secure UNIX）