Configuración y depuración de CiscoSecure 2.x TACACS+

Contenido

Introducción

Este documento tiene como objetivo ayudar al usuario Cisco Secure 2.x por primera vez en la configuración y depuración de una configuración de Cisco Secure TACACS+. No se trata de una descripción exhaustiva de las funciones de Cisco Secure.

Consulte la documentación de Cisco Secure para obtener información más completa sobre el software del servidor y la configuración del usuario. Consulte la documentación del software del IOS de Cisco para la versión apropiada para obtener más información sobre los comandos del router.

Prerequisites

Requirements

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure ACS 2.x y posterior
- Cisco IOS® Software Release 11.3.3 y posteriores

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configuración de Cisco Secure

Complete estos pasos:

1. Asegúrese de utilizar las instrucciones incluidas con el software para instalar el código de Cisco Secure en el servidor UNIX.
2. Para confirmar que el producto se detiene y comienza, ingrese `cd a /etc/rc0.d` y como root, ejecute `./K80Cisco Secure` (para detener los demonios).Ingrese `cd a /etc/rc2.d` y como root, ejecute `./S80Cisco Secure` (para iniciar los demonios).Al iniciar, debería ver mensajes como:
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   Ejecute `$BASE/utils/psg` para asegurarse de que al menos uno de cada uno de los procesos individuales se ejecuta, por ejemplo, SQLAnywhere u otro motor de base de datos, proceso del servidor de base de datos Cisco Secure, Servidor Web Netscape, Administrador Web Netscape, Servidor Web Acme, Proceso AAA Cisco Secure o Proceso de reinicio automático.
3. Para asegurarse de que se encuentra en los directorios adecuados, configure variables ambientales y rutas en su entorno de shell. c-shell se utiliza aquí.**$BASE** es el directorio donde se instala Cisco Secure, elegido durante la instalación. Contiene directorios como DOCS, DBServer, CSU, etc.En este ejemplo, se asume la instalación en /opt/CSCOacs, pero esto puede diferir en su sistema:
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY es el directorio donde se instala la base de datos predeterminada de Cisco Secure, seleccionada durante la instalación. Si se utilizó la base de datos predeterminada que viene con el producto, SQLAnywhere, contiene directorios como base de datos, doc, etc.En este ejemplo, se asume la instalación en /opt/CSCOacs/SYBSsa50, pero esto puede diferir en su sistema.
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   Agregue rutas en su entorno de shell a:
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD a $BASE/config**CSU.cfg** es el archivo de control de servidor de Cisco Secure. Haga una copia de seguridad de este archivo.En este archivo, `LIST config_license_key` muestra la clave de licencia que recibió a través del proceso de licencia si adquirió el software; si se trata de una licencia de prueba de 4 puertos, puede dejar fuera de esta línea.La sección **NAS config_nas_config** puede contener un servidor de acceso a la red (NAS) o router predeterminado, o el NAS que ingresó durante la instalación. Para fines de depuración en este ejemplo, puede permitir que *cualquier* NAS se comunique con el servidor Cisco Secure *sin* una clave. Por ejemplo, quite el nombre del NAS y la clave de las líneas que contienen `/* el nombre NAS puede ir aquí */`" y */*NAS/clave secreta segura de Cisco */*. La única *plaza* en esa zona dice:

```
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 = {
```

Cuando lo haga, le dirá a Cisco Secure que se le permite hablar con todos los NAS sin intercambio de claves.

5. Si desea que la información de depuración vaya a /var/log/csuslog, debe tener una línea en la sección superior de CSU.cfg, que indica al servidor cuánta depuración debe realizar. 0X7FFFFFFF agrega toda la depuración posible. Agregue o modifique esta línea en consecuencia:

   ```
   NUMBER config_logging_configuration = 0x7FFFFFFF;
   ```

   Esta línea adicional envía la información de depuración a local0:

   ```
   NUMBER config_system_logging_level = 0x80;
   ```

   Además, agregue esta entrada para modificar el archivo /etc/syslog.conf:

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

   Luego recicle el syslogd para volver a leer:

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

   Reciclaje del servidor Cisco Secure:

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

   Todavía debería empezar.

6. Puede utilizar el explorador para agregar usuarios, grupos, etc., o la utilidad CSimport. Los usuarios de ejemplo del archivo plano al final de este documento pueden moverse fácilmente a la base de datos mediante CSimport. Estos usuarios trabajarán con fines de prueba y podrá eliminarlos una vez que haya accedido a sus propios usuarios. Una vez importados, puede ver los usuarios importados a través de la GUI.Si decide utilizar CSimport:

   ```
   CD $BASE/utils
   ```

   Coloque los perfiles de usuario y de grupo al final de este documento en un archivo como en cualquier lugar del sistema, luego desde el directorio $BASE/utils, con los demonios ejecutándose, por ejemplo, /etc/rc2.d/S80Cisco Secure, y como raíz de usuario, ejecute CSimport con la opción test (-t):

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

   Esto prueba la sintaxis para los usuarios; debería recibir mensajes como:

   ```
   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...
   ```

   No debe recibir mensajes como:

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

   Si hubo errores o no, examine upgrade.log para asegurarse de que los perfiles estén desprotegidos. Una vez corregidos los errores, desde el directorio $BASE/utils, con los demonios en ejecución (/etc/rc2.d/S80Cisco Secure) y como usuario root, ejecute CSimport

con la opción commit (-c) para mover los usuarios a la base de datos:
`./CSimport -c -p <path_to_file> -s <name_of_file>`
De nuevo, no debe haber errores en la pantalla o en upgrade.log.

7. Los navegadores admitidos se enumeran en la sugerencia técnica Cisco Secure Compatibility. Desde el navegador de su PC, apunte al cuadro Cisco Secure/Solaris **http://#.#.#.#/cs** donde **#.#.#.#** es la IP del servidor Cisco Secure/Solaris.En la pantalla que aparece, para el usuario ingrese **superuser** y para la contraseña, ingrese **changeme**. No cambie la contraseña en este momento. Debería ver los usuarios/grupos agregados si utiliza CSimport en el paso anterior o puede hacer clic en el bloque de exploración **desactivado** y agregar manualmente usuarios y grupos a través de la GUI.

Configuración de la autenticación

Nota: Esta configuración del router se desarrolló en un router que ejecuta Cisco IOS Software Release 11.3.3. Cisco IOS Software Release 12.0.5.T y posteriores muestran **tacacs de grupo** en lugar de **tacacs**.

En este momento, configure el router.

1. Mate Cisco Secure mientras configura el router.
   `/etc/rc0.d/K80Cisco Secure to stop the daemons.`
2. En el router, comience a configurar TACACS+. Ingrese enable mode y escriba `conf t` antes del comando set. Esta sintaxis garantiza que no esté bloqueado del router *inicialmente* siempre que Cisco Secure no se esté ejecutando. Introduzca `ps -ef | grep Secure` para asegurarse de que Cisco Secure no se esté ejecutando y finalizar -9 el proceso si es:

   ```
   !--- 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. Asegúrese de que aún puede acceder al router con Telnet y a través del puerto de la consola antes de continuar. Dado que Cisco Secure no se está ejecutando, se debe aceptar la contraseña de activación.**Precaución:** Mantenga activa la sesión del puerto de la consola y manténgase en modo de activación; esta sesión no debería agotarse. En este momento, comienza a limitar el acceso al router y debe poder realizar cambios en la configuración sin bloquearse.Ejecute estos comandos para ver la interacción servidor a router en el router:
   ```
   terminal monitor
   debug aaa authentication
   ```
4. Como raíz, inicie Cisco Secure en el servidor:
   `/etc/rc2.d/S80Cisco Secure`
   Esto inicia los procesos, pero desea habilitar más depuración de la configurada en S80Cisco Secure, de modo que:
   ```
   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
```

Con la opción `-x`, Cisco Secure se ejecuta en primer plano para que se pueda observar la interacción entre el router y el servidor. No debe ver mensajes de error. El proceso Cisco Secure debe iniciarse y colgarse allí debido a la opción -x.

5. En otra ventana, asegúrese de que Cisco Secure se ha iniciado. Introduzca `ps -ef` y busque el proceso Cisco Secure.
6. Los usuarios de Telnet (vty) ahora deben autenticarse a través de Cisco Secure. Con la depuración en el router, conecte Telnet al router desde otra parte de la red. El router debe producir un mensaje de nombre de usuario y contraseña. Debe poder acceder al router con estas combinaciones de ID de usuario/contraseña:

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

   Vea el servidor y el router donde debe ver la interacción, es decir, qué se envía donde, respuestas y solicitudes, etc. Corrija cualquier problema antes de continuar.
7. Si también desea que los usuarios se autentiquen a través de Cisco Secure para entrar en el modo de activación, asegúrese de que la sesión del puerto de la consola sigue activa y agregue este comando al router:

   ```
   !--- 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. Ahora debe tener que **habilitar** a través de Cisco Secure. Con la depuración en el router, conecte Telnet al router desde otra parte de la red. Cuando el router solicita el nombre de usuario/contraseña, responda con `operador/oper`.Cuando el operador de usuario intenta ingresar en el modo enable (nivel de privilegio 15), se requiere la contraseña "cisco". Otros usuarios no podrán entrar en el modo de habilitación sin la instrucción de nivel de privilegio (o Cisco Secure daemon down).Vea el servidor y el router donde debería ver la interacción de Cisco Secure, por ejemplo, qué se envía donde, respuestas y solicitudes, etc. Corrija cualquier problema antes de continuar.
9. Apague el proceso Cisco Secure en el servidor mientras aún está conectado al puerto de la consola para asegurarse de que los usuarios puedan acceder al router si Cisco Secure no funciona:

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

   Repita Telnet y active el paso anterior. El router debe darse cuenta de que el proceso de Cisco Secure no responde y permitir a los usuarios iniciar sesión y activarse con las contraseñas de activación predeterminadas.
10. Vuelva a activar el servidor Cisco Secure y establezca una sesión Telnet al router, que debe autenticarse a través de Cisco Secure, con userid/password **operador/oper** para verificar la autenticación de los usuarios del puerto de consola a través de Cisco Secure. Permanezca conectado a la red telefónica en el router y en el modo de activación hasta que esté seguro de que puede iniciar sesión en el router a través del puerto de la consola, por ejemplo, desconecte la conexión original al router a través del puerto de la consola y luego vuelva a conectarse al puerto de la consola. La autenticación del puerto de la consola para iniciar sesión con el uso de las combinaciones de ID de usuario/contraseña anteriores debe realizarse ahora a través de Cisco Secure. Por ejemplo, userid/password **operator/oper** luego **cisco** debe utilizarse para **habilitar**.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Agregado de autorización

Agregar autorización es opcional.

De forma predeterminada, hay tres niveles de comando en el router:

- Nivel de privilegio 0: que incluye inhabilitar, habilitar la salida, ayudar y cerrar la sesión
- Nivel de privilegio 1: nivel normal en Telnet y el mensaje indica `router>`
- Nivel de privilegio 15: el nivel de activación y el mensaje indican `router#`

Dado que los comandos disponibles dependen del conjunto de funciones de Cisco IOS, de la versión de software de Cisco IOS, del modelo de router, etc., no hay una lista completa de todos los comandos en los niveles 1 y 15. Por ejemplo, **show ipx route** no está presente en un conjunto de funciones sólo IP, **show ip nat trans** no está en el código de Cisco IOS Software Release 10.2.X porque NAT no se introdujo en ese momento, y **show environment** no está presente en los modelos de router sin fuente de alimentación y monitoreo de temperatura.

¿Se pueden encontrar comandos disponibles en un router determinado a un nivel determinado ingresando un comando **?** en el mensaje del router cuando se encuentra en ese nivel de privilegio.

La autorización del puerto de consola no se agregó como una función hasta que se implementó CSCdi82030. La autorización del puerto de consola está desactivada de forma predeterminada para reducir la probabilidad de que se bloquee accidentalmente el router. Si un usuario tiene acceso físico al router a través de la consola, la autorización del puerto de consola no es extremadamente efectiva. Pero, la autorización de puerto de consola se puede activar bajo el comando **line con 0** en una imagen de Cisco IOS en la que se implementó CSCdi82030 con el comando **authorization exec default|WORD**.

Complete estos pasos:

1. El router se puede configurar para autorizar comandos a través de Cisco Secure en todos o algunos niveles. Esta configuración del router permite que todos los usuarios tengan configurada la autorización por comando en el servidor. Puede autorizar todos los comandos a través de Cisco Secure pero si el servidor está inactivo, no es necesaria ninguna autorización, de ahí la `ausencia`.Con el servidor Cisco Secure inactivo, ingrese estos comandos:Ingrese este comando para eliminar el requisito de habilitar la autenticación a través de Cisco Secure:
   ```
   no aaa authentication enable default tacacs+ none
   ```
   Ingrese estos comandos para requerir que la autorización de los comandos se realice a través de Cisco Secure:
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. Mientras el servidor Cisco Secure se ejecuta, Telnet ingresa al router con userid/password **loneusr/lonepwd**. Este usuario no debe ser capaz de realizar ningún comando que no sea:
   ```
   show version
   ```

```
ping <anything>
logout
```

Los usuarios anteriores, **administrador/administrador**, **operador/oper**, **desusr/encrypt**, deben poder hacer todos los comandos en virtud de su **servicio predeterminado = permit**. Si hay problemas con el proceso, ingrese enable mode en el router y active la depuración de autorización con este comando:

```
terminal monitor
debug aaa authorization
```

Vea el servidor y el router donde debería ver la interacción de Cisco Secure, por ejemplo, qué se envía donde, respuestas y solicitudes, etc. Corrija cualquier problema antes de continuar.

3. El router se puede configurar para autorizar sesiones exec a través de Cisco Secure. El comando **aaa authorization exec default tacacs+ none** instituye la autorización TACACS+ para las sesiones exec.Si aplica esto, afecta a los usuarios tiempo/hora, **telnet/telnet**, **todam/todam**, **todpm/todpm** y **somerouters/somerouters**. Después de agregar este comando al router y a Telnet al router como **tiempo/hora** de usuario, una sesión exec permanece abierta durante un minuto (set timeout = 1). El usuario **telnet/telnet** ingresa al router pero se envía inmediatamente a la otra dirección (set autocmd = "telnet 171.68.118.102"). Es posible que los usuarios **todam/todam** y **todpm/todpm** puedan o no acceder al router, lo que depende de la hora del día que sea durante las pruebas. Los **somerouters** de usuario sólo pueden conectarse mediante Telnet al router koala.rtp.cisco.com desde la red 10.31.1.x. Cisco Secure intenta resolver el nombre del router. Si utiliza la dirección IP 10.31.1.5, es válida si la resolución no tiene lugar y si utiliza el nombre koala, es válida si la resolución ha terminado.

Incorporación de contabilidad

Agregar contabilidad es opcional.

1. La contabilidad no se realiza a menos que esté configurada en el router, si el router ejecuta la versión de software del IOS de Cisco posterior a la versión 11.0 del software del IOS de Cisco. Puede habilitar la contabilización en el router:

```
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+
```

Nota: La contabilidad de comandos se ha roto, en el ID de bug Cisco CSCdi44140, pero si utiliza una imagen en la que se ha corregido, también se puede habilitar la contabilidad de comandos.

2. Agregar depuración de registro de contabilización en el router:

```
terminal monitor
debug aaa accounting
```

3. La depuración en la consola debe mostrar los registros de contabilización que ingresan al servidor a medida que los usuarios inician sesión.
4. Para recuperar registros de contabilidad, como root:

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

`no_truncate` significa que los datos se conservan en la base de datos.

Incorporación de usuarios de marcación manual

Complete estos pasos:

1. Asegúrese de que las otras funciones de Cisco Secure funcionan antes de agregar usuarios de acceso telefónico. Si el servidor Cisco Secure y el módem no funcionaron antes de este momento, no funcionarán después de este punto.
2. Agregue este comando a la configuración del router:
   ```
   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
   ```
   Las configuraciones de la interfaz difieren, lo que depende de cómo se realice la autenticación, pero las líneas de marcado se utilizan en este ejemplo, con estas configuraciones:
   ```
   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. Desde el archivo de usuario de Cisco Secure:chapuser—CHAP/PPP—el usuario marca en la línea 1; dirección es asignada por **peer default ip address pool async e ip local pool async 10.6.100.101 10.6.100.103** en el routerchapaddr—CHAP/PPP—el usuario marca en la línea 1; la dirección 10.29.1.99 es asignada por el servidorchapacl—CHAP/PPP—el usuario marca en la línea 1; el servidor asigna la dirección 10.29.1.100 y se aplica la lista de acceso entrante 101 (que se debe definir en el router)papuser—PAP/PPP— el usuario marca en la línea 2; dirección es asignada por **peer default ip address pool async e ip local pool async 10.6.100.101 10.6.100.103** en el routerpapaddr—PAP/PPP—el usuario marca en la línea 2; la dirección 10.29.1.98 es asignada por el servidorpapacl—PAP/PPP—el usuario marca en la línea 2; el servidor asigna la dirección 10.29.1.100 y se aplica la lista de acceso entrante 101, que se debe definir en el routerloginauto: el usuario marca en la línea 3; la autenticación de inicio de sesión con el comando automático en la línea fuerza al usuario a la conexión PPP y asigna la dirección del conjunto
4. Configuración de Microsoft Windows para todos los usuarios excepto usuario loginautoElija **Inicio > Programas > Accesorios > Dial-Up Networking**.Elija **Conexiones > Crear nueva conexión**. Escriba un nombre para la conexión.Introduzca la información específica del módem. En **Configure > General**, elija la velocidad más alta del módem, pero no marque la casilla debajo de esta.En **Configure > Connection**, utilice 8 bits de datos, sin paridad y 1 bit de parada. Las preferencias de llamada son **Esperar el tono de marcado antes de marcar** y **Cancelar la llamada si no está conectada después de 200 segundos**.En Advanced, elija solamente **Hardware Flow Control** y **Modulation Type Standard**.En **Configurar > Opciones**, no se debe marcar nada excepto bajo el control de estado. Click OK.En la ventana Next (Siguiente), introduzca el número de teléfono del destino, haga clic en **Next** y, a

continuación, haga clic en **Finish**.Una vez que aparezca el nuevo icono de conexión, haga clic con el botón derecho del ratón en él y elija **Properties** y, a continuación, haga clic en **Server Type**.Elija **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** y no verifique ninguna opción avanzada.En los protocolos de red permitidos, verifique al menos **TCP/IP**.En TCP/IP settings, elija **Server assigned IP address**, **Server assigned name server address** y **Use default gateway on remote network**. Click OK.Al hacer doble clic en el icono para abrir la ventana Conectar a para marcar, debe rellenar los campos Nombre de usuario y Contraseña y, a continuación, hacer clic en **Conectar**.

5. Configuración de Microsoft Windows 95 para el inicio de sesión del usuario automáticoLa configuración para el usuario loginauto, el usuario de autenticación con autocommand PPP, es la misma que para otros usuarios excepto en la ventana **Configurar > Opciones**. Marque la **ventana de activación de terminal después de marcar**.Cuando hace doble clic en el icono para abrir la ventana Conectar a para marcar, no rellena los campos Nombre de usuario y Contraseña. Haga clic en **Connect** y después de que se realice la conexión al router, escriba el nombre de usuario y la contraseña en la ventana negra que aparece.Después de la autenticación, haga clic en **Continue(F7)**.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Servidor

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

Router

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**. Para obtener más información sobre comandos específicos, vea Referencia de Comandos Debug de Cisco IOS.

- **terminal monitor**: muestra el resultado del comando **debug** y los mensajes de error del sistema para el terminal y la sesión actuales.
- **debug ppp negotiation**: muestra los paquetes PPP transmitidos durante el inicio PPP, donde se negocian las opciones PPP.
- **debug ppp packet**: muestra los paquetes PPP que se envían y reciben. Este comando indica el vaciado de paquetes de bajo nivel.
- **debug ppp chap**: muestra información sobre tráfico e intercambios en una red que implementa el protocolo de autenticación por desafío mutuo (CHAP).

- **debug aaa authentication** —Vea qué métodos de autenticación se utilizan y cuáles son los resultados de estos métodos.
- **debug aaa authorization**: vea qué métodos de autorización se están utilizando y cuáles son los resultados de estos métodos.

Archivo seguro de usuarios de Cisco

```
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
   }
   }
```

Información Relacionada

- Soporte de Productos Cisco Secure ACS para UNIX
- Avisos de campo de productos de seguridad (incluido Cisco Secure UNIX)