Einrichten und Debuggen von CiscoSecure 2.x TACACS+

Inhalt

Einführung

Dieses Dokument soll den erstmaligen Benutzer von Cisco Secure 2.x beim Einrichten und Debuggen einer Cisco Secure TACACS+-Konfiguration unterstützen. Es handelt sich hierbei nicht um eine umfassende Beschreibung der Cisco Secure-Funktionen.

Weitere vollständige Informationen zur Serversoftware und zum Einrichten der Benutzer finden Sie in der Cisco Secure-Dokumentation. Weitere Informationen zu Routerbefehlen finden Sie in der Cisco IOS Software-Dokumentation für die entsprechende Version.

Voraussetzungen

Anforderungen

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS 2.x oder höher
- Cisco IOS® Softwareversion 11.3.3 und höher

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Einrichten von Cisco Secure

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie die mit der Software gelieferten Anweisungen verwenden, um den Cisco Secure Code auf dem UNIX-Server zu installieren.
2. Um zu bestätigen, dass das Produkt anhält und startet, geben Sie `cd zu /etc/rc0.d ein` und als root `ein`, führen Sie `./K80Cisco Secure` (um die Daemons zu stoppen) aus.Geben Sie `cd zu /etc/rc2.d ein`, und als root führen Sie `./S80Cisco Secure` (zum Starten der Daemons) aus.Beim Start sollten folgende Meldungen angezeigt werden:
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   Führen Sie `$BASE/utils/psg aus`, um sicherzustellen, dass mindestens einer der einzelnen Prozesse ausgeführt wird, z. B. SQLAnywhere oder eine andere Datenbankengine, der Cisco Secure Database Server-Prozess, Netscape Web Server, Netscape Web Admin, Acme Web Server, Cisco Secure AAA-Prozess oder Auto Restart Process.
3. Um sicherzustellen, dass Sie sich in den richtigen Verzeichnissen befinden, richten Sie Umgebungsvariablen und Pfade in Ihrer Shell-Umgebung ein. c-shell wird hier verwendet.**$BASE** ist das Verzeichnis, in dem Cisco Secure installiert wird. Die Auswahl erfolgt während der Installation. Es enthält Verzeichnisse wie DOCS, DBServer, CSU usw.In diesem Beispiel wird von einer Installation in /opt/CSCOacs ausgegangen, die sich jedoch auf Ihrem System unterscheiden kann:
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY ist das Verzeichnis, in dem die Cisco Secure-Standarddatenbank installiert wird, die während der Installation ausgewählt wird. Wenn die mit dem Produkt gelieferte Standarddatenbank SQLAnywhere verwendet wurde, enthält sie Verzeichnisse wie Datenbanken, Dokumente usw.In diesem Beispiel wird von einer Installation in /opt/CSCOacs/SYBSsa50 ausgegangen, diese kann sich jedoch auf Ihrem System unterscheiden.
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   Fügen Sie Pfade in der Shell-Umgebung hinzu, um:
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD zu $BASE/Konfiguration**CSU.cfg** ist die Cisco Secure Server Control-Datei. Erstellen Sie eine Sicherungskopie dieser Datei.In dieser Datei zeigt `LIST config_license_key` den Lizenzschlüssel an, den Sie beim Erwerb der Software über den Lizenzprozess erhalten haben. Wenn es sich um eine 4-Port-Testlizenz handelt, können Sie diese Zeile weglassen.Der Abschnitt **NAS config_nas_config** kann einen Standard-Netzwerkzugriffsserver (NAS) oder einen Router oder das NAS enthalten, das Sie während der Installation eingeben. Zu Debugzwecken in diesem Beispiel können Sie *jedem* NAS-Gerät die Kommunikation mit dem Cisco Secure-Server *ohne* Schlüssel ermöglichen.

Entfernen Sie z. B. den Namen des NAS und den Schlüssel aus den Posten, die den `/* NAS-Namen` enthalten, `hier */`" und */*NAS/Cisco Secure geheim Key */*. Die einzige *Stanza* in diesem Bereich lautet:

```
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 = {
```

Wenn Sie dies tun, teilen Sie Cisco Secure mit, dass die Kommunikation mit allen NASs ohne Austausch von Schlüsseln zulässig ist.

5. Wenn Sie Debuginformationen wünschen, gehen Sie zu /var/log/csuslog, müssen Sie eine Zeile im oberen Abschnitt von CSU.cfg haben, die dem Server mitteilt, wie viel Debugging ausgeführt werden soll. 0X7FFFFFFF fügt alle möglichen Debugging hinzu. Fügen Sie diesen Posten hinzu oder ändern Sie ihn entsprechend:

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

   Diese zusätzliche Zeile sendet Debuginformationen an local0:

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

   Fügen Sie diesen Eintrag auch hinzu, um die Datei /etc/syslog.conf zu ändern:

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

   Recyclen Sie anschließend das Systemprotokoll, um es erneut zu lesen:

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

   Recyclen Sie den Cisco Secure Server:

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

   Es sollte immer noch beginnen.

6. Sie können den Browser verwenden, um Benutzer, Gruppen usw. hinzuzufügen, oder das CSimport-Dienstprogramm. Die Beispielbenutzer in der flachen Datei am Ende dieses Dokuments können mithilfe von CSimport problemlos in die Datenbank verschoben werden. Diese Benutzer arbeiten zu Testzwecken und Sie können sie löschen, sobald Sie Ihre eigenen Benutzer hinzubekommen. Nach dem Import können Sie die importierten Benutzer über die Benutzeroberfläche anzeigen.Wenn Sie CSimport verwenden möchten:

   ```
   CD $BASE/utils
   ```

   Fügen Sie die Benutzer- und Gruppenprofile am Ende dieses Dokuments in eine Datei ein, z. B. an einer beliebigen Stelle im System, dann aus dem $BASE/utils-Verzeichnis, wobei die Daemons z. B. /etc/rc2.d/S80Cisco Secure laufen, und führen Sie als Benutzerstamm CSimport mit der Testoption (-t) aus:

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

   Diese testet die Syntax für die Benutzer. erhalten Sie beispielsweise folgende Nachrichten:

   ```
   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...
   ```

   Sie sollten *keine* Nachrichten empfangen, z. B.:

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

Unabhängig davon, ob Fehler aufgetreten sind, überprüfen Sie die Datei upgrade.log, um sicherzustellen, dass Profile ausgecheckt wurden. Nach der Korrektur von Fehlern aus dem $BASE/utils-Verzeichnis mit den ausgeführten Daemons (/etc/rc2.d/S80Cisco Secure) und als Benutzer-Root führen Sie CSimport mit der Commit-c-Option aus, um die Benutzer in die Datenbank zu verschieben:
`./CSimport -c -p <path_to_file> -s <name_of_file>`
Auch hier sollte es keine Fehler auf dem Bildschirm oder in der upgrade.log geben.

7. Die unterstützten Browser sind im technischen Tipp zu Cisco Secure Compatibility aufgeführt. Zeigen Sie im PC-Browser auf das Feld Cisco Secure/Solaris **http://#.#.#.#/cs**, wobei **#.#.#.#.#** die IP des Cisco Secure/Solaris-Servers ist.Geben Sie auf dem angezeigten Bildschirm für den Benutzer **Superuser** und für das Kennwort **change** ein. Ändern Sie das Kennwort zu diesem Zeitpunkt nicht. Sie sollten die hinzugefügten Benutzer/Gruppen sehen, wenn Sie CSimport im vorherigen Schritt verwenden, oder Sie können auf den Browser-Block **deaktivieren** und Benutzer und Gruppen manuell über die Benutzeroberfläche hinzufügen.

Einrichten der Authentifizierung

Hinweis: Diese Router-Konfiguration wurde auf einem Router entwickelt, auf dem die Cisco IOS Software, Version 11.3.3, ausgeführt wird. In der Cisco IOS Software-Version 12.0.5.T und höher werden **Gruppentaktiken** anstelle von **Takaks** angezeigt.

Konfigurieren Sie an diesem Punkt den Router.

1. Kill Cisco Secure when you configure the router.
`/etc/rc0.d/K80Cisco Secure to stop the daemons.`
2. Konfigurieren Sie auf dem Router TACACS+. Wechseln Sie in den Aktivierungsmodus, und geben Sie `conf t` vor dem Befehlssatz ein. Diese Syntax stellt sicher, dass Sie nicht vom Router ausgeschlossen sind, *wenn* Cisco Secure nicht ausgeführt wird. Geben Sie `ps-ef ein | grep Secure`, um sicherzustellen, dass Cisco Secure nicht ausgeführt wird, und -9 den Prozess zu beenden, wenn er:

```
!--- 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. Stellen Sie sicher, dass Sie weiterhin über Telnet und den Konsolenport auf den Router zugreifen können, bevor Sie fortfahren. Da Cisco Secure nicht ausgeführt wird, sollte das enable-Kennwort akzeptiert werden.**Vorsicht:** Lassen Sie die Konsolenport-Sitzung aktiv, und bleiben Sie im Aktivierungsmodus. Diese Sitzung sollte nicht abgebrochen werden. Sie beginnen, den Zugriff auf den Router zu beschränken, und Sie müssen in der Lage sein, Konfigurationsänderungen vorzunehmen, ohne sich selbst zu sperren.Führen Sie die folgenden Befehle aus, um die Interaktion zwischen Server und Router am Router anzuzeigen:

```
terminal monitor
debug aaa authentication
```

4. Starten Sie als root Cisco Secure auf dem Server:
   ```
   /etc/rc2.d/S80Cisco Secure
   ```
   Dadurch werden die Prozesse gestartet, Sie möchten jedoch mehr Debugging aktivieren, als in S80Cisco Secure konfiguriert ist. Dies bedeutet:
   ```
   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
   ```
   Bei `-x` Option wird Cisco Secure im Vordergrund ausgeführt, sodass eine Interaktion zwischen Router und Server möglich ist. Fehlermeldungen sollten nicht angezeigt werden. Der Cisco Secure-Prozess sollte dort beginnen und hängen, da die Option -x aktiviert ist.
5. Überprüfen Sie in einem anderen Fenster, ob Cisco Secure gestartet wurde. Geben Sie `ps -ef ein`, und achten Sie auf den Cisco Secure-Prozess.
6. Telnet-Benutzer (vty) müssen sich jetzt über Cisco Secure authentifizieren. Beim Debuggen auf dem Router wird Telnet von einem anderen Teil des Netzwerks in den Router geleitet. Der Router sollte eine Eingabeaufforderung für Benutzername und Kennwort erstellen. Sie sollten mit den folgenden Kombinationen aus Benutzer-ID und Kennwort auf den Router zugreifen können:
   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```
   Beobachten Sie den Server und den Router, wo Sie die Interaktion sehen sollten, d. h. was wo, Antworten, Anfragen usw. gesendet wird. Korrigieren Sie alle Probleme, bevor Sie fortfahren.
7. Wenn Ihre Benutzer sich auch über Cisco Secure authentifizieren möchten, um in den Aktivierungsmodus zu wechseln, stellen Sie sicher, dass Ihre Konsolenport-Sitzung noch aktiv ist, und fügen Sie diesen Befehl zum Router hinzu:

   ```
   !--- 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. Sie sollten die **Aktivierung** jetzt über Cisco Secure durchführen müssen. Beim Debuggen auf dem Router wird Telnet von einem anderen Teil des Netzwerks in den Router geleitet. Wenn der Router nach Benutzername/Kennwort fragt, antwortet er mit `Operator/Operator`.Wenn der Benutzeroperator versucht, in den Aktivierungsmodus zu wechseln (Berechtigungsebene 15), ist das Kennwort "cisco" erforderlich. Andere Benutzer können nicht in den Aktivierungsmodus wechseln, ohne die Anweisung auf Berechtigungsebene (oder den Daemon Cisco Secure) anzugeben.Beobachten Sie den Server und den Router, wo Sie beispielsweise die Cisco Secure-Interaktion sehen sollten, was wo, Antworten und Anfragen gesendet werden usw. Korrigieren Sie alle Probleme, bevor Sie fortfahren.
9. Schalten Sie den Cisco Secure-Prozess auf dem Server aus, während Sie weiterhin mit dem Konsolenport verbunden sind, um sicherzustellen, dass Ihre Benutzer weiterhin auf den Router zugreifen können, wenn Cisco Secure nicht verfügbar ist:
   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```
   Wiederholen Sie das Telnet, und aktivieren Sie den vorherigen Schritt. Der Router sollte erkennen, dass der Cisco Secure-Prozess nicht reagiert und Benutzern erlaubt, sich anzumelden und mit den Standard-enable-Passwörtern zu aktivieren.
10. Stellen Sie den Cisco Secure-Server wieder auf, und richten Sie eine Telnet-Sitzung zum Router ein. Diese sollte sich über Cisco Secure authentifizieren, mit dem Benutzer-

ID/Kennwort-**Operator/Oper**, um die Authentifizierung Ihrer Konsolenport-Benutzer über Cisco Secure zu überprüfen. Lassen Sie die Verbindung mit dem Router und im Aktivierungsmodus so lange ferngehalten, bis Sie sich über den Konsolenport beim Router anmelden können. Melden Sie sich beispielsweise über den Konsolenport von der ursprünglichen Verbindung zum Router ab, und schließen Sie dann wieder den Konsolenport an. Die Konsolen-Port-Authentifizierung für die Anmeldung mit den vorherigen Benutzer-ID/Kennwort-Kombinationen sollte jetzt über Cisco Secure erfolgen. Beispielsweise muss für die **Aktivierung** ein Benutzer-ID/Kennwort-**Operator/Operator** und ein Kennwort **cisco** verwendet werden.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Autorisierung hinzufügen

Das Hinzufügen einer Autorisierung ist optional.

Standardmäßig gibt es drei Befehlsstufen auf dem Router:

- Berechtigungsstufe 0 - einschließlich Deaktivierung, Aktivierung von Exit, Hilfe und Abmeldung
- Berechtigungsstufe 1 - Normalstufe auf einem Telnet und Eingabeaufforderung sagt `Router>`
- Privilege Level 15 (Berechtigungsebene 15): Aktivierungsebene und Eingabeaufforderung steht für `Router#`

Da die verfügbaren Befehle vom Cisco IOS-Feature-Set, der Cisco IOS-Softwareversion, dem Router-Modell usw. abhängen, gibt es keine umfassende Liste aller Befehle der Ebenen 1 und 15. Beispielsweise ist **show ipx route** nicht in einem nur IP-fähigen Feature-Set vorhanden, **show ip nat trans** ist nicht im Cisco IOS Software Release 10.2.X-Code enthalten**,** da NAT zu diesem Zeitpunkt nicht eingeführt wurde, und **show environment** ist in Routermodellen ohne Stromversorgung und Temperaturüberwachung nicht vorhanden.

Die Befehle, die auf einer bestimmten Ebene auf einem bestimmten Router verfügbar sind, können in der Eingabe eines Befehls gefunden werden**?** an der Eingabeaufforderung im Router, wenn auf dieser Berechtigungsebene.

Die Konsolenport-Autorisierung wurde erst als Funktion hinzugefügt, nachdem CSCdi82030 implementiert wurde. Die Konsolen-Port-Autorisierung ist standardmäßig deaktiviert, um die Wahrscheinlichkeit zu verringern, dass der Router versehentlich gesperrt wird. Wenn ein Benutzer über die Konsole physischen Zugriff auf den Router hat, ist die Konsolenport-Autorisierung nicht sehr effektiv. Die Konsolen-Port-Autorisierung kann jedoch mit dem Befehl **line con 0** in einem Cisco IOS-Image aktiviert werden, in dem CSCdi82030 mit dem Befehl **authorized exec default|WORD** implementiert wurde.

Gehen Sie wie folgt vor:

1. Der Router kann so konfiguriert werden, dass er Befehle über Cisco Secure auf allen oder einigen Ebenen autorisiert. Diese Router-Konfiguration ermöglicht es allen Benutzern, eine Berechtigung für jeden Befehl auf dem Server einzurichten. Sie können alle Befehle über Cisco Secure autorisieren. Wenn der Server jedoch ausgefallen ist, ist keine Autorisierung erforderlich, daher `keine`.Geben Sie bei deaktiviertem Cisco Secure Server die folgenden Befehle ein:Geben Sie diesen Befehl ein, um die Anforderung zu entfernen, dass die Authentifizierung über Cisco Secure erfolgen muss:
   ```
   no aaa authentication enable default tacacs+ none
   ```
   Geben Sie diese Befehle ein, damit die Befehlsautorisierung über Cisco Secure erfolgen muss:
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. Während der Cisco Secure-Server ausgeführt wird, wird Telnet mit der Benutzer-ID/dem Kennwort **loneusr/lonepwd** in den Router geleitet. Dieser Benutzer sollte nur folgende Befehle ausführen können:
   ```
   show version
   ping <anything>
   logout
   ```
   Die vorherigen Benutzer, **adminusr/adminusr**, **operator/oper**, **desusr/encrypt**, sollten weiterhin alle Befehle aufgrund ihres `Standarddiensts = permit ausführen können`. Wenn Probleme mit dem Prozess auftreten, wechseln Sie in den Aktivierungsmodus des Routers, und aktivieren Sie das Autorisierungsdebuggen mit dem folgenden Befehl:
   ```
   terminal monitor
   debug aaa authorization
   ```
   Beobachten Sie den Server und den Router, wo Sie beispielsweise die Cisco Secure-Interaktion sehen sollten, was wo, Antworten und Anfragen gesendet werden usw. Korrigieren Sie alle Probleme, bevor Sie fortfahren.
3. Der Router kann so konfiguriert werden, dass exec-Sitzungen über Cisco Secure autorisiert werden. Die **AAA-Autorisierung exec default tacacs+ none**-Befehl **bedeutet** TACACS+-Autorisierung für Exec-Sitzungen.Wenn Sie dies anwenden, betrifft es Benutzer **Zeit/Zeit**, **Telnet/Telnet**, **todam/todam**, **todpm/todpm** und **somerouters/somerouters.** Nachdem Sie diesen Befehl zum Router und Telnet zum Router als **Uhrzeit/Uhrzeit** des Benutzers hinzugefügt haben, bleibt eine exec-Sitzung eine Minute lang geöffnet (Timeout = 1). Benutzer **telnet/telnet** betritt den Router, wird aber sofort an die andere Adresse gesendet (Set autocmd = "telnet 171.68.118.102"). Es ist möglich, dass die Benutzer **todam/todam** und **todpm/todpm** den Router erreichen oder nicht, was von der Tageszeit während der Prüfung abhängt. Benutzer **somerouters** können Telnet nur von Netzwerk 10.31.1.x aus in den Router koala.rtp.cisco.com eingeben. Cisco Secure versucht, den Namen des Routers aufzulösen. Wenn Sie die IP-Adresse 10.31.1.5 verwenden, ist sie gültig, wenn die Auflösung nicht erfolgt, und wenn Sie den Namen koala verwenden, ist sie gültig, wenn die Auflösung erreicht ist.

Hinzufügen von Buchhaltung

Die Rechnungslegung ist optional.

1. Die Abrechnung findet nur nach Konfiguration im Router statt, wenn der Router die Cisco IOS-Softwareversion später als die Cisco IOS-Softwareversion 11.0 ausführt. Sie können Accounting auf dem Router aktivieren:

```
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+
```

Hinweis: Die Befehlsabrechnung wurde in der Cisco Bug-ID CSCdi44140 unterbrochen. Wenn Sie jedoch ein Image verwenden, in dem dies behoben ist, kann auch die Befehlsabrechnung aktiviert werden.

2. Debuggen von Accounting-Datensätzen auf dem Router hinzufügen:
```
terminal monitor
debug aaa accounting
```
3. Die Fehlerbehebung auf der Konsole sollte Accounting-Datensätze anzeigen, die beim Anmelden von Benutzern auf den Server eingegeben werden.
4. So rufen Sie Accounting-Datensätze als root ab:
```
CD $BASE/utils/bin
./AcctExport <filename> no_truncate
```
`no_truncate` bedeutet, dass die Daten in der Datenbank gespeichert werden.

Hinzufügen von DFÜ-Benutzern

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die anderen Funktionen von Cisco Secure funktionieren, bevor Sie DFÜ-Benutzer hinzufügen. Wenn der Cisco Secure Server und das Modem vor diesem Zeitpunkt nicht funktionierten, funktionieren sie nach diesem Zeitpunkt nicht mehr.
2. Fügen Sie diesen Befehl zur Router-Konfiguration hinzu:
```
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
```
Die Schnittstellenkonfigurationen unterscheiden sich je nach Authentifizierungsmethode, in diesem Beispiel werden jedoch Einwahlleitungen mit den folgenden Konfigurationen verwendet:
```
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. Aus der Benutzerdatei von Cisco Secure:chapuser - CHAP/PPP - Benutzer wählt in Zeile 1; Adresse wird durch **Peer-Standard-IP-Adresspool async und ip local pool async 10.6.100.101 10.6.100.103** auf dem Router zugewiesenchapadr - CHAP/PPP - Benutzer wählt in Zeile 1; Adresse 10.29.1.99 wird vom Server zugewiesenchapacl - CHAP/PPP - Benutzer wählt in Zeile 1; Die Adresse 10.29.1.100 wird vom Server zugewiesen, und die eingehende Zugriffsliste 101 wird angewendet (die auf dem Router definiert werden

muss).papuser - PAP/PPP - Benutzer wählt in Zeile 2; Adresse wird durch **Peer-Standard-IP-Adresspool async und ip local pool async 10.6.100.101 10.6.100.103** auf dem Router zugewiesenpapadr - PAP/PPP - Benutzer wählt in Zeile 2; Adresse 10.29.1.98 wird vom Server zugewiesenpapacl - PAP/PPP - Benutzer wählt in Zeile 2; Die Adresse 10.29.1.100 wird vom Server zugewiesen, und es wird die eingehende Zugriffsliste 101 angewendet, die auf dem Router definiert werden muss.loginauto - Benutzer wählt in Zeile 3 ein; Anmeldeauthentifizierung mit automatischem Befehl online zwingt Benutzer zur PPP-Verbindung und weist Adresse aus dem Pool zu

4. Microsoft Windows-Setup für alle Benutzer außer User Login AutoWählen Sie **Start > Programme > Zubehör > DFÜ-Netzwerk aus**.Wählen Sie **Verbindungen > Neue Verbindung herstellen aus**. Geben Sie einen Namen für die Verbindung ein.Geben Sie die modemspezifischen Informationen ein. Wählen Sie unter **Konfigurieren > Allgemein** die höchste Modemgeschwindigkeit aus, aber aktivieren Sie nicht das Kontrollkästchen darunter.Verwenden Sie unter **Konfigurieren > Verbindung** 8 Datenbits, keine Parität und 1 Stoppbit. Die Anrufvoreinstellungen lauten **Warten Sie auf den Wählton, bevor Sie wählen**, und **Abbrechen des Anrufs, wenn der Anruf nach 200 Sekunden nicht verbunden ist**.Wählen Sie unter Advanced (Erweitert) nur **Hardware Flow Control** and **Modulation Type Standard (Hardware-Flusssteuerung** und **Modulationstyp Standard)** aus.Unter **Konfigurieren > Optionen** sollte nur unter Statussteuerung eine Überprüfung durchgeführt werden. Klicken Sie auf **OK**.Geben Sie im nächsten Fenster die Telefonnummer des Ziels ein, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.Wenn das neue Verbindungssymbol angezeigt wird, klicken Sie mit der rechten Maustaste auf das Symbol, wählen **Eigenschaften aus**, und klicken Sie dann auf **Servertyp**.Wählen Sie **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** und überprüfen Sie keine erweiterten Optionen.Aktivieren Sie unter Zulässige Netzwerkprotokolle mindestens **TCP/IP**.Wählen Sie unter TCP/IP-Einstellungen die Option **Server assigned IP address** (**Server-zugewiesene IP-Adresse**), **Server assigned name server address (Server-Serveradressen)** und **Use default gateway on remote network (Standardgateway im Remote-Netzwerk verwenden)**. Klicken Sie auf **OK**.Wenn Sie auf das Symbol doppelklicken, um das Fenster Connect To (Verbinden mit) zu öffnen, um eine Nummer zu wählen, müssen Sie die Felder User name (Benutzername) und Password (Kennwort) eingeben und dann auf **Connect (Verbinden)** klicken.
5. Microsoft Windows 95-Setup für die BenutzeranmeldungDie Konfiguration für die BenutzeranmeldungAuto, den Authentifizierungsbenutzer mit dem Befehl autocommand PPP, ist mit Ausnahme der Konfiguration **> Optionen** für andere Benutzer identisch. Aktivieren Sie **nach dem Wählen die Option Terminalfenster öffnen**.Wenn Sie auf das Symbol doppelklicken, um das Fenster Connect To (Verbindung mit) zum Wählen aufzurufen, füllen Sie die Felder User name (Benutzername) und Password (Kennwort) nicht aus. Klicken Sie auf **Verbinden**, und geben Sie nach Herstellung der Verbindung zum Router im schwarzen Fenster Benutzername und Kennwort ein.Klicken Sie nach der Authentifizierung auf **Weiter(F7)**.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Server

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

Router

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen. Weitere Informationen zu bestimmten Befehlen finden Sie unter Cisco IOS Debug Command Reference.

- **terminal monitor** - Zeigt **Debug**-Befehlsausgaben und Systemfehlermeldungen für das aktuelle Terminal und die aktuelle Sitzung an.
- **debug ppp negotiation** - Zeigt die PPP-Pakete an, die während des PPP-Starts übertragen werden und über die PPP-Optionen ausgehandelt werden.
- **debug ppp packet** - Zeigt PPP-Pakete an, die gesendet und empfangen werden. Dieser Befehl zeigt Low-Level Packet Dumps an.
- **debug ppp chap** - Zeigt Informationen über Datenverkehr und Austausch in einem Internetwork an, das das Challenge Authentication Protocol (CHAP) implementiert.
- **debug aaa authentication** - Erfahren Sie, welche Authentifizierungsmethoden verwendet werden und welche Ergebnisse diese Methoden haben.
- **debug aaa authorized** - Erfahren Sie, welche Autorisierungsmethoden verwendet werden und welche Ergebnisse diese Methoden liefern.

Cisco Secure Users-Datei

```
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
   }
   }
```

Zugehörige Informationen

- Produktsupport für Cisco Secure ACS für UNIX
- Problemhinweise zu Sicherheitsprodukten (einschließlich Cisco Secure UNIX)