Installatie en verwijdering van Cisco Secure 2.x TACACS+

Inhoud

Inleiding

Dit document is bedoeld om de eerste gebruiker van Cisco Secure 2.x te helpen bij de installatie en het foutherstel van een Cisco Secure TACACS+-configuratie. Het is geen volledige beschrijving van de Cisco Secure-functies.

Raadpleeg uw Cisco Secure-documentatie voor meer volledige informatie over serversoftware en gebruikersinstelling. Raadpleeg de Cisco IOS-softwaredocumentatie voor de juiste release voor meer informatie over routeropdrachten.

Voorwaarden

Vereisten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure ACS 2.x en hoger
- Cisco IOS-softwarerelease 11.3.3 en hoger

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Cisco Secure-installatie

Voer de volgende stappen uit:

1. Zorg ervoor dat u de instructies gebruikt die met de software zijn meegeleverd, om de Cisco Secure-code op de UNIX-server te installeren.
2. Om te bevestigen dat het product stopt en start, `cd` invoeren `op /etc/rc0.d` en als wortel, `uitvoeren./K80Cisco Secure` (om de datums te stoppen).Voer `cd in op /etc/rc2.d` en als wortel, voer `/S80Cisco Secure` (om de datums te starten) uit.Bij het opstarten, dient u berichten te zien zoals:
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   Start `$BASE/utils/psg` om er zeker van te zijn dat ten minste één van de afzonderlijke processen wordt uitgevoerd, bijvoorbeeld SQL, waar of een andere database-machine, Cisco Secure Database Server-proces, Netscape Web Server, NetWeb Admin, Access Web Server, Cisco Secure AAA-proces of Auto-start-proces.
3. Om u te verzekeren dat u in de juiste gidsen bent, stel milieuvariabelen en paden in uw shell omgeving op. c-shell wordt hier gebruikt.**$BASE** is de map waarin Cisco Secure is geïnstalleerd, geselecteerd tijdens de installatie. Het bevat zoals DOCS, DBServer, CSU, enzovoort.In dit voorbeeld wordt de installatie in /opt/CSCOacs verondersteld, maar dit kan op uw systeem verschillen:
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $QLANY is de folder waar de standaard Cisco Secure-database is geïnstalleerd, geselecteerd tijdens installatie. Als de standaard database die bij het product komt, SQLnytoe, gebruikt werd, bevat het zulke directories als database, doc, enzovoort.In dit voorbeeld wordt de installatie in /opt/CSCOacs/SYBSsa50 verondersteld, maar dit kan op uw systeem verschillen.
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   Voeg paden toe in uw shell omgeving:
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD naar $BASE/fig**CSU.cfg** is het Cisco Secure-serverbeheerbestand. Maak een reservekopie van dit bestand.In dit bestand toont `LIST`_LIST_licentie_key de licentiesleutel die u via het licentieproces hebt ontvangen als u de software hebt aangeschaft; als dit een 4-poorts proeflicentie is, kun je deze regel verlaten.De sectie **NAS_configuratie_nas_klaar** kan een standaard server van de netwerktoegang (NAS) of router bevatten, of het NAS dat u tijdens de installatie invoert. Voor het debuggen in dit voorbeeld kunt u *elke* NAS toestaan om te communiceren met de Cisco Secure server *zonder* een sleutel. Verwijder bijvoorbeeld de naam van de NAS en de toets van de lijnen die `/* NAS-naam` bevatten, `en` de `NAS-naam kan hier */`" en */*NAS/Cisco beveiligde geheime sleutel */*. De enige *stanza* in dat gebied luidt:
   ```
   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 = {
```

Wanneer u dit doet, vertel u Cisco Secure dat het toegestaan is om met alle NAS's te praten zonder uitwisseling van toetsen.

5. Als u de debuginformatie wilt laten gaan naar /var/log/csuslog, moet u een regel hebben in de bovenste sectie van CSU.cfg, die de server vertelt hoeveel debugging te doen is. 0X7FFFFFF voegt alle mogelijke debugging toe. Voeg deze regel toe of wijzig deze dienovereenkomstig:
   ```
   NUMBER config_logging_configuration = 0x7FFFFFFF;
   ```
   Deze extra lijn stuurt de zuiverende informatie naar local0:
   ```
   NUMBER config_system_logging_level = 0x80;
   ```
   Voeg dit item toe om het /etc/syslog.conf-bestand te wijzigen:
   ```
   local0.debug /var/log/csuslog
   ```
   recycleren van de computer om opnieuw te lezen:
   ```
   kill -HUP `cat /etc/syslog.pid`
   ```
   Recycleert de Cisco Secure-server:
   ```
   /etc/rc0.d/K80Cisco Secure
   /etc/rc2.d/S80Cisco Secure
   ```
   Het moet nog beginnen.
6. U kunt de browser gebruiken om gebruikers, groepen, enz. toe te voegen, of de CSimportvoorziening. De gebruikers van de steekproef in het vlakke bestand aan het eind van dit document kunnen gemakkelijk met CSimport in de database worden verplaatst. Deze gebruikers werken voor testdoeleinden en u kunt deze verwijderen zodra u uw eigen gebruikers hebt. Nadat u de invoer hebt ingevoerd, kunt u de geïmporteerde gebruikers zien via de GUI.Als u beslist CSimport te gebruiken:
   ```
   CD $BASE/utils
   ```
   Leg de gebruiker en groepsprofielen aan het eind van dit document in een bestand zoals overal op het systeem, dan van de $BASE/utils folder, met de daemons die, bijvoorbeeld, /etc/rc2.d/S80Cisco Secure, en als gebruikerswortel, CCSimport met de test (-t) optie lopen:
   ```
   ./CSimport -t -p <path_to_file> -s <name_of_file>
   ```
   Deze test syntax voor de gebruikers; U dient berichten te ontvangen zoals:
   ```
   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...
   ```
   U dient *geen* berichten te ontvangen, zoals:
   ```
   Error at line 2: password = "adminusr"
   Couldn't repair and continue parse
   ```
   Of er fouten zijn gemaakt, onderzocht de upgrade.log om te controleren of de profielen zijn geselecteerd. Zodra fouten worden gecorrigeerd, van de $BASE/utils folder, met de datums die lopen (/etc/rc2.d/S80Cisco Secure), en als gebruikerswortel, runt CSimport met de optie gecommitteerd (-c) om de gebruikers in de database te verplaatsen:
   ```
   ./CSimport -c -p <path_to_file> -s <name_of_file>
   ```
   Opnieuw dienen er geen fouten te worden gemaakt op het scherm of in het upgrade.log.

7. Ondersteunde webbrowsers zijn vermeld in de technische knop Cisco Secure Compatibiliteit. Vanaf uw PC browser, punt naar de Cisco Secure/Solaris doos **http://#.#.#.#/cs** waar **#.#.#.#** is de IP van de Cisco Secure/Solaris server.Voer op het scherm dat verschijnt een **verandering in** voor de gebruiker **superuser** en voor het wachtwoord. Wijzig het wachtwoord op dit moment niet. U dient de toegevoegde gebruikers/groepen te zien als u de CSimport in de vorige stap gebruikt of als u in de GUI kunt klikken op blokkering van het bladeren en gebruikers en groepen handmatig door de GUI toevoegen.

Verificatie instellen

Opmerking: Deze routerconfiguratie is ontwikkeld op een router die Cisco IOS-softwarerelease 11.3.3.draait. Cisco IOS-softwarerelease 12.0.5.T en laat later **groeptacs** in plaats van **tacs** zien.

Op dit punt, moet u de router configureren.

1. Vermoord Cisco Secure terwijl u de router vormt.
   `/etc/rc0.d/K80Cisco Secure to stop the daemons.`
2. Op de router, start om TACACS+ te configureren. Geef de modus op en type `conversie naar` voordat de opdracht wordt ingesteld. Deze syntaxis garandeert dat u niet uit de router bent vergrendeld en *aanvankelijk* Cisco Secure-netwerk niet actief is. Voer `ps in -ef | grep Secure` om te controleren of Cisco Secure niet wordt uitgevoerd en vermoord -9 het proces als dit zo is:

   ```
   !--- 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. Test om zeker te zijn dat u nog toegang tot de router met telnet en door de troostpoort kunt hebben voordat u verdergaat. Omdat Cisco Secure niet actief is, dient het enabled-wachtwoord te worden geaccepteerd.**Waarschuwing:** houd de console poortsessie actief en blijf in de activiteitsmodus; deze zitting mag niet worden uitgesteld . U start om de toegang tot de router op dit punt te beperken en u moet configuratieveranderingen kunnen doorvoeren zonder uzelf te vergrendelen.Geef deze opdrachten uit om de interactie tussen server en router op de router te bekijken:
   ```
   terminal monitor
   debug aaa authentication
   ```
4. Als wortel, start Cisco Secure op de server:
   `/etc/rc2.d/S80Cisco Secure`
   Dit begint de processen, maar u wilt meer het debuggen mogelijk maken dan wordt ingesteld in S80Cisco Secure, dus:
   ```
   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
   ```
   Met `-x` optie draait Cisco Secure op de voorgrond zodat interactie tussen router en server

kan worden waargenomen. U dient geen foutmeldingen te zien. Het Cisco Secure-proces moet starten en ophangen vanwege de -x-optie.

5. Controleer vanuit een ander venster of Cisco Secure is gestart. Voer `IPS -ef in` en kijk naar het Cisco Secure-proces.
6. Telnet (vty) gebruikers moeten nu authentiek moeten zijn door Cisco Secure. Met debug op de router, Telnet in de router van een ander deel van het netwerk. De router zou een gebruikersnaam en een wachtwoord moeten produceren. U hebt toegang tot de router met deze combinaties gebruiker-id/wachtwoord:
   ```
   adminusr/adminusr
   operator/oper
   desusr/encrypt
   ```
   Kijk naar de server en de router waar je de interactie zou moeten zien, dat wil zeggen wat er wordt verzonden waar, reacties en verzoeken, enzovoort. Corrigeer alle problemen voordat u verdergaat.
7. Als u wilt dat uw gebruikers ook voor authenticatie door Cisco Secure om in machtigingsmodus te geraken, zorg er dan voor dat uw console poortsessie nog actief is en voeg deze opdracht aan de router toe:

   ```
   !--- 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. U dient nu via Cisco Secure in te **schakelen**. Met debug op de router, Telnet in de router van een ander deel van het netwerk. Wanneer de router om een gebruikersnaam/wachtwoord vraagt, reageert hij met `operator/oper`.Wanneer de gebruikershandleiding probeert de activeringsmodus in te voeren (voorkeursniveau 15), moet het wachtwoord "cisco" worden ingevoerd. Andere gebruikers zullen geen machtigingsmodus kunnen invoeren zonder de verklaring op voorkeursniveau (of de Cisco Secure Data Down).Let op de server en de router waar u de Cisco Secure-interactie wilt zien, bijvoorbeeld, wat wordt verzonden waar, antwoorden en verzoeken, enzovoort. Corrigeer alle problemen voordat u doorgaat.
9. Stel het Cisco Secure-proces op de server ingedrukt terwijl u nog steeds verbonden is met de poort op de console om er zeker van te zijn dat uw gebruikers nog steeds toegang hebben tot de router als Cisco Secure is uitgeschakeld:
   ```
   'ps -ef' and look for Cisco Secure process
   kill -9 pid_of_Cisco Secure
   ```
   Herhaal het telnet en stel de vorige stap in. De router moet zich realiseren dat het Cisco Secure-proces niet reageert en gebruikers de mogelijkheid biedt om in te loggen en wachtwoorden in te schakelen met de standaardinstelling.
10. Breng de Cisco Secure server opnieuw aan en stel een Telnet-sessie aan de router op, die door Cisco Secure moet worden geauthentiseerd, met **user**-id/wachtwoord **operator/oper** om verificatie van uw console-poortgebruikers via Cisco Secure te controleren. Blijft in de router aangesloten en in plaats zet in modus tot u zeker bent u aan de router door de console poort kunt inloggen, bijvoorbeeld, log uit van uw oorspronkelijke verbinding met de router door de console poort en sluit dan opnieuw aan op de console poort. Verificatie van console-poorten om in te loggen met het gebruik van de vorige gebruikers-id/wachtwoord combinaties, dient nu te worden uitgevoerd via Cisco Secure. Bijvoorbeeld, de **operator/oper van** de gebruikersid/wachtwoord**/oper** en **cisco van het** wachtwoord moeten worden gebruikt om **cisco** in te **schakelen**.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Toestemming toevoegen

Toevoegen van de vergunning is facultatief.

Standaard zijn er drie commando-niveaus op de router:

- Niveau 0 op basis van prioriteit, dat behalve blokjes, uittreding, hulp en uitloging omvat
- Primair niveau 1-normaal niveau op een telnet en de vraag zegt `router>`
- Niveau 15-toelaten niveau en de vraag stelt `router#`

Aangezien beschikbare opdrachten afhankelijk zijn van de Cisco IOS-functieset, Cisco IOS-softwarerelease, routermodel, enzovoort, is er geen uitgebreide lijst van alle opdrachten op niveau 1 en 15. **Bijvoorbeeld**, laat **ipx-route** niet aanwezig zijn in een IP-alleen-functieset, **laat zien dat ip nat-trans** niet in Cisco IOS-softwarerelease 10.2.X-code staat omdat NAT op dat niet op dat moment is geïntroduceerd, , het aantoonbare milieu is niet aanwezig in routermodellen zonder elektriciteitstoevoer en temperatuurcontrole.

Opdrachten beschikbaar in een bepaalde router op een bepaald niveau kunnen gevonden worden als ze een opdracht invoeren**?** bij de aanwijzing in de router wanneer op dat voorkeursniveau.

Console poortvergunning werd niet als optie toegevoegd tot CSCdi82030 werd geïmplementeerd. Console poortautorisatie is standaard uitgeschakeld om de kans te verminderen dat per ongeluk buiten de router wordt gehouden. Als een gebruiker fysieke toegang tot de router door de console heeft, is de console havenvergunning niet zeer effectief. Maar, console kan poortautorisatie worden ingeschakeld onder de **lijn con 0** opdracht in een Cisco IOS beeld waarin CSCdi82030 werd geïmplementeerd met de **autorisatie exec standaard|WORD** opdracht.

Voer de volgende stappen uit:

1. De router kan worden geconfigureerd om opdrachten door Cisco Secure op alle of sommige niveaus toe te staan. Deze routerconfiguratie stelt alle gebruikers in staat om een autorisatie per opdracht op de server in te stellen. U kunt alle opdrachten via Cisco Secure autoriseren maar als de server beneden is, is er geen autorisatie nodig, dus `geen`.Voer deze opdrachten in als de Cisco Secure-server beneden is:Voer deze opdracht in om het vereiste te verwijderen dat verificatie mogelijk maakt via Cisco Secure:
   ```
   no aaa authentication enable default tacacs+ none
   ```
   Voer deze opdrachten in om te eisen dat er een autorisatie voor opdrachten wordt uitgevoerd via Cisco Secure:
   ```
   aaa authorization commands 0 default tacacs+ none
   aaa authorization commands 1 default tacacs+ none
   aaa authorization commands 15 default tacacs+ none
   ```
2. Terwijl de Cisco Secure-server draait, gaat telnet naar de router met gebruikers-id/wachtwoord **langer** in**/uitgebreid**. Deze gebruiker kan geen andere opdrachten dan:
   ```
   show version
   ping <anything>
   logout
   ```
   De vorige gebruikers, **beheerder/beheerder**, **operator/oper**, **desusr/encrypt**, moeten nog

steeds alle opdrachten kunnen doen op grond van hun `standaardservice = licentie`. Als er problemen zijn met het proces, geef dan mode op de router in en zet autorisatie aan het zuiveren met deze opdracht:

```
terminal monitor
debug aaa authorization
```

Let op de server en de router waar u de Cisco Secure-interactie wilt zien, bijvoorbeeld, wat wordt verzonden waar, antwoorden en verzoeken, enzovoort. Corrigeer alle problemen voordat u verdergaat.

3. De router kan worden geconfigureerd om extra sessies toe te staan door Cisco Secure. De **Aa autorisatie EXec standaard tacacs+ geen** commando instituten TACACS+ toestemming voor spoedeisende sessies.Als u dit toepast, heeft dit gevolgen voor gebruikers **tijd/tijd**, **telnet/telnet**, **dam/dam**, **todpm/todpm** en **somerouters/somerouters.** Nadat u deze opdracht aan de router en het telnet aan de router als **tijd/tijd van de** gebruiker toevoegt, blijft een exec-sessie voor één minuut open (set timeout = 1). Gebruiker **telnet/telnet** gaat de router in maar wordt onmiddellijk naar het andere adres verzonden (set autocom = "telnet 171.68.118.102"). Het is mogelijk dat gebruikers van **stuwdam/stuwdam** en **todpm/todpm** toegang tot de router hebben of kunnen krijgen, wat afhangt van het tijdstip van de dag dat het tijdens de test is. Gebruiker **somerouters** is alleen in staat om in de router koala.rtp.cisco.com te tellen vanaf netwerk 10.31.1.x. Cisco Secure probeert de naam van de router op te lossen. Als u het IP-adres 10.31.1.5 gebruikt, is deze geldig als er geen resolutie plaatsvindt en als u de naam koala gebruikt, is deze geldig als de resolutie is doorlopen.

Boekhouding toevoegen

Boekhouding toevoegen is niet verplicht.

1. Boekhouding vindt niet plaats behalve wanneer dit in de router is geconfigureerd, als de router Cisco IOS-softwarerelease later dan Cisco IOS-softwarerelease 11.0 uitvoert. U kunt accounting op de router inschakelen:

```
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+
```

Opmerking: Opdracht-accounting was defect, in Cisco bug ID CSCdi44140, maar als u een afbeelding gebruikt waarin dit vaststaat, kan commandoaccounting ook ingeschakeld zijn.

2. Voeg accounting record debugging op de router toe:

```
terminal monitor
debug aaa accounting
```

3. Debug op de console zou boekhoudkundige records moeten tonen die de server als gebruikerslog in gaan.
4. Om boekhoudkundige gegevens terug te krijgen, als wortel:

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

`no_truncate` betekent dat de gegevens in de database bewaard blijven.

Gebruikers van de inbel toevoegen

Voer de volgende stappen uit:

1. Zorg ervoor dat de andere functies van Cisco Secure-werk zijn voordat u inbelgebruikers

toevoegt. Als de Cisco Secure-server en de modem niet voor dit punt werkten, werken ze niet meer na dit punt.

2. Voeg dit bevel aan de routerconfiguratie toe:

```
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
```

De interfaceconfiguraties verschillen, wat afhangt van de manier waarop de authenticatie wordt uitgevoerd, maar inbellijnen worden in dit voorbeeld gebruikt, met deze configuraties:

```
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. Uit gebruikersbestand van Cisco Secure:chapuser-CHAP/PPP-gebruiker intoetsen op regel 1; Het adres wordt toegewezen door **peer standaard IP adrestoewijzing async en ip lokale pool async 10.6.100.101 10.6.100.103** op de routerchapaddr-CHAP/PPP-gebruiker intoetsen op regel 1; adres 10.29.1.99 wordt toegewezen per serverkabel-CHAP/PPP—gebruiker intoetsen op lijn 1; Adres 10.29.1.100 wordt toegewezen door server en de inkomende toegangslijst 101 wordt toegepast (die op de router moet worden bepaald)papuser-PAP/PPP— user dials in on line 2; Het adres wordt toegewezen door **peer standaard IP adrestoewijzing async en ip lokale pool async 10.6.100.101 10.6.100.103** op de routerpop-document-PAP/PPP-gebruiker intoetsen op regel 2; adres 10.29.1.98 wordt toegewezen per servertoepassing—PAP/PPP—gebruiker intoetsen op regel 2; Adres 10.29.1.100 wordt toegewezen door server en de inkomende toegangslijst 101 wordt toegepast, die op de router moet worden bepaaldloginauto-gebruiker wijst in op lijn 3; inlogverificatie met automatische commando op line force user to PPP-verbinding en toewijzing van adres uit de pool
4. Microsoft Windows Setup voor alle gebruikers behalve gebruikershandleidingKies **Start > Programma's > Accessoires > Inbelnetwerken**.Kies **verbindingen > Nieuwe verbinding maken**. Typ een naam voor de aansluiting.Voer uw modemspecifieke informatie in. In **Configureren > Algemeen** kiest u de hoogste snelheid van de modem, maar schakelt u het onderstaande vakje niet in.In **Configureer > verbinding**, gebruik 8 gegevensbits, geen pariteit en 1 stopbit. Voorkeuren van de vraag **wachten op kiestoon alvorens te draaien** en **annuleren de vraag als niet verbonden na 200 seconden**.Kies in Advanced alleen de **standaard voor Hardware Flow Control** en **Modulatie**.Bij **het configureren > Opties** dient er niets te worden gecontroleerd behalve onder statuscontrole. Klik op **OK**.Voer in het volgende venster het telefoonnummer van de bestemming in en klik vervolgens op **Volgende** en klik vervolgens op **Voltooien**.Klik met de rechtermuisknop op het pictogram voor de nieuwe verbinding en kies **Eigenschappen**. Klik vervolgens op **Type server**.Kies **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** en controleer geen geavanceerde opties.In toegestane

netwerkprotocollen controleert u ten minste **TCP/IP**.Selecteer onder TCP/IP-instellingen **het IP-adres van de server**, de **servertoegewezen naam serveradressen** en de **standaardgateway op een extern netwerk**. Klik op **OK**.Wanneer u dubbelklikt op het pictogram om het venster Connect To op te roepen om te bellen, moet u de velden Gebruikersnaam en Wachtwoord invullen en vervolgens op **Connect** klikken.

5. Microsoft Windows 95 Instellingen voor gebruikershandleidingDe configuratie voor gebruikersloginauto, de authenticatiegebruiker met automatische opdracht PPP, is hetzelfde als voor andere gebruikers behalve in het venster **Configure > Opties**. Controleer **Breng het eindvenster op na het draaien**.Wanneer u op het pictogram dubbelklikt om het venster Connect To terug te draaien, vult u de velden Gebruikersnaam en Wachtwoord niet in. Klik op **Connect** en nadat de verbinding met de router is gemaakt, typt u de gebruikersnaam en het wachtwoord in het zwarte venster dat verschijnt.Klik na verificatie op **Doorgaan (F7)**.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Server

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

router

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt. Voor meer informatie over specifieke opdrachten, zie Cisco IOS Opdrachtreferentie voor bug Opdrachten.

- **de terminal monitor**—Display **debug** van de opdrachtoutput en de systeemfoutmeldingen voor de huidige terminal en sessie.
- **debug van PPP onderhandeling**-display PPP-pakketten die tijdens PPP-opstarten worden verzonden, waar PPP-opties worden onderhandeld.
- **bug** van **PPP pakket**-display PPP-pakketten die worden verzonden en ontvangen. Deze opdracht geeft pakjes op een laag niveau weer.
- **debug ppp chap**-display informatie over verkeer en uitwisseling in een internetwerk dat Challenge Authentication Protocol (CHAP) implementeert.
- **debug a authenticatie** - Zie welke methoden van authenticatie worden gebruikt en wat de resultaten van deze methoden zijn.
- **debug a autorisatie**—Bekijk welke methoden van autorisatie worden gebruikt en wat de resultaten van deze methoden zijn.

Cisco Secure-gebruikersbestand

```
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
   }
   }
```

Gerelateerde informatie

- Cisco Secure ACS voor UNIX-productondersteuning
- Security producten meldingen uit het veld (inclusief Cisco Secure UNIX)