Configuration et débogage de CiscoSecure 2.x TACACS+

Contenu

Introduction

Ce document est destiné à aider le premier utilisateur Cisco Secure 2.x à configurer et à déboguer une configuration Cisco Secure TACACS+. Il ne s'agit pas d'une description exhaustive des fonctionnalités Cisco Secure.

Reportez-vous à la documentation Cisco Secure pour plus d'informations sur le logiciel serveur et la configuration utilisateur. Reportez-vous à la documentation du logiciel Cisco IOS pour obtenir la version appropriée pour plus d'informations sur les commandes du routeur.

Conditions préalables

Conditions requises

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure ACS 2.x et versions ultérieures
- Logiciel Cisco IOS® version 11.3.3 et ultérieure

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration de Cisco Secure

Procédez comme suit :

1. Veillez à utiliser les instructions fournies avec le logiciel afin d'installer le code sécurisé Cisco sur le serveur UNIX.
2. Afin de confirmer que le produit s'arrête et démarre, entrez `cd à /etc/rc0.d` et en tant que root, exécutez `./K80Cisco Secure` (pour arrêter les démons).Entrez `cd sur /etc/rc2.d` et en tant que root, exécutez `./S80Cisco Secure` (pour démarrer les démons).Au démarrage, des messages tels que :
   ```
   Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
   DBServer, AAA Server
   ```
   Exécutez `$BASE/utils/psg` afin de vous assurer qu'au moins un des processus individuels s'exécute, par exemple, SQLAnywhere ou un autre moteur de base de données, le processus de serveur de base de données Cisco Secure, Netscape Web Server, Netscape Web Admin, Acme Web Server, Cisco Secure AAA ou le processus de redémarrage automatique.
3. Afin de vous assurer que vous êtes dans les répertoires appropriés, configurez des variables et des chemins d'environnement dans votre environnement shell. c-shell est utilisé ici.**$BASE** est le répertoire dans lequel Cisco Secure est installé, choisi lors de l'installation. Il contient des répertoires tels que DOCS, DBServer, CSU, etc.Dans cet exemple, l'installation dans /opt/CSCOacs est supposée, mais cela peut différer sur votre système :
   ```
   setenv $BASE   /opt/CSCOacs
   ```
   $SQLANY est le répertoire dans lequel la base de données Cisco Secure par défaut est installée, choisi lors de l'installation. Si la base de données par défaut fournie avec le produit, SQLAnywhere, a été utilisée, elle contient des répertoires tels que base de données, doc, etc.Dans cet exemple, l'installation dans /opt/CSCOacs/SYBSsa50 est supposée, mais cela peut différer sur votre système.
   ```
   setenv $SQLANY /opt/CSCOacs/SYBSsa50
   ```
   Ajoutez des chemins dans votre environnement Shell pour :
   ```
   $BASE/utils
   $BASE/bin
   $BASE/CSU
   $BASE/ns-home/admserv
   $BASE/Ns-home/bin/httpd
   $SQLANY/bin
   ```
4. CD à $BASE/config**CSU.cfg** est le fichier de contrôle du serveur sécurisé Cisco. Effectuez une copie de sauvegarde de ce fichier.Dans ce fichier, `LIST config_license_key` affiche la clé de licence que vous avez reçue lors du processus de licence si vous avez acheté le logiciel ; s'il s'agit d'une licence d'essai à 4 ports, vous pouvez laisser cette ligne de côté.La section **NAS config_nas_config** peut contenir un serveur ou un routeur d'accès au réseau par défaut, ou le NAS que vous avez saisi lors de l'installation. À des fins de débogage dans cet exemple, vous pouvez autoriser *tout* NAS à communiquer avec le serveur Cisco Secure *sans* clé. Par exemple, supprimez le nom du NAS et la clé des lignes qui contiennent `/* le nom du NAS peut aller ici */`" et */*NAS/Cisco Secure secret key */*. La seule *strophe* dans ce

domaine :

```
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 = {
```

Dans ce cas, vous indiquez à Cisco Secure qu'il est autorisé à communiquer avec tous les NAS sans échange de clés.

5. Si vous souhaitez que les informations de débogage aillent dans /var/log/csuslog, vous devez avoir une ligne dans la section supérieure de CSU.cfg, qui indique au serveur combien le débogage doit être effectué. 0X7FFFFFFF ajoute tout le débogage possible. Ajoutez ou modifiez cette ligne en conséquence :

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

   Cette ligne supplémentaire envoie les informations de débogage à local0 :

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

   Ajoutez également cette entrée afin de modifier le fichier /etc/syslog.conf :

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

   Ensuite, recyclez le slogd pour le relire :

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

   Recycler le serveur Cisco Secure :

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

   Il devrait encore commencer.

6. Vous pouvez utiliser le navigateur pour ajouter des utilisateurs, des groupes, etc., ou l'utilitaire CSimport. Les exemples d'utilisateurs dans le fichier plat à la fin de ce document peuvent facilement être déplacés dans la base de données à l'aide de CSimport. Ces utilisateurs fonctionneront à des fins de test et vous pouvez les supprimer une fois que vous aurez vos propres utilisateurs. Une fois importé, vous pouvez voir les utilisateurs importés via l'interface utilisateur graphique.Si vous décidez d'utiliser CSimport :

   ```
   CD $BASE/utils
   ```

   Placez les profils utilisateur et de groupe à la fin de ce document dans un fichier tel que n'importe où sur le système, puis à partir du répertoire $BASE/utils, avec les démons qui s'exécutent, par exemple /etc/rc2.d/S80Cisco Secure, et en tant que racine utilisateur, exécutez CSimport avec l'option test (-t) :

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

   Cette commande teste la syntaxe des utilisateurs ; vous devez recevoir des messages tels que :

   ```
   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...
   ```

   Vous *ne* devez *pas* recevoir de messages tels que :

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

   Qu'il y ait ou non des erreurs, examinez le fichier upgrade.log afin de vous assurer que les

profils ont été extraits. Une fois les erreurs corrigées, à partir du répertoire $BASE/utils, avec les démons en cours d'exécution (/etc/rc2.d/S80Cisco Secure) et en tant qu'utilisateur root, exécutez CSimport avec l'option commit (-c) pour déplacer les utilisateurs dans la base de données :

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

Encore une fois, il ne doit pas y avoir d'erreurs sur l'écran ou dans le fichier upgrade.log.

7. Les navigateurs pris en charge sont répertoriés dans l'astuce technique Cisco Secure Compatibility. Dans le navigateur de votre PC, pointez sur la zone Cisco Secure/Solaris **http://#.#.#.#.#/cs** où **#.#.#.#** est l'adresse IP du serveur Cisco Secure/Solaris.Dans l'écran qui s'affiche, pour l'utilisateur, entrez **superutilisateur** et pour le mot de passe, saisissez **changeme**. Ne modifiez pas le mot de passe à ce stade. Vous devriez voir les utilisateurs/groupes ajoutés si vous utilisez l'importation CS à l'étape précédente ou si vous pouvez cliquer sur le bouton Parcourir **désactivé** et ajouter manuellement des utilisateurs et des groupes via l'interface utilisateur graphique.

Configuration de l'authentification

Remarque : Cette configuration de routeur a été développée sur un routeur qui exécute le logiciel Cisco IOS Version 11.3.3. Le logiciel Cisco IOS version 12.0.5.T et ultérieure affiche **tacacs de groupe** au lieu de **tacacs**.

Àce stade, configurez le routeur.

1. Exécutez Cisco Secure lors de la configuration du routeur.
   `/etc/rc0.d/K80Cisco Secure to stop the daemons.`
2. Sur le routeur, commencez à configurer TACACS+. Passez en mode enable et tapez `conf t` avant le jeu de commandes. Cette syntaxe garantit que vous n'êtes pas verrouillé hors du routeur *initialement* à condition que Cisco Secure ne soit pas en cours d'exécution. Entrez `ps -ef | grep Secure` afin de vérifier que Cisco Secure n'est pas en cours d'exécution, et tuez -9 le processus s'il est :

   ```
   !--- 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. Essayer pour être sûr que vous pouvez encore accéder au routeur avec le telnet et par le port de console avant que vous continuiez. Cisco Secure n'étant pas en cours d'exécution, le mot de passe enable doit être accepté.**Attention :** Maintenez la session du port de console active et restez en mode enable ; cette session ne devrait pas expirer. Vous commencez à limiter l'accès au routeur à ce stade et vous devez être en mesure d'apporter des modifications de configuration sans vous verrouiller.Émettez ces commandes afin de voir l'interaction serveur-routeur au niveau du routeur :

   ```
   terminal monitor
   debug aaa authentication
   ```

4. En tant que racine, démarrez Cisco Secure sur le serveur :

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

Ceci démarre les processus, mais vous voulez activer plus de débogage que configuré dans S80Cisco Secure, de sorte 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
```

Avec l'option `-x`, Cisco Secure s'exécute au premier plan afin d'observer l'interaction entre les routeurs et les serveurs. Les messages d'erreur ne doivent pas s'afficher. Le processus Cisco Secure doit démarrer et s'y suspendre en raison de l'option -x.

5. Dans une autre fenêtre, vérifiez que Cisco Secure a démarré. Entrez `ps -ef` et recherchez le processus Cisco Secure.
6. Les utilisateurs de Telnet (vty) doivent désormais s'authentifier via Cisco Secure. Avec debug sur le routeur, établissez une connexion Telnet avec le routeur à partir d'une autre partie du réseau. Le routeur doit produire une invite de nom d'utilisateur et de mot de passe. Vous devez être en mesure d'accéder au routeur avec les combinaisons d'ID utilisateur/mot de passe suivantes :

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

   Observez le serveur et le routeur où vous devriez voir l'interaction, c'est-à-dire ce qui est envoyé où, les réponses, les requêtes, etc. Corrigez tous les problèmes avant que vous continuiez.
7. Si vous souhaitez également que vos utilisateurs s'authentifient via Cisco Secure pour passer en mode enable, assurez-vous que votre session de port de console est toujours active et ajoutez cette commande au routeur :

   ```
   !--- 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. Vous devez maintenant **activer** via Cisco Secure. Avec debug sur le routeur, établissez une connexion Telnet avec le routeur à partir d'une autre partie du réseau. Lorsque le routeur demande un nom d'utilisateur/mot de passe, répondez par `opérateur/oper`.Lorsque l'utilisateur tente de passer en mode enable (niveau de privilège 15), le mot de passe « cisco » est requis. Les autres utilisateurs ne pourront pas passer en mode enable sans l'instruction de niveau de privilège (ou sans le démon Cisco Secure).Observez le serveur et le routeur où vous devriez voir l'interaction Cisco Secure, par exemple, ce qui est envoyé, où, les réponses, les requêtes, etc. Corrigez les problèmes avant de continuer.
9. Désactivez le processus Cisco Secure sur le serveur tout en étant connecté au port de console pour vous assurer que vos utilisateurs peuvent toujours accéder au routeur en cas de panne de Cisco Secure :

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

   Répétez le telnet et l'activation de l'étape précédente. Le routeur doit se rendre compte que le processus Cisco Secure ne répond pas et permettre aux utilisateurs de se connecter et de s'activer avec les mots de passe d'activation par défaut.
10. Relancez le serveur sécurisé Cisco et établissez une session Telnet sur le routeur, qui doit s'authentifier via Cisco Secure, avec l'**opérateur/opérateur** userid/mot de passe afin de vérifier l'authentification des utilisateurs du port de console via Cisco Secure. Restez connecté via une connexion Telnet au routeur et en mode enable jusqu'à ce que vous soyez sûr de pouvoir vous connecter au routeur via le port de console, par exemple,

déconnectez-vous de votre connexion d'origine au routeur via le port de console, puis reconnectez-vous au port de console. L'authentification du port de console permettant de se connecter à l'aide des précédentes combinaisons userid/mot de passe doit maintenant passer par Cisco Secure. Par exemple, userid/password **opérateur/oper** puis password **cisco** doit être utilisé pour **activer**.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Ajout d'autorisation

Ajouter l'autorisation est facultatif.

Par défaut, il y a trois niveaux de commande sur le routeur :

- Niveau de privilège 0, qui inclut la désactivation, l'activation de la sortie, l'aide et la déconnexion
- Niveau de privilège 1 : niveau normal sur une connexion Telnet et invite indiquant `routeur>`
- Niveau de privilège 15 : le niveau et l'invite enable indiquent `router#`

Comme les commandes disponibles dépendent de l'ensemble de fonctionnalités de Cisco IOS, de la version du logiciel Cisco IOS, du modèle de routeur, etc., il n'existe pas de liste complète de toutes les commandes aux niveaux 1 et 15. Par exemple, **show ipx route** n'est pas présent dans un jeu de fonctions IP uniquement, **show ip nat trans** n'est pas dans le code du logiciel Cisco IOS Version 10.2.X parce que NAT n'a pas été introduit à l'époque et **show environment** n'est pas présent dans les modèles de routeur sans alimentation et surveillance de la température.

Les commandes disponibles sur un routeur particulier à un niveau particulier peuvent-elles entrer dans un **?** à l'invite du routeur correspondant à ce niveau de privilège.

L'autorisation de port de console n'a pas été ajoutée en tant que fonctionnalité avant la mise en oeuvre de CSCdi82030. L'autorisation du port de console est désactivée par défaut pour réduire la probabilité d'être verrouillé accidentellement hors du routeur. Si un utilisateur a un accès physique au routeur par la console, l'autorisation de port de console n'est pas extrêmement pertinente. Mais l'autorisation de port de console peut être activée sous la commande **line con 0** dans une image Cisco IOS dans laquelle CSCdi82030 a été implémentée avec la commande **d'autorisation exec default|WORD**.

Procédez comme suit :

1. Le routeur peut être configuré pour autoriser des commandes via Cisco Secure à tous les niveaux ou à certains niveaux. Cette configuration du routeur permet à tous les utilisateurs d'avoir l'autorisation par-commande installée sur le serveur. Vous pouvez autoriser toutes les commandes via Cisco Secure, mais si le serveur est en panne, aucune autorisation n'est nécessaire, d'où la `valeur none`.Lorsque le serveur Cisco Secure est désactivé, entrez les commandes suivantes :Entrez cette commande afin de supprimer la condition requise pour

activer l'authentification par l'intermédiaire de Cisco Secure :

```
no aaa authentication enable default tacacs+ none
```

Entrez ces commandes afin d'exiger que l'autorisation des commandes soit effectuée 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. Pendant que le serveur Cisco Secure s'exécute, établissez une connexion Telnet au routeur avec les **lignes** userid/password**/lonepwd**. Cet utilisateur ne doit pas pouvoir exécuter d'autres commandes que :

```
show version
ping <anything>
logout
```

Les utilisateurs précédents, **adminusr/adminusr**, **opérateur/oper**, **desusr/encrypt**, devraient toujours pouvoir exécuter toutes les commandes en vertu de leur `service par défaut = permit`. En cas de problème avec le processus, passez en mode enable sur le routeur et activez le débogage d'autorisation à l'aide de cette commande :

```
terminal monitor
debug aaa authorization
```

Observez le serveur et le routeur où vous devriez voir l'interaction Cisco Secure, par exemple, ce qui est envoyé, les réponses, les requêtes, etc. Corrigez tous les problèmes avant que vous continuiez.

3. Le routeur peut être configuré pour autoriser les sessions d'exécution via Cisco Secure. La commande **aaa Authorization exec default tacacs+ none** instaure l'autorisation TACACS+ pour les sessions exec.Si vous appliquez cela, cela affecte le temps/l'heure des utilisateurs, **telnet/telnet**, **todam/todam**, **todpm/todpm** et **somerouters/somerouters**. Après avoir ajouté cette commande au routeur et Telnet au routeur en tant qu'**heure/heure** utilisateur, une session exec reste ouverte pendant une minute (set timeout = 1). L'utilisateur **telnet/telnet** entre dans le routeur mais est immédiatement envoyé à l'autre adresse (set autocmd = « telnet 171.68.118.102 »). Il est possible que les utilisateurs **todam/todam** et **todpm/todpm** soient ou ne puissent pas accéder au routeur, ce qui dépend de l'heure de la journée pendant le test. Les utilisateurs **somerouters** peuvent uniquement établir une connexion Telnet au routeur koala.rtp.cisco.com à partir du réseau 10.31.1.x. Cisco Secure tente de résoudre le nom du routeur. Si vous utilisez l'adresse IP 10.31.1.5, elle est valide si la résolution n'a pas lieu, et si vous utilisez le nom koala, elle est valide si la résolution est passée.

Ajout de comptabilité

L'ajout de la comptabilité est facultatif.

1. La comptabilisation n'a lieu que si elle est configurée dans le routeur, si le routeur exécute la version du logiciel Cisco IOS postérieure à la version 11.0 du logiciel Cisco IOS. Vous pouvez activer la comptabilité sur le routeur :

```
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+
```

Remarque : Command-accounting a été rompu, dans l'ID de bogue Cisco CSCdi44140, mais si vous utilisez une image dans laquelle ceci est corrigé, la commande-accounting peut également être activée.

2. Ajoutez le débogage d'enregistrement de comptabilité sur le routeur :
   ```
   terminal monitor
   debug aaa accounting
   ```
3. Le débogage sur la console doit afficher les enregistrements comptables qui entrent dans le serveur lorsque les utilisateurs se connectent.
4. Afin de récupérer les enregistrements comptables, en tant que racine :
   ```
   CD $BASE/utils/bin
   ./AcctExport <filename> no_truncate
   ```
   `no_truncate` signifie que les données sont conservées dans la base de données.

Ajout d'utilisateurs à distance

Procédez comme suit :

1. Assurez-vous que les autres fonctions de Cisco Secure fonctionnent avant d'ajouter des utilisateurs commutés. Si le serveur sécurisé Cisco et le modem n'ont pas fonctionné avant ce point, ils ne fonctionnent pas après ce point.
2. Ajoutez cette commande à la configuration du routeur :
   ```
   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
   ```
   Les configurations d'interface diffèrent, ce qui dépend de la façon dont l'authentification est effectuée, mais les lignes commutées sont utilisées dans cet exemple, avec les configurations suivantes :
   ```
   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. Àpartir du fichier utilisateur de Cisco Secure :chapuser—CHAP/PPP—utilisateur compose le numéro à la ligne 1 ; adresse est attribuée par **peer default ip address pool async et ip local pool async 10.6.100.101 10.6.100.103** sur le routeurchapadder—CHAP/PPP—numérotation utilisateur à la ligne 1 ; l'adresse 10.29.1.99 est attribuée par le serveurchapacl—CHAP/PPP—numérotation utilisateur à la ligne 1 ; l'adresse 10.29.1.100 est attribuée par le serveur et la liste d'accès entrante 101 est appliquée (qui doit être définie sur le routeur).papuser—PAP/PPP— numérotation utilisateur à la ligne 2 ; adresse est attribuée par **peer default ip address pool async et ip local pool async 10.6.100.101 10.6.100.103** sur le routeurpapaddr—PAP/PPP—numérotation utilisateur à la ligne 2 ; l'adresse 10.29.1.98 est attribuée par le serveurpapacl—PAP/PPP—numérotation utilisateur à la ligne 2 ; l'adresse 10.29.1.100 est attribuée par le serveur et la liste d'accès entrante 101 est appliquée, qui doit être définie sur le routeurloginauto : numérotation utilisateur à la ligne

3 ; authentification de connexion avec autocommande en ligne force l'utilisateur à se connecter à PPP et attribue l'adresse à partir du pool

4. Installation de Microsoft Windows pour tous les utilisateurs, à l'exception de la connexion utilisateur automatiqueChoisissez **Démarrer > Programmes > Accessoires > Réseau à distance**.Choisissez **Connexions > Créer une connexion**. Tapez un nom pour votre connexion.Saisissez les informations spécifiques à votre modem. Dans **Configure > General**, sélectionnez la vitesse la plus élevée de votre modem, mais ne cochez pas la case en dessous de celle-ci.Dans **Configure > Connection**, utilisez 8 bits de données, aucune parité et 1 bit d'arrêt. Les préférences d'appel sont **Attendre la tonalité avant de composer le numéro** et **Annuler l'appel s'il n'est pas connecté après 200 secondes**.Dans Advanced, sélectionnez uniquement **Hardware Flow Control** and **Modulation Type Standard**.Dans **Configurer > Options**, rien ne doit être vérifié sauf sous contrôle d'état. Click OK.Dans la fenêtre Suivant, entrez le numéro de téléphone de la destination, puis cliquez sur **Suivant**, puis sur **Terminer**.Une fois que l'icône de nouvelle connexion apparaît, cliquez dessus avec le bouton droit de la souris et sélectionnez **Propriétés**, puis cliquez sur **Type de serveur**.Choisissez **PPP : WINDOWS 95, WINDOWS NT 3.5, Internet** et ne vérifiez aucune option avancée.Dans les protocoles réseau autorisés, vérifiez au moins **TCP/IP**.Sous Paramètres TCP/IP, sélectionnez **Adresse IP attribuée au serveur**, **Adresses serveur de noms attribuées au serveur** et **Utiliser la passerelle par défaut sur le réseau distant**. Click OK.Lorsque vous double-cliquez sur l'icône pour afficher la fenêtre Se connecter à afin de composer un numéro, vous devez renseigner les champs Nom d'utilisateur et Mot de passe, puis cliquez sur **Se connecter**.
5. Installation de Microsoft Windows 95 pour l'ouverture de session utilisateurLa configuration de l'utilisateur loginauto, utilisateur d'authentification avec autocommand PPP, est identique à celle des autres utilisateurs, sauf dans la fenêtre **Configurer > Options**. Cochez la case **Monter la fenêtre du terminal après avoir composé le numéro**.Lorsque vous double-cliquez sur l'icône pour afficher la fenêtre Se connecter à pour composer le numéro, vous ne renseignez pas les champs Nom d'utilisateur et Mot de passe. Cliquez sur **Connect** et une fois la connexion au routeur établie, saisissez le nom d'utilisateur et le mot de passe dans la fenêtre noire qui s'affiche.Après l'authentification, cliquez sur **Continue(F7)**.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Serveur

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

Routeur

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**. Pour plus d'informations sur des commandes spécifiques, consultez Référence des commandes de débogage de Cisco IOS.

- **terminal monitor** - Affiche la sortie de la commande **debug** et les messages d'erreur système pour le terminal et la session en cours.
- **debug ppp negotiation** - Affiche les paquets PPP transmis lors du démarrage PPP, où les options PPP sont négociées.
- **debug ppp packet** - Affiche les paquets PPP envoyés et reçus. Cette commande affiche les vidages de paquets de bas niveau.
- **debug ppp chap** - Affiche des informations sur le trafic et les échanges dans un interréseau mettant en oeuvre le protocole CHAP (Challenge Authentication Protocol).
- **debug aaa authentication** : voyez quelles méthodes d'authentification sont utilisées et quels sont les résultats de ces méthodes.
- **debug aaa Authorization** : voir quelles méthodes d'autorisation sont utilisées et quels sont les résultats de ces méthodes.

Fichier des utilisateurs sécurisés 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
   }
   }
```

Informations connexes

- Assistance produit Cisco Secure ACS pour UNIX
- Avis de champs relatifs aux produits de sécurité (y compris Cisco Secure UNIX)