Configuration de Secure Shell sur les routeurs et les commutateurs exécutant Cisco IOS

Contenu

Introduction

Secure Shell (SSH) est un protocole qui fournit une connexion d'accès distant sécurisé aux périphériques réseau. La communication entre le client et le serveur est chiffrée à la fois dans la version SSH 1 et dans la version SSH 2. Implémentez la version SSH 2 lorsque cela est possible, car elle utilise un algorithme de chiffrement de sécurité optimisé.

Ce document discute comment configurer et mettre au point le SSH sur les Routeurs ou les

Commutateurs de Cisco qui exécutent une version du logiciel de Cisco IOS® qui prend en charge le SSH. Ce document contient des informations supplémentaires sur des versions et des images du logiciel spécifiques.

Conditions préalables

Conditions requises

L'image Cisco IOS utilisée doit être une image **k9 (crypto)** afin de prendre en charge SSH. Par exemple, **c3750e-universalk9-tar.122-35.SE5.tar** est une image k9 (crypto).

Composants utilisés

Les informations contenues dans ce document sont basées sur le logiciel Cisco IOS 3600 (C3640-IK9S-M), Version 12.2(2)T1.

SSH a été introduit dans les plates-formes et images Cisco IOS suivantes :

Le serveur SSH version 1.0 (SSH v1) a été introduit dans certaines plates-formes et images Cisco IOS à partir du logiciel Cisco IOS version 12.0.5.S.

Le client SSH a été introduit dans certaines plates-formes et images Cisco IOS à partir du logiciel Cisco IOS Version 12.1.3.T.

L'accès à la ligne de terminal SSH (également connu sous le nom de Telnet inverse) a été introduit dans certaines plates-formes et images Cisco IOS à partir du logiciel Cisco IOS version 12.2.2.T.

La prise en charge de SSH version 2.0 (SSH v2) a été introduite dans certaines plates-formes et images Cisco IOS à partir du Logiciel Cisco IOS version 12.1(19)E.

Consultez Configuration de SSH sur des commutateurs Catalyst exécutant CatOS pour plus d'informations sur la prise en charge de SSH dans les commutateurs.

Consultez l'outil Software Advisor (clients enregistrés seulement) pour une liste complète des ensembles de fonctionnalités pris en charge dans les différentes versions et sur les différentes plates-formes du logiciel Cisco IOS.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous êtes sur un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

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

SSH v1 et SSH v2

Utilisez l'outil Software Advisor Cisco (clients enregistrés seulement) afin de trouver la version de code avec la prise en charge appropriée pour SSH v1 ou SSH v2.

Diagramme du réseau

Test d'authentification

Test d'authentification sans SSH

Testez d'abord l'authentification sans SSH pour vous assurer que l'authentification fonctionne avec le routeur Carter avant d'ajouter SSH. L'authentification peut être avec un nom d'utilisateur local et un mot de passe, ou avec un serveur AAA (Authentication, Authorization, and Accounting) qui exécute TACACS+ ou RADIUS. (L'authentification via le mot de passe de ligne n'est pas possible avec SSH.) Cet exemple illustre l'authentification locale, qui vous permet d'utiliser Telnet dans le routeur avec le nom d'utilisateur « Cisco » et le mot de passe « Cisco ».

```
!--- The aaa new-model command causes the local username and password on the router !--- to be used in the absence of other AAA statements. aaa new-model username cisco password 0 cisco line vty 0 4 transport input telnet !--- Instead of aaa new-model, you can use the login local command.
```

Test d'authentification avec SSH

Pour tester l'authentification avec SSH, vous devez ajouter le code suivant aux instructions précédentes afin d'activer SSH sur Carter et tester SSH à partir du PC et des stations UNIX.

```
ip domain-name rtp.cisco.com
!--- Generate an SSH key to be used with SSH. crypto key generate rsa ip ssh time-out 60 ip ssh authentication-retries 2
```

Àce stade, la commande **show crypto key mypubkey rsa** doit afficher la clé générée. Après avoir ajouté la configuration SSH, testez votre capacité à accéder au routeur à partir du PC et de la station UNIX. Si ça ne fonctionne pas, consultez la section relative au débogage de ce document.

Paramètres de configuration facultatifs

Empêcher les connexions non SSH

Si vous voulez empêcher les connexions non SSH, ajoutez la commande **transport input ssh** sous les lignes pour limiter le routeur aux connexions SSH seulement. Les Telnets directs (non SSH) sont refusés.

```
line vty 0 4
!--- Prevent non-SSH Telnets. transport input ssh
```

Effectuez un test pour vous assurer que les utilisateurs non SSH ne peuvent pas effectuer de Telnet vers le routeur Carter.

Configurer un routeur ou un commutateur IOS comme client SSH

Il y a quatre étapes nécessaires pour activer la prise en charge de SSH sur un routeur Cisco IOS :

Configurez la commande **hostname**.

Configurez le domaine DNS.

Générez la clé SSH à utiliser.

Activez la prise en charge du transport SSH pour le terminal de type virtuel (vtys).

Si vous voulez avoir un périphérique qui joue le rôle de client SSH pour l'autre, vous pouvez ajouter SSH à un deuxième périphérique appelé Reed. Ces périphériques sont alors dans un agencement client-serveur, où Carter joue le rôle de serveur, et Reed joue le rôle de client. La configuration du client Cisco IOS SSH sur Reed est la même que celle requise pour la configuration du serveur SSH sur Carter.

```
!--- Step 1: Configure the hostname if you have not previously done so. hostname carter !--- The
 aaa new-model command causes the local username and password on the router !--- to be used in
the absence of other AAA statements. aaa new-model username cisco password 0 cisco !--- Step 2:
Configure the DNS domain of the router. ip domain-name rtp.cisco.com !--- Step 3: Generate an
SSH key to be used with SSH. crypto key generate rsa ip ssh time-out 60 ip ssh authentication-
retries 2 !--- Step 4: By default the vtys' transport is Telnet. In this case, !--- Telnet is
disabled and only SSH is supported. line vty 0 4 transport input SSH !--- Instead of aaa new-
model, you can use the login local command.
```

Émettez la commande suivante à partir du client Cisco IOS SSH (Reed) vers le serveur Cisco IOS SSH (Carter) afin de tester cela :

SSH v1 :

```
ssh -l cisco -c 3des 10.13.1.99
```

SSH v2 :

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99
```

Installez un routeur IOS en tant que serveur de SSH qui exécute l'authentification de l'utilisateur basée par RSA

Terminez-vous ces étapes afin de configurer le serveur de SSH pour exécuter l'authentification basée par RSA.

Spécifiez le nom d'hôte.

```
Router(config)#hostname <host name>
```

Définissez un nom de domaine par défaut.

```
Router(config)#ip domain-name <Domain Name>
```

Générez les paires de clés RSA.

```
Router(config)#crypto key generate rsa
```

Configurez les clés SSH-RSA pour l'authentification d'utilisateur et de serveur.

```
Router(config)#ip ssh pubkey-chain
```

Configurez le nom d'utilisateur de SSH.

```
Router(conf-ssh-pubkey)#username <user name>
```

Spécifiez la clé publique RSA du pair distant.

```
Router(conf-ssh-pubkey-user)#key-string
```

Spécifiez le type et la version de ssh key. (facultatif)

```
Router(conf-ssh-pubkey-data)#key-hash ssh-rsa <key ID>
```

Quittez le mode courant et revenez au mode d'exécution privilégié.

```
Router(conf-ssh-pubkey-data)#end
```

Remarque: Référez-vous au pour en savoir plus sécurisé de support de version 2 de shell.

Ajouter un accès à la ligne de terminal SSH

Si vous avez besoin d'une authentification de ligne de terminal SSH sortante, vous pouvez configurer et tester SSH pour les Telnets inverses sortants via Carter, qui joue le rôle de serveur de communication vers Philly.

```
ip ssh port 2001 rotary 1
line 1 16
   no exec
   rotary 1
   transport input ssh
   exec-timeout 0 0
   modem In Out
   Stopbits 1
```

Si Philly est attaché au port 2 de Carter, vous pouvez configurer SSH sur Philly via Carter à partir de Reed avec l'aide de la commande suivante :

SSH v1 :

```
ssh -c 3des -p 2002 10.13.1.99
```

SSH v2 :

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -p 2002 10.31.1.99
```

Vous pouvez utiliser la commande suivante de Solaris :

```
ssh -c 3des -p 2002 -x -v 10.13.1.99
```

Restreindre l'accès SSH à un sous-réseau

Vous devez limiter la connectivité SSH à un sous-réseau spécifique où toutes les autres tentatives SSH à partir d'IP en dehors du sous-réseau doivent être abandonnées.

Vous pouvez utiliser les étapes suivantes pour obtenir ce résultat :

Définissez une liste d'accès qui autorise le trafic à partir de ce sous-réseau spécifique.

Limitez l'accès à l'interface de ligne VTY avec une commande access-class.

Voici un exemple de configuration. Dans cet exemple, seul l'accès SSH au sous-réseau 10.10.10.0 255.255.255.0 est autorisé ; tout autre accès est refusé.

```
Router(config)#access-list 23 permit 10.10.10.0 0.0.0.255 Router(config)#line vty 5 15
Router(config-line)#transport input ssh Router(config-line)#access-class 23 in Router(config-
line)#exit
```

Remarque: La même procédure pour verrouiller l'accès SSH est également applicable sur les plates-formes de commutation.

Configurer la version SSH

Configurez SSH v1 :

```
carter(config)#ip ssh version 1
```

Configurez SSH v2 :

```
carter(config)#ip ssh version 2
```

Configurez SSH v1 et v2 :

```
carter(config)#no ip ssh version
```

Remarque: Vous recevez le message d'erreur suivant quand vous utilisez SSH v1 :

```
%SCHED-3-THRASHING: Process thrashing on watched message event.
```

Remarque: Le bogue Cisco ayant l'ID CSCsu51740 (clients enregistrés seulement) est déclaré pour ce problème. La solution de contournement consiste à configurer SSHv2.

Variations sur la sortie de la commande banner

La sortie de la commande **banner** varie entre la connexion Telnet et les différentes versions de connexions SSH. Le tableau suivant montre comment les différentes options de la commande **banner** fonctionnent avec différents types de connexions.

Option de la	Telnet	SSH v1 seulement	SSH v1 et v2	SSH v2 seulement

commande banner				
banner login	Affiché **avant** la connexion au périphérique.	Non affiché.	Affiché **avant** la connexion au périphérique.	Affiché **avant** la connexion au périphérique.
banner motd	Affiché **avant** la connexion au périphérique.	Affiché **après** la connexion au périphérique.	Affiché **après** la connexion au périphérique.	Affiché **après** la connexion au périphérique.
banner exec	Affiché **après** la connexion au périphérique.	Affiché **après** la connexion au périphérique.	Affiché **après** la connexion au périphérique.	Affiché **après** la connexion au périphérique.

Impossible d'afficher la bannière de connexion

SSH version 2 prend en charge la bannière de connexion. La bannière de connexion est affichée si le client SSH envoie le nom d'utilisateur quand il lance la session SSH avec le routeur Cisco. Par exemple, quand le client Secure Shell SSH est utilisé, la bannière de connexion est affichée. Quand le client SSH PuTTY est utilisé, la bannière de connexion n'est pas affichée. C'est parce que Secure Shell envoie le nom d'utilisateur par défaut et que PuTTY n'envoie pas le nom d'utilisateur par défaut.

Le client Secure Shell a besoin du nom d'utilisateur pour lancer la connexion au périphérique SSH. Le bouton Connect n'est pas activé si vous n'entrez pas le nom d'hôte et le nom d'utilisateur. La capture d'écran suivante montre que la bannière de connexion est affichée quand Secure Shell se connecte au routeur. Puis l'invite de mot de passe de la bannière de connexion s'affiche.

Le client PuTTY ne nécessite pas le nom d'utilisateur pour lancer la connexion SSH au routeur. La capture d'écran suivante montre que le client PuTTY se connecte au routeur et demande le nom d'utilisateur et le mot de passe. Il n'affiche pas la bannière de connexion.

Cette copie d'écran prouve que la bannière de procédure de connexion est affichée quand le mastic est configuré pour envoyer le nom d'utilisateur au routeur.

Commandes debug et show

Avant d'émettre les commandes **debug** décrites et illustrées ici, consultez Informations importantes sur les commandes Debug. Certaines commandes **show** sont prises en charge par l' Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

mettez au point les messages de débogage d'affichages de de de **sshâ d'IP** pour le SSH.

affichez que de de **sshâ** affiche les états de connexion du serveur SSH.

```
carter#show ssh Connection Version Encryption State Username 0 1.5 DES Session started cisco
```

le de de **sshâ de show ip** affiche les données de version et de configuration pour le SSH.

Connexion version 1 et aucune version 2

```
carter#show ip ssh SSH Enabled - version 1.5 Authentication timeout: 60 secs;
Authentication retries: 2
```

Connexion version 2 et aucune version 1

```
carter#show ip ssh SSH Enabled - version 2.0 Authentication timeout: 120 secs;
Authentication retries: 3
```

Connexions version 1 et version 2

```
carter#show ip ssh SSH Enabled - version 1.99 Authentication timeout: 120 secs;
Authentication retries: 3
```

Exemple de sortie de débogage

Débogage du routeur

Remarque: Une partie de cette sortie de débogage correcte est présentée sur plusieurs lignes pour des raisons d'espace.

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-1.5-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH0: sending encryption confirmation
00:23:21: SSH0: keys exchanged and encryption on
00:23:21: SSH0: SSH_CMSG_USER message received
00:23:21: SSH0: authentication request for userid cisco
00:23:21: SSH0: SSH_SMSG_FAILURE message sent
00:23:23: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:23:23: SSH0: authentication successful for cisco
00:23:23: SSH0: requesting TTY
00:23:23: SSH0: setting TTY - requested: length 24, width 80; set:
   length 24, width 80
00:23:23: SSH0: invalid request - 0x22
00:23:23: SSH0: SSH_CMSG_EXEC_SHELL message received
00:23:23: SSH0: starting shell for vty
```

Débogage du serveur

Remarque: Cette sortie a été capturée sur un ordinateur Solaris.

```
rtp-evergreen.rtp.cisco.com#ssh -c 3des -l cisco -v 10.31.1.99 rtp-evergreen#
/opt/CISssh/bin/ssh -c 3des -l cisco -v 10.13.1.99 SSH Version 1.2.26 [sparc-sun-solaris2.5.1],
protocol version 1.5. Compiled with RSAREF. rtp-evergreen: Reading configuration data
/opt/CISssh/etc/ssh_config rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0 rtp-evergreen:
Allocated local port 1023. rtp-evergreen: Connecting to 10.13.1.99 port 22. rtp-evergreen:
Connection established. rtp-evergreen: Remote protocol version 1.5, remote software version
Cisco-1.25 rtp-evergreen: Waiting for server public key. rtp-evergreen: Received server public
key (768 bits) and host key (512 bits). rtp-evergreen: Host '10.13.1.99' is known and matches
the host key. rtp-evergreen: Initializing random; seed file //.ssh/random_seed rtp-evergreen:
Encryption type: 3des rtp-evergreen: Sent encrypted session key. rtp-evergreen: Installing crc
compensation attack detector. rtp-evergreen: Received encrypted confirmation. rtp-evergreen:
Doing password authentication. cisco@10.13.1.99's password: rtp-evergreen: Requesting pty. rtp-
evergreen: Failed to get local xauth data. rtp-evergreen: Requesting X11 forwarding with
authentication spoofing. Warning: Remote host denied X11 forwarding, perhaps xauth program could
not be run on the server side. rtp-evergreen: Requesting shell. rtp-evergreen: Entering
interactive session.
```

Causes de problèmes potentiels

Les sections suivantes présentent un exemple de sortie de débogage provenant de plusieurs configurations incorrectes.

SSH à partir d'un client SSH non compilé avec Data Encryption Standard (DES)

Débogage de Solaris

```
rtp-evergreen#/opt/CISssh/bin/ssh -c des -l cisco -v 10.13.1.99 SSH Version 1.2.26 [sparc-sun-
solaris2.5.1], protocol version 1.5. Compiled with RSAREF. rtp-evergreen: Reading configuration
data /opt/CISssh/etc/ssh_config rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0 rtp-
evergreen: Allocated local port 1023. rtp-evergreen: Connecting to 10.13.1.99 port 22. rtp-
evergreen: Connection established. rtp-evergreen: Remote protocol version 1.5, remote software
version Cisco-1.25 rtp-evergreen: Waiting for server public key. rtp-evergreen: Received server
public key (768 bits) and host key (512 bits). rtp-evergreen: Host '10.13.1.99' is known and
matches the host key. rtp-evergreen: Initializing random; seed file //.ssh/random_seed rtp-
evergreen: Encryption type: des rtp-evergreen: Sent encrypted session key. cipher_set_key:
unknown cipher: 2
```

Débogage du routeur

```
00:24:41: SSH0: Session terminated normally
00:24:55: SSH0: starting SSH control process
00:24:55: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:24:55: SSH0: protocol version id is - SSH-1.5-1.2.26
00:24:55: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:24:55: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:24:55: SSH: RSA decrypt started
00:24:56: SSH: RSA decrypt finished
00:24:56: SSH: RSA decrypt started
```

```
00:24:56: SSH: RSA decrypt finished
00:24:56: SSH0: sending encryption confirmation
00:24:56: SSH0: Session disconnected - error 0x07
```

Mot de passe incorrect

Débogage du routeur

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-1.5-1.2.26
00:26:52: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

Envoi, par un client SSH, d'un chiffrement (Blowfish) non pris en charge

Débogage du routeur

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-1.5-W1.0
00:39:26: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

Obtenir le "%SSH-3-PRIVATEKEY : Incapable de récupérer la clé privée RSA pour la » erreur

Si vous recevez ce message d'erreur, il peut sont provoqué par en raison de n'importe quel changement du nom de domaine ou du nom d'hôte. Afin de résoudre ceci, essayez ces contournements.

Mettez à zéro les clés RSA et régénérez les clés.

```
crypto key zeroize rsa label key_name
crypto key generate rsa label key_name modulus key_size
```

Si le contournement précédent ne fonctionne pas, essayez ces étapes :

Mettez à zéro toutes les clés RSA.

Rechargez le périphérique.

Créez les nouvelles clés étiquetées pour le SSH.

L'ID de bogue Cisco CSCsa83601 (clients enregistrés seulement) a été classé pour adresser ce comportement.

Conseils de dépannage

Si vos commandes de configuration SSH sont rejetées comme étant des commandes illégales, vous n'avez pas correctement généré une paire de clés RSA pour votre routeur. Vérifiez que vous avez spécifié un nom d'hôte et un domaine. Utilisez ensuite la commande **crypto key generate rsa** pour générer une paire de clés RSA et activer le serveur SSH.

Quand vous configurez la paire de clés RSA, vous pouvez rencontrer les messages d'erreur suivant :

```
No hostname specified
```

Vous devez configurer un nom d'hôte pour le routeur à l'aide de la commande de configuration globale **hostname**.

```
No domain specified
```

Vous devez configurer un domaine hôte pour le routeur à l'aide de la commande de configuration globale **ip domain-name**.

Le nombre de connexions SSH autorisées est limité au nombre maximal de vtys configurés pour le routeur. Chaque connexion SSH utilise une ressource vty.

SSH utilise la sécurité locale ou le protocole de sécurité qui est configuré via AAA sur votre routeur pour l'authentification des utilisateurs. Quand vous configurez AAA, vous devez vous assurer que la console n'est pas en cours d'exécution sous AAA en appliquant un mot clé en mode de configuration globale pour désactiver AAA sur la console.

```
No SSH server connections running.
```

```
carter#show ssh %No SSHv2 server connections running. %No SSHv1 server connections running.
```

Cette sortie suggère que le serveur SSH est désactivé ou pas correctement activé. Si vous avez déjà configuré SSH, il est recommandé de reconfigurer le serveur SSH sur le périphérique. Effectuez les étapes suivantes afin de reconfigurer le serveur SSH sur le périphérique.

Supprimez la paire de clés RSA. Une fois la paire de clés RSA supprimée, le serveur SSH est automatiquement désactivé.

```
carter(config)#crypto key zeroize rsa
```

Remarque: Il est important de générer une paie de clés avec une taille de bits d'au moins 768 quand vous activez SSH v2.

Attention : Une fois votre configuration enregistrée, cette commande ne peut pas être annulée, et après avoir supprimé les clés RSA, vous ne pouvez utiliser des certificats ou la CA, ou participer à des échanges de certificats avec d'autres homologues de sécurité IP (IPSec) que si vous reconfigurez l'interopérabilité de CA en régénérant des clés RSA, en obtenant le certificat de la CA et en redemandant votre propre certificat. Consultez crypto key zeroize rsa - Référence des commandes de sécurité Cisco IOS, Version 12.3 pour plus d'informations sur cette commande.

Reconfigurez le nom d'hôte et le nom de domaine du périphérique.

```
carter(config)#hostname hostname carter(config)#ip domain-name domainname
```

Générez une paire de clés RSA pour votre routeur, ce qui active automatiquement SSH.

```
carter(config)#crypto key generate rsa
```

Consultez crypto key generate rsa - Référence des commandes de sécurité Cisco IOS, version 12.3 pour plus d'informations sur l'utilisation de cette commande.

Remarque: Vous pouvez recevoir le message d'erreur SSH2 0: Unexpected mesg type received en raison d'un paquet reçu qui n'est pas compréhensible par le routeur. Augmentez la longueur de clé tandis que vous générez des clés RSA pour SSH afin de résoudre ce problème.

Configurez le serveur SSH. Afin d'activer et configurer un routeur de Cisco/commutateur pour le serveur de SSH, vous pouvez configurer des paramètres de SSH. Si vous ne configurez pas de paramètres SSH, les valeurs par défaut sont utilisées.

ip ssh {[timeout seconds] | [[authentication-retries integer]} `carter(config)# ip ssh`

Consultez ip ssh - Référence des commandes de sécurité Cisco IOS, Version 12.3 pour plus d'informations sur l'utilisation de cette commande.

Informations connexes

- Comment configurer SSH sur les commutateurs Catalyst qui exécutent CatOS
- Prise en charge de Secure Shell version 2
- Pages d'assistance sur les produits SSH
- Support et documentation techniques - Cisco Systems