Secure Shell configureren op routers en switches die Cisco IOS draaien

Inhoud

Inleiding

Secure Shell (SSH) is een protocol waarmee een beveiligde verbinding wordt opgezet voor externe toegang tot netwerkapparaten. Communicatie tussen client en server is versleuteld in zowel SSH-versie 1 als SSH-versie 2. Implementeer waar mogelijk SSH-versie 2 omdat hierin een encryptie-algoritme met betere security wordt gebruikt.

In dit document wordt beschreven hoe u SSH kunt configureren en debuggen op Cisco-routers of

-switches waarop een softwareversie van Cisco IOS® wordt gebruikt die SSH ondersteunt. Dit document bevat meer informatie over specifieke versies en software-images.

Voorwaarden

Vereisten

De gebruikte Cisco IOS-image moet een **k9 (crypto)-image zijn om SSH te ondersteunen. c3750e-universalk9-tar.122-35.SE5.tar is bijvoorbeeld een k9 (crypto)-image.**

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS 3600-software (C3640-IK9S-M), release 12.2(2)T1.

SSH werd geïntroduceerd in de volgende Cisco IOS-platforms en -images:

SSH-server versie 1.0 (SSH v1) werd geïntroduceerd in enkele Cisco IOS-platforms en -images vanaf Cisco IOS-softwarerelease 12.0.5.S.

SSH-client werd geïntroduceerd in enkele Cisco IOS-platforms en -images vanaf Cisco IOS-softwarerelease 12.1.3.T.

Toegang via SSH-terminallijn (omgekeerde Telnet) werd geïntroduceerd in enkele Cisco IOS-platforms en -images vanaf Cisco IOS-softwarerelease 12.2.2.T.

Ondersteuning voor SSH-versie 2.0 (SSH v2) werd geïntroduceerd in enkele Cisco IOS-platforms en -images vanaf Cisco IOS-softwarerelease 12.1(19)E.

Raadpleeg How to Configure SSH on Catalyst Switches Running CatOS (SSH configureren op Catalyst-switches die CatOS gebruiken) voor meer informatie over SSH-ondersteuning op switches.

Raadpleeg Software Advisor (alleen voor geregistreerde klanten) voor een volledige lijst van functiesets die in verschillende Cisco IOS-softwarereleases en op verschillende platforms worden ondersteund.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen voordat u deze gebruikt.

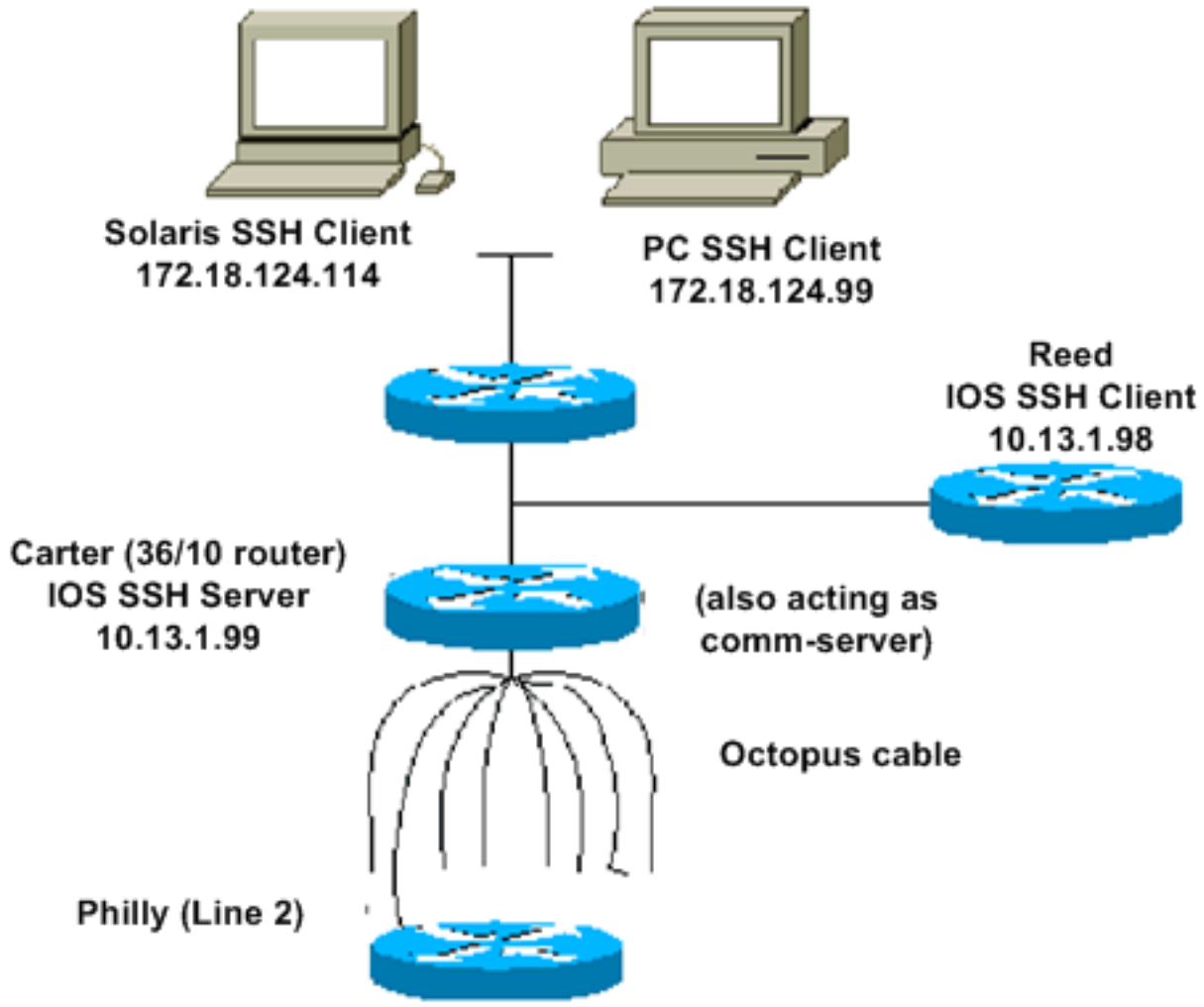
Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

SSH v1 vergeleken met SSH v2

Gebruik de tool Cisco Software Advisor (alleen voor geregistreerde klanten) om de codeversie met toepasselijke ondersteuning voor SSH v1 of SSH v2 te bepalen.

Netwerkdiagram



Verificatie testen

Verificatietest zonder SSH

Test de verificatie eerst zonder SSH om er zeker van te zijn dat verificatie werkt met de router Carter voordat u SSH toevoegt. Verificatie kan worden uitgevoerd met een lokale gebruikersnaam en wachtwoord of met een verificatie-, autorisatie- en accounting-server (AAA) die TACACS+ of RADIUS uitvoert (Verificatie via het lijnwachtwoord is niet mogelijk bij SSH.) In dit voorbeeld wordt lokale verificatie getoond waarmee u via Telnet toegang krijgt tot de router met gebruikersnaam ‘cisco’ en wachtwoord ‘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.
```

Verificatietest met SSH

Om verificatie met SSH te testen, moet u de vorige instructies uitbreiden om SSH in te schakelen op de router Carter en SSH te testen vanaf pc's en UNIX-stations.

```
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
```

De opdracht **show crypto key mypubkey rsa moet nu de gegenereerde sleutel tonen.** Nadat u de SSH-configuratie heeft toegevoegd, kunt u testen of u de router kunt benaderen vanaf pc's en UNIX-stations. Zie de sectie Voorbeeld van output van foutopsporing in dit document als het niet werkt.

Optionele configuratie-instellingen

Niet-SSH-verbindingen voorkomen

Als u niet-SSH-verbindingen wilt voorkomen, voegt u onder de regels de opdracht **transport input ssh toe om de router te beperken tot alleen SSH-verbindingen.** Normale Telnet-verbindingen (niet-SSH) worden geweigerd.

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

Test om er zeker van te zijn dat niet-SSH-gebruikers geen toegang via Telnet kunnen krijgen tot de router Carter.

Een IOS-router of -switch instellen als SSH-client

Er zijn vier stappen vereist om SSH-ondersteuning in te schakelen op een Cisco IOS-router:

Configureer de opdracht **hostname.**

Configureer het DNS-domein.

Genereer de te gebruiken SSH-sleutel.

Schakel ondersteuning van SSH-transport in voor virtuele terminals (VTY's).

Als u wilt dat één apparaat fungeert als SSH-client voor het andere apparaat, kunt u SSH toevoegen aan een tweede apparaat met de naam Reed. Deze apparaten vormen dan een client/server-combinatie waarbij Carter fungeert als de server en Reed als de client. De SSH-clientconfiguratie van Cisco IOS op Reed is gelijk aan de configuratie die vereist is voor de SSH-serverconfiguratie op 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.
```

Geef SSH de volgende opdracht van Cisco IOS SSH-client (Reed) naar Cisco IOS SSH-server (Carter) om dit te testen:

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
```

Een IOS-router instellen als SSH-server die op RSA gebaseerde gebruikersverificatie uitvoert

Voer de volgende stappen uit om de SSH-server zodanig te configureren dat deze op RSA gebaseerde verificatie uitvoert.

Geef de hostnaam op.

```
Router(config)#hostname
```

Definieer een standaarddomeinnaam.

```
Router(config)#ip domain-name
```

Genereer RSA-sleutelparen.

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

Configureer SSH-RSA-sleutels voor verificatie van gebruikers en de server.

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

Configureer de SSH-gebruikersnaam.

```
Router(conf-ssh-pubkey)#username
```

Geef de openbare RSA-sleutel van de externe peer op.

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

Geef het type en de versie van de SSH-sleutel op. (Optioneel)

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

Sluit de huidige modus af en keer terug naar de modus Privileged EXEC.

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

Opmerking: Raadpleeg Ondersteuning voor Secure Shell (versie 2) voor meer informatie.

Toegang via SSH-terminallijn toevoegen

Als verificatie van de uitgaande SSH-terminallijn nodig is, kunt u SSH configureren en testen voor uitgaande omgekeerde Telnet-verbindingen via Carter die fungeert als communicatieserver voor 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
```

Als Philly is verbonden met poort 2 van Carter, kunt u SSH vanaf Reed via Carter naar Philly configureren met de volgende opdracht:

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
```

U kunt de volgende Solaris-opdracht gebruiken:

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

SSH-toegang tot een subnet beperken

U moet SSH-connectiviteit met een specifiek subnetwerk beperken wanneer alle andere SSH-pogingen van IP-adressen buiten het subnetwerk moeten worden afgewezen.

U kunt de volgende stappen nemen om dit te bewerkstelligen:

Definieer een toegangslijst die het verkeer afkomstig van dat specifieke subnetwerk toelaat.

Beperk toegang tot de VTY-lijninterface met de opdracht `access-class`.

Hierna volgt een configuratievoorbeeld. In dit voorbeeld is alleen SSH-toegang tot het subnet 10.10.10.0 met subnetmasker 255.255.255.0 toegestaan; toegang tot andere adressen wordt geweigerd.

```
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
```

Opmerking: Dezelfde procedure om de SSH-toegang af te sluiten is ook van toepassing op switches.

De SSH-versie configureren

Configureer SSH v1:

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

Configureer SSH v2:

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

Configureer SSH v1 en v2:

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

Opmerking: U ontvangt deze foutmelding als u SSHv1 gebruikt:

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

Opmerking: Cisco bug-ID CSCsu51740 (alleen geregistreerde klanten) is voor deze kwestie ingediend. Dit kan worden omzeild door SSH v2 te configureren.

Variaties in output van opdracht banner

De output van de opdracht **banner verschilt tussen Telnet- en verschillende versies van SSH-verbindingen.** In deze tabel wordt aangegeven hoe de verschillende opties van de opdracht **banner werken bij verschillende typen verbindingen.**

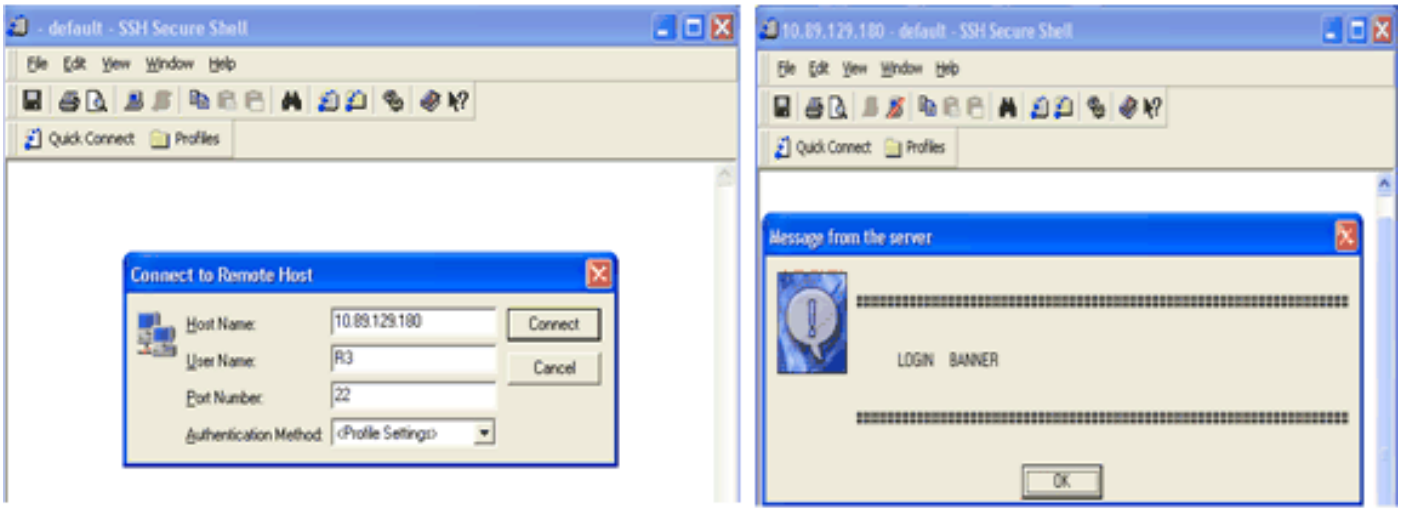
Optie van opdracht banner	Telnet	Alleen SSH v1	SSH v1 en v2	Alleen SSH v2
banner	Getoond voordat bij	Niet getoond.	Getoond voordat bij	Getoond voordat bij

login	het apparaat is aangemeld.		het apparaat is aangemeld.	het apparaat is aangemeld.
banner motd	Getoond voordat bij het apparaat is aangemeld.	Getoond nadat bij het apparaat is aangemeld.	Getoond nadat bij het apparaat is aangemeld.	Getoond nadat bij het apparaat is aangemeld.
banner exec	Getoond nadat bij het apparaat is aangemeld.	Getoond nadat bij het apparaat is aangemeld.	Getoond nadat bij het apparaat is aangemeld.	Getoond nadat bij het apparaat is aangemeld.

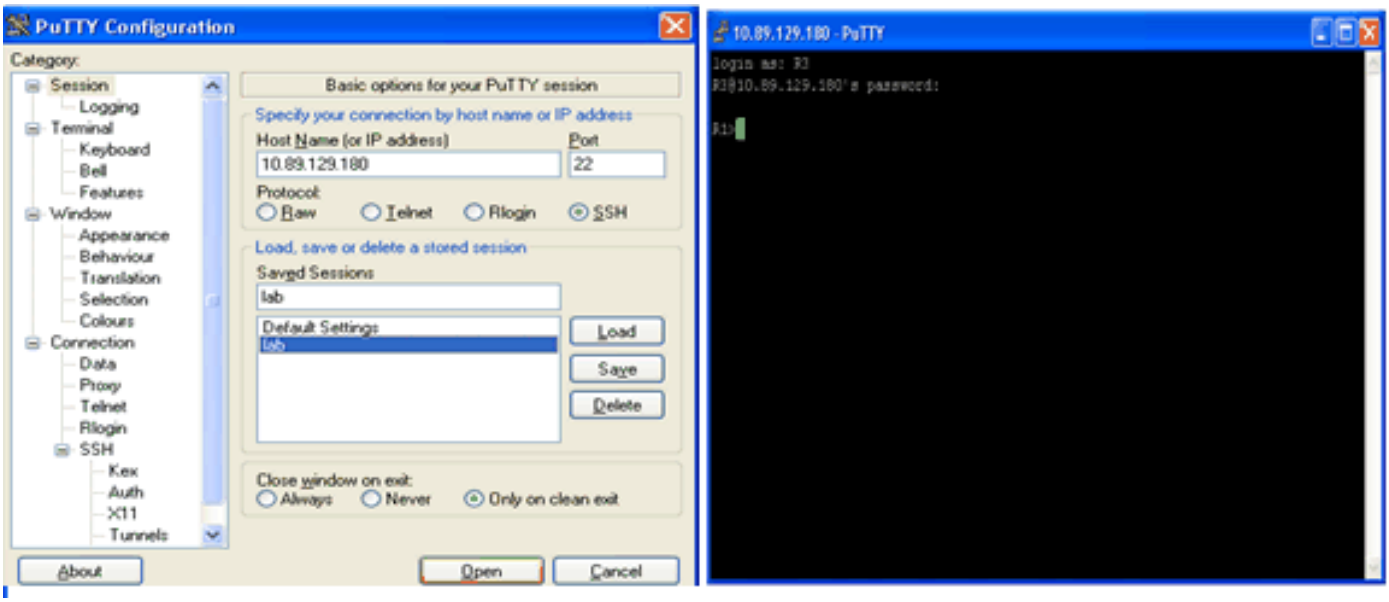
Kan aanmeldingsbanner niet tonen

SSH-versie 2 ondersteunt de aanmeldingsbanner. De aanmeldingsbanner wordt getoond wanneer de SSH-client de gebruikersnaam verzendt bij het initiëren van de SSH-sessie met de Cisco-router. Wanneer bijvoorbeeld de Secure Shell-opdracht ‘ssh client’ wordt gebruikt, wordt de aanmeldingsbanner getoond. Wanneer de PuTTY-opdracht ‘ssh client’ wordt gebruikt, wordt de aanmeldingsbanner niet getoond. Dat komt doordat Secure Shell standaard de gebruikersnaam verzendt en PuTTY niet.

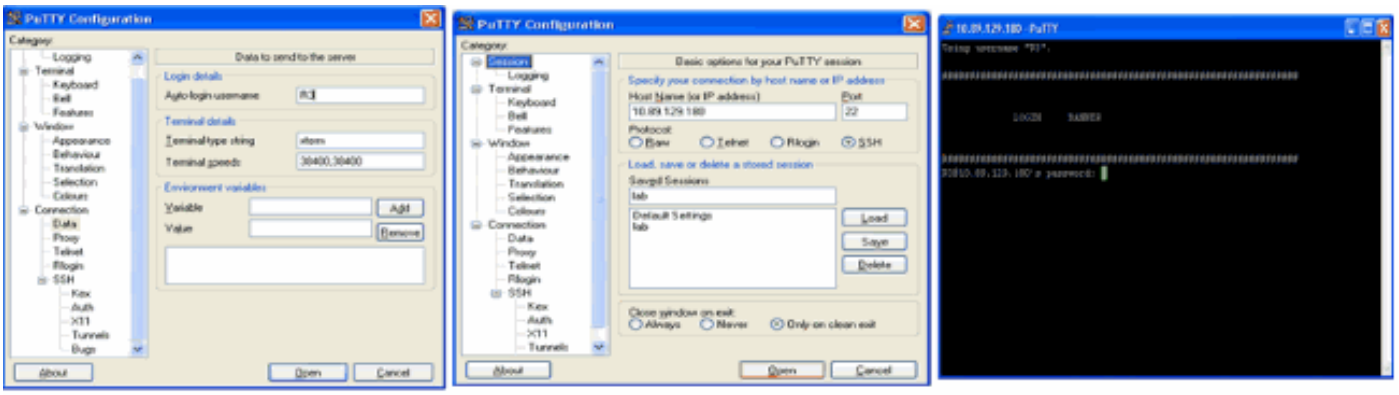
De Secure Shell-client heeft de gebruikersnaam nodig om de verbinding met het apparaat met ingeschakelde SSH te initiëren. De knop om te verbinden is niet actief wanneer u de hostnaam en gebruikersnaam niet opgeeft. In deze schermopname is te zien dat de aanmeldingsbanner wordt getoond wanneer Secure Shell verbinding maakt met de router. Vervolgens wordt gevraagd naar het wachtwoord van de aanmeldingsbanner.



De PuTTY-client heeft de gebruikersnaam niet nodig om de SSH-verbinding met de router te initiëren. In deze schermopname is te zien dat de PuTTY-client verbinding maakt met de router en dat wordt gevraagd naar gebruikersnaam en wachtwoord. De aanmeldingsbanner wordt niet getoond.



In deze schermopname is te zien dat de aanmeldingsbanner wordt getoond wanneer PuTTY is geconfigureerd om de gebruikersnaam naar de router te verzenden.



Category → Connection → Data

Opdrachten met debug en show

Voordat u de beschreven en getoonde opdrachten met **debug opgeeft, moet u de TechNote** Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) raadplegen. Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

debug ip ssh – toont foutopsporingsberichten voor SSH.

show ssh – toont de status van SSH-serververbindingen.

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

show ip ssh – toont de versie en configuratiegegevens voor SSH.

Verbinding via versie 1 en geen versie 2

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

Verbinding via versie 2 en geen versie 1

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

Verbindingen via versie 1 en versie 2

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

Voorbeeld van output van foutopsporing

Foutopsporing op router

Opmerking: Sommige van deze goede debug-uitvoer zijn vanwege ruimtelijke overwegingen verpakt in meerdere regels.

```
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
```

Foutopsporing op server

Opmerking: deze uitvoer werd opgenomen op een Solaris-machine.

```
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.
```

Wat er kan misgaan

De volgende secties bevatten voorbeelden van output van foutopsporing bij diverse onjuiste configuraties.

SSH van een SSH-client niet gecompileerd met Data Encryption Standard (DES)

Foutopsporing op 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
```

Foutopsporing op router

```
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
```

Onjuist wachtwoord

Foutopsporing op router

```
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
```

SSH-client stuurt niet-ondersteund algoritme (Blowfish)

Foutopsporing op router

```
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
```

Foutmelding '%SSH-3-PRIVATEKEY: Unable to retrieve RSA private key for' (Kan

persoonlijke RSA-sleutel niet ophalen voor)

Als u deze foutmelding krijgt, is dat mogelijk het gevolg van een wijziging in de domeinnaam of hostnaam. Probeer deze tijdelijke oplossingen om dit probleem op te lossen.

Zet alle RSA-sleutels op nul en genereer de sleutels opnieuw.

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

Als de vorige tijdelijke oplossing niet werkt, voert u de volgende stappen uit:

Zet alle RSA-sleutels op nul.

Laad het apparaat opnieuw.

Maak nieuwe gelabelde sleutels voor SSH.

Cisco-bug-id CSCsa83601 (alleen voor geregistreerde klanten) is voor dit gedrag vastgelegd.

Tips bij het oplossen van problemen

Als de SSH-configuratieopdrachten worden afgewezen als ongeldig, is er geen RSA-sleutelpaar voor de router gegenereerd. Zorg dat u een hostnaam en een domeinnaam opgeeft. Gebruik vervolgens de opdracht **crypto key generate rsa om een RSA-sleutelpaar te genereren en de SSH-server in te schakelen.**

Wanneer u het RSA-sleutelpaar configureert, kunnen de volgende foutmeldingen worden getoond:

```
No hostname specified (Geen hostnaam opgegeven)
```

U moet een hostnaam voor de router configureren met de Global Configuration-opdracht **hostname.**

```
No domain specified (Geen domein opgegeven)
```

U moet een hostdomein voor de router configureren met de Global Configuration-opdracht **ip domain-name.**

Het aantal toegestane SSH-verbindingen is beperkt tot het maximale aantal VTY's dat voor de router is geconfigureerd. Elke SSH-verbinding gebruikt een VTY-bron.

SSH gebruikt lokale security of het security protocol dat is geconfigureerd via AAA op de

router voor gebruikersverificatie. Wanneer u AAA configureert, moet u ervoor zorgen dat op de console AAA niet actief is door in de modus Global Configuration een trefwoord op te geven om AAA op de console uit te schakelen.

```
Er zijn geen SSH-serververbindingen actief.
```

```
carter#show ssh

%No SSHv2 server connections running.
%No SSHv1 server connections running.
```

Deze output geeft aan dat de SSH-server is uitgeschakeld of niet goed is ingeschakeld. Als u SSH al heeft geconfigureerd, is het raadzaam de SSH-server van het apparaat opnieuw te configureren. Voer de volgende stappen uit om de SSH-server van het apparaat opnieuw te configureren.

Verwijder het RSA-sleutelpaar. Nadat het RSA-sleutelpaar is verwijderd, wordt de SSH-server automatisch uitgeschakeld.

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

Opmerking: het is belangrijk om een key-pair te genereren met minimaal 768 als bit size wanneer u SSH v2 instelt.

Waarschuwing: deze opdracht kan niet ongedaan worden gemaakt nadat u de configuratie hebt opgeslagen, en nadat de RSA-toetsen zijn verwijderd, kunt u geen certificaten of de CA gebruiken of deelnemen aan certificeringsuitwisselingen met andere IP Security (IPSec) peers tenzij u de CA-interoperabiliteit opnieuw configureren door RSA-toetsen te regenereren, het CA-certificaat te verkrijgen en uw eigen certificaat opnieuw te vragen.Raadpleeg crypto-encryptie-sleutel RSA - Cisco IOS security opdracht, opdracht, release 1 2.3 voor meer informatie over deze opdracht.

Configureer de hostnaam en domeinnaam van het apparaat opnieuw.

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

Genereer een RSA-sleutelpaar voor de router waarmee SSH automatisch wordt ingeschakeld.

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

Raadpleeg crypto key generate rsa – Cisco IOS Security Command Reference, Release 12.3 voor meer informatie over deze opdracht.

Opmerking: U kunt de `SSH2 0` ontvangen: `Unexpected mesg type received (Onverwacht`

`berichttype ontvangen) krijgen wanneer een pakket wordt ontvangen dat de router niet kan verwerken.` Vergroot de sleutellengte tijdens het genereren van RSA-sleutels voor SSH om dit probleem op te lossen.

Configureer de SSH-server. Om een Cisco-router/switch te configureren en in te schakelen als SSH-server kunt u SSH-parameters configureren. Als u de SSH-parameters niet configureert, worden de standaardwaarden gebruikt.

ip ssh {[timeout *seconden*] | [authenticatie *integers*]}

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

Raadpleeg ip ssh – Cisco IOS Security Command Reference, Release 12.3 voor meer informatie over deze opdracht.

Gerelateerde informatie

- How to Configure SSH on Catalyst Switches Running CatOS (SSH configureren op Catalyst-switches die CatOS gebruiken)
- Secure Shell Version 2 Support (Ondersteuning voor Secure Shell, versie 2)
- Productondersteuningspagina voor SSH
- Technische ondersteuning en documentatie – Cisco Systems