Häufig gestellte Fragen zu Secure Shell (SSH)

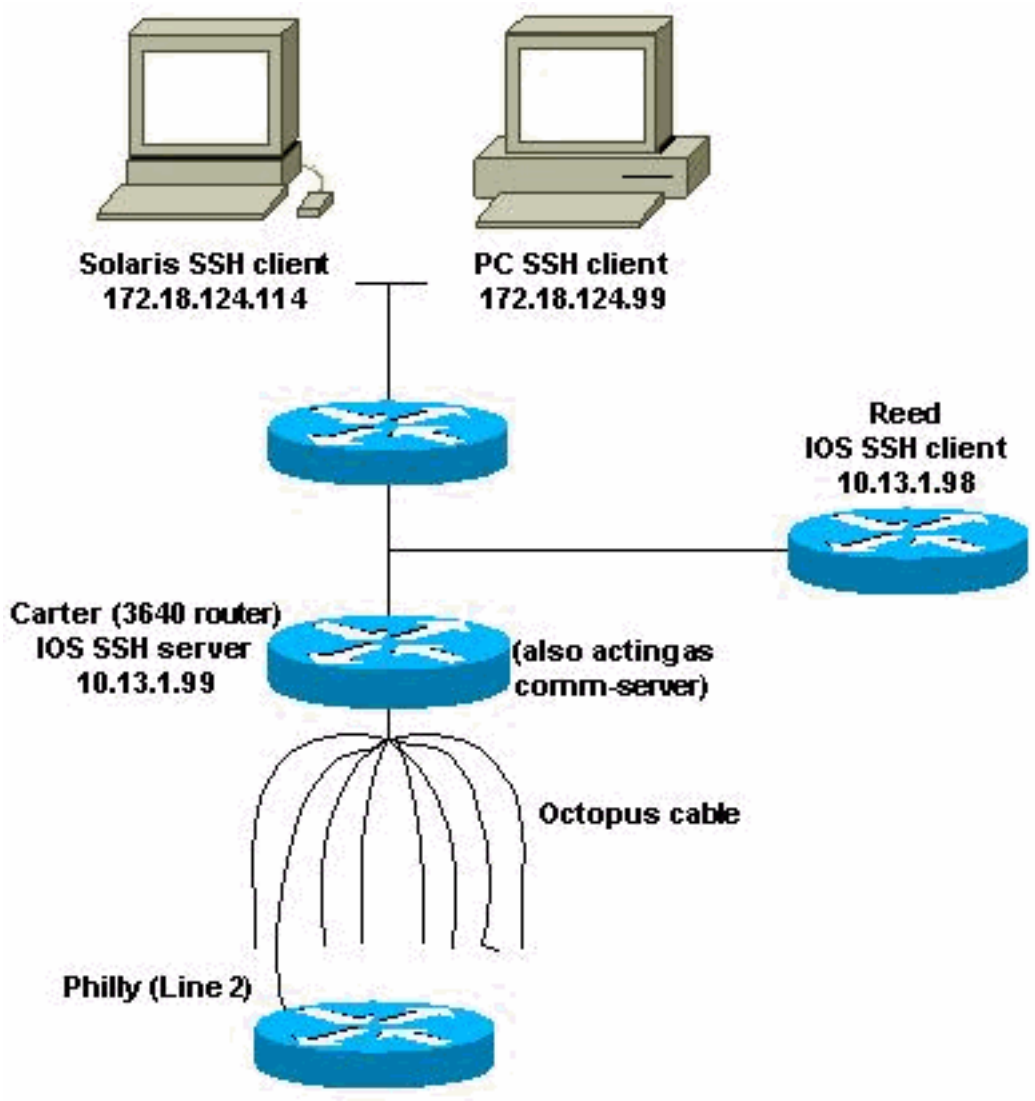
Inhalt

Einführung

Dieses Dokument beantwortet die am häufigsten gestellten Fragen (FAQs) im Zusammenhang mit Secure Shell (SSH). Der Cisco IOS® SSH-Code ist der ursprüngliche Cisco Code.

Wie konfiguriere ich den Zugriff auf SSH-Terminalleitungen (auch Reverse-Telnet genannt)?

Dies wurde erstmals auf einigen Plattformen der Cisco IOS Software-Version 12.2.2.T eingeführt.




```
Router(config)#line line-number [ending-line-number]
Router(config-line)#no exec
Router(config-line)#login {local | authentication listname
Router(config-line)#rotary group
Router(config-line)#transport input {all | ssh}
Router(config-line)#exit
Router(config)#ip ssh port portnum rotary group

!--- Line 1 SSH Port Number 2001 line 1 no exec login authentication default rotary 1 transport
input ssh !--- Line 2 SSH Port Number 2002 line 2 no exec login authentication default rotary 2
transport input ssh !--- Line 3 SSH Port Number 2003 line 3 no exec login authentication default
rotary 3 transport input ssh ip ssh port 2001 rotary 1 3
```

Befehlsreferenz

ip ssh port
ip ssh port *portnum* **rotary** *group*
no ip ssh port *portnum* **rotary** *group*

- portnum - Gibt den Port an, mit dem SSH eine Verbindung herstellen muss, z. B. 2001.
- Rundgruppe - Gibt das definierte Drehfeld an, das nach einem gültigen Namen suchen muss.

Wird SSH auf dem Catalyst 2900 unterstützt?

Nein.

Wie kann ich feststellen, welche Plattformen und Versionen von Code SSH unterstützen?

Siehe Feature Navigator (nur registrierte Kunden) und geben Sie die **SSH**-Funktion an.

Wenn ich versuche, bestimmte SSH-Befehle von meinem Router zu entfernen, wird ich weiterhin aufgefordert, RSA-Schlüssel zu erstellen, um SSH zu aktivieren. Warum ist das so?

Ein Beispiel für dieses Problem ist hier dargestellt:

```
804#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
804(config)#no ip ssh time-out 120
Please create RSA keys to enable SSH.
804(config)#no ip ssh authen
Please create RSA keys to enable SSH.
804(config)
```

Sie haben die Cisco Bug-ID CSCdv70159 erhalten (nur registrierte Kunden).

Unterstützt Cisco IOS SSH Version 2 DSS (Digital Signature Standard)?

Cisco IOS SSH Version 2 unterstützt DSS nicht.

Unterstützt der Cisco IOS SSH-Server die Agentenweiterleitung?

Cisco IOS SSH unterstützt keine Agentenweiterleitung. Sie ist mit allen kommerziellen SSH-Implementierungen kompatibel.

Welche Client-Authentifizierungsmechanismen werden auf dem Cisco IOS SSH-Server unterstützt?

Cisco IOS SSH Version 2 (SSHv2) unterstützt tastateinteraktive und kennwortbasierte Authentifizierungsverfahren. Zusätzlich zu diesen Authentifizierungsmethoden unterstützt die Funktion SSHv2 Enhancements for RSA Keys (verfügbar in Version 15.0(1)M und höher der Cisco IOS-Software) die RSA-basierte Authentifizierung von öffentlichen Schlüsseln für Client und Server. Weitere Informationen zu den vom Cisco IOS SSH-Server unterstützten Authentifizierungsmechanismen finden Sie unter Secure Shell Version 2 Support.

Was bewirkt der Fehler `Lokal: Beschädigte Prüfbytes im` Eingabemaar?

Beschädigte Checkbyte bedeuten, dass das empfangene SSH-Paket seine Integritätsprüfung nicht bestanden hat. Dies liegt in der Regel an der falschen Entschlüsselung. Dies liegt auch daran, dass ein falscher Schlüssel verwendet wird. Der falsche Schlüssel wird durch das Verwerfen eines verschlüsselten SSH-Pakets verursacht. Sie haben entweder ein verschlüsseltes Paket verworfen, das hätte gesendet werden sollen, oder ein empfangenes verschlüsseltes Paket verworfen, das hätte entschlüsselt werden sollen.

Unterstützt Cisco IOS SSH mit Blowfish-Chiffre?

Cisco IOS unterstützt SSH nicht mit Blowfish-Chiffre. Wenn ein SSH-Client eine solche nicht unterstützte Chiffre sendet, zeigt der Router die in SSH-Client erwähnten Debugmeldungen an (Blowfish-Chiffre).

Wenn ich versuche, RSA-Schlüssel für den SSH-Zugriff auf einem Router mit dem Befehl crypto key generate rsa im Konfigurationsmodus zu generieren, erhalte ich den folgenden Fehler: `% Ungültige Eingabe erkannt an '^' Marker.`. Der Router kann die RSA-Schlüssel nicht generieren, um den SSH-Zugriff für den Router zu aktivieren. Wie wird dieser Fehler behoben?

Dieser Fehler wird angezeigt, wenn das auf dem Router verwendete Image den Befehl **crypto key generate rsa** nicht unterstützt. Dieser Befehl wird nur in Sicherheitsabbildern unterstützt. Um diesen Fehler zu beheben, verwenden Sie das Sicherheits-Image der entsprechenden Serie des verwendeten Cisco IOS-Routers.

Unterstützen Krypto-Images Strong Chipher für die Verwendung von SSH mit Chiffren wie 3DES oder AES?

Ja. Nur Krypto-Bilder unterstützen Strong Chipher. Um SSH mit Chiffren wie 3DES oder AES zu verwenden, müssen auf Ihrem Cisco Gerät Crypto-Images vorhanden sein.

Diese Meldungen werden in den Protokollen angezeigt, wenn ich versuche, SSH auf einem Router zu konfigurieren: `SSH2 13: RSA_sign: privater Schlüssel nicht gefunden` und `SSH2 13: Signaturerstellung fehlgeschlagen, Status -1.` Wie wird das gelöst?

Diese Protokollmeldungen werden aufgrund der Cisco Bug-IDs CSCsa83601 (nur registrierte Kunden) und CSCtc41114 (nur registrierte Kunden) angezeigt. Weitere Informationen finden Sie in diesen Bugs.

Zugehörige Informationen

- SSH-Support-Seite

- Technischer Support und Dokumentation - Cisco Systems