Secure Shell（SSH）に関する FAQ

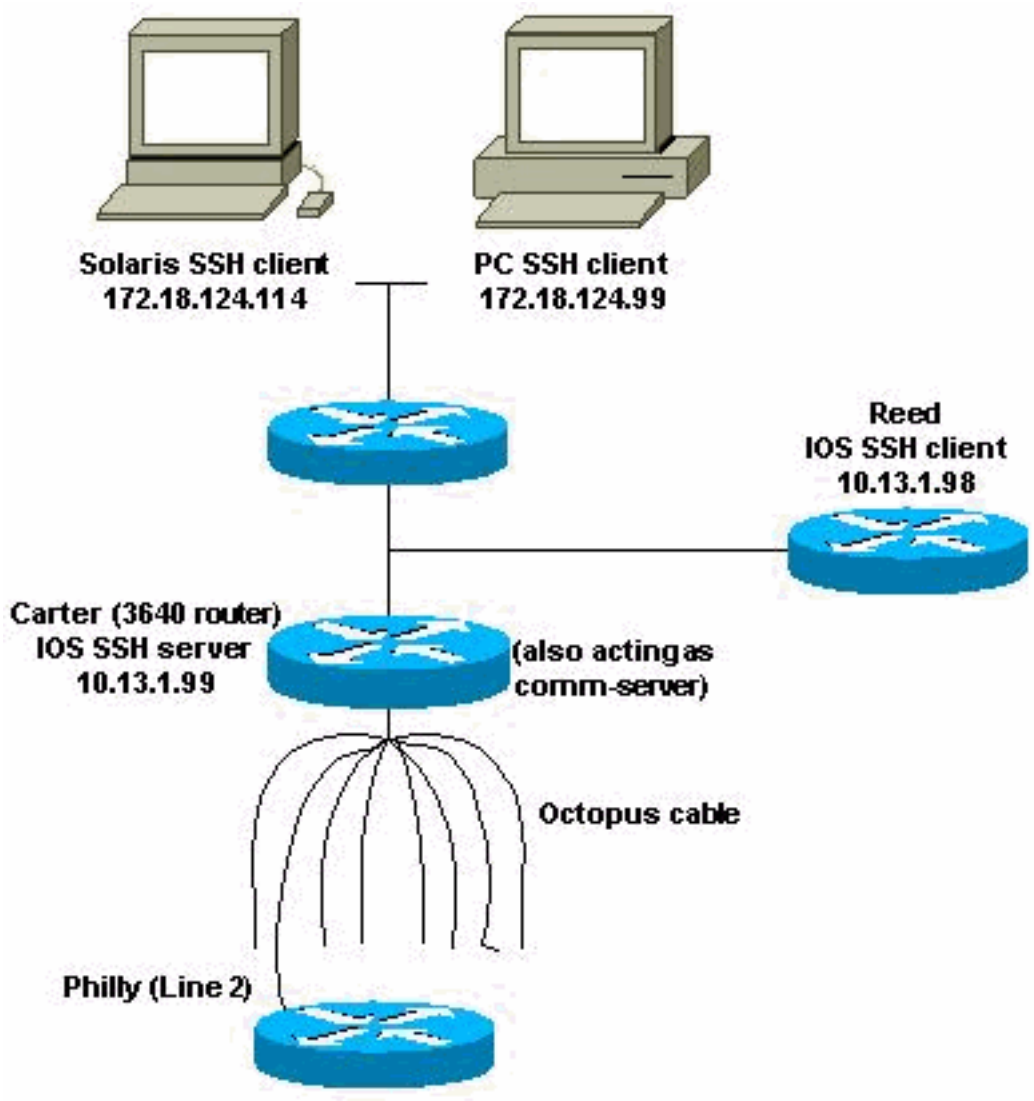
内容

概要

このドキュメントでは、セキュア シェル（SSH）に関して最もよく寄せられる質問（FAQ）への回答を説明します。 Cisco IOS® SSHコードは、シスコのオリジナルコードです。

SSH 端末回線アクセス（別名、リバース Telnet）はどのように設定するのですか。

これは、Cisco IOSソフトウェアリリース12.2.2.Tの一部のプラットフォームで初めて導入されました。




```
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
```

コマンド リファレンス

```
ip ssh port
ip ssh port portnum rotary group
no ip ssh port portnum rotary group
```

- portnum:SSHが接続する必要があるポート（2001など）を指定します。
- rotary group – 有効な名前を検索する必要がある定義済みの回ータリーを指定します。

Catalyst 2900 では SSH はサポートされていますか。

いいえ。サポートされていません。

どのプラットフォームとコード バージョンで SSH がサポートされているかを識別するにはどうすればよいのですか。

Feature Navigator (>登録ユーザ専用) を参照し、SSH 機能を指定してください。

ルータから特定の SSH コマンドを削除しようとしましたが、SSH をイネーブルにするには、RSA キーを作成するようにという指示が繰り返し表示されます。なぜでしょうか。

この問題の例を次に示します。

```
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)
```

Cisco Bug ID CSCdv70159(登録ユーザ専用)が発生しています。

Cisco IOS SSHバージョン2はDigital Signature Standard (DSS ; デジタルシグニチャ標準) をサポートしていますか。

Cisco IOS SSHバージョン2はDSSをサポートしていません。

Cisco IOS SSH サーバでは、エージェント転送がサポートされていますか。

Cisco IOS SSH は、エージェント転送をサポートしていません。Cisco IOS SSH は、流通しているすべての SSH 実装と相互運用できます。

Cisco IOS SSHサーバでは、どのクライアント認証メカニズムがサポートされていますか。

Cisco IOS SSHバージョン2(SSHv2)は、キーボードインタラクティブおよびパスワードベースの認証方式をサポートしています。これらの認証方式に加えて、SSHv2 Enhancements for RSA Keys機能(Cisco IOSソフトウェアリリース15.0(1)M以降で利用可能)は、クライアントおよびサーバのRSAベースの公開キー認証をサポートしています。Cisco IOS SSHサーバでサポートされている認証メカニズムの詳細については、『Secure Shellバージョン2のサポート』を参照してください。

Local:`Corrupted check bytes on input`

Corrupted checkbytes（チェックバイトの破損）は、受信した SSH パケットで完全性チェックが失敗したことを意味しています。これは通常、不適切な復号化が原因です。また、不適切なキーを使用したことも原因です。不適切なキーは、暗号化された SSH パケットのドロップによって発生します。送信されているはずの暗号化パケットがドロップされたか、復号化されているはずの受信暗号化パケットがドロップされたかのいずれかです。

Cisco IOSはBlowfish暗号を使用したSSHをサポートしていますか。

Cisco IOSでは、Blowfish暗号を使用したSSHはサポートされていません。SSHクライアントがこのようなサポートされていない暗号を送信すると、ルータは「SSHクライアントがサポートされていない(Blowfish)暗号を送信する」に記載されたデバッグメッセージを表示します。

configモードでcrypto key generate rsaコマンドを使用して、ルータでSSHアクセス用のRSAキーを生成しようとすると、次のエラーが表示されます。% '^'。ルータがルータのSSHアクセスを有効にするためにRSAキーを生成することはありません。この問題の解決方法を次に説明します。

このエラーは、ルータで使用されているイメージがcrypto key generate rsaコマンドをサポートしていない場合に表示されます。このコマンドは、セキュリティイメージでのみサポートされます。このエラーを解決するには、使用するCisco IOSルータの適切なシリーズのセキュリティイメージを使用します。

暗号イメージは、3DESやAESなどの暗号でSSHを使用する強力な暗号をサポートしていますか。

はい。暗号化イメージだけが強力な暗号をサポートします。3DESやAESなどの暗号でSSHを使用するには、シスコデバイスに暗号イメージが必要です。

ルータでSSHを設定しようとすると、次のメッセージがログに表示されます。`SSH2 13:RSA_sign:`ん。`SSH2 13:-1`。 この問題を解決するにはどうすればよいですか。

これらのログメッセージは、Cisco Bug ID CSCsa83601(登録ユーザ専用)およびCSCtc4114(登録ユーザ専用)が原因で表示されます。 詳細については、これらのバグを参照してください。

関連情報

- SSH サポート ページ
- テクニカル サポートとドキュメント – Cisco Systems