Configuring Secure Shell

Last Updated: January 16, 2012

This chapter describes the Secure Shell (SSH) feature. The SSH feature consists of an application and a protocol.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring SSH

Prior to configuring SSH, perform the following tasks:

- Download the required image on your router. (The SSH server requires you to have an IPsec (DES or 3DES) encryption software image downloaded on your router; the SSH client requires you to have an IPsec (DES or 3DES) encryption software image downloaded on your router.) For more information

on downloading a software image, see the *Cisco IOS XE Configuration Fundamentals Configuration Guide* , Release 2.

- Configure a host name and host domain for your router.

To configure a host name and host domain, enter the **hostname** *hostname* and **ip domain-name** *domainname* commands in global configuration mode:

- Generate an RSA key pair for your router, which automatically enables SSH.

To generate an RSA key pair, enter the **crypto key generate rsa** command.

Note To delete the RSA key-pair, use the **crypto key zeroize rsa** global configuration command. Once you delete the RSA key-pair, you automatically disable the SSH server.

- Configure user authentication for local or remote access. You can configure authentication with or without AAA. For more information on AAA, see the Authentication, Authorization, and Accounting chapters in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2 and the *Cisco IOS Security Command Reference* .

Restrictions for Configuring SSH

- RSA authentication available in SSH clients is not supported in the SSH server for Cisco IOS XE software.
- SSH server and SSH client are supported on DES (56-bit) and 3DES (168-bit) data encryption software images only.
- Execution shell is the only application supported.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.

Information About Secure Shell

Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley **rexec** and **rsh** tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. This document describes SSH Version 1. For information about SSH Version 2, see the Secure Shell Version 2 Support document.

Note Hereafter, unless otherwise noted, the term “SSH” will denote “SSH Version 1” only.

How SSH Works

- SSH Integrated Client, page 3

SSH Server

The SSH Server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to that of an inbound Telnet connection. Before SSH, security was limited to Telnet security. SSH allows a strong encryption to be used with the Cisco IOS XE software authentication. The SSH server in Cisco IOS XE software will work with publicly and commercially available SSH clients.

SSH Integrated Client

The SSH Integrated Client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running the SSH server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco IOS XE software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), Triple DES (3DES), and password authentication. User authentication is performed like that in the Telnet session to the router. The user authentication mechanisms supported for SSH are RADIUS, TACACS+ and the use of locally stored user names and passwords.

Note The SSH client functionality is available only when the SSH server is enabled.

Related Features and Technologies

For more information about SSH-related features and technologies, review the following:

- Authentication, Authorization, and Accounting (AAA) feature. AAA is a suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server. For more information on AAA, see the Authentication, Authorization, and Accounting chapters in the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2 and the *Cisco IOS Security Command Reference* .
- IP Security (IPsec) feature. IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. For more information on IPsec, see the chapter Configuring Security for VPNs with IPsec and the *Cisco IOS Security Command Reference* .

How to Configure SSH

- Configuring SSH Server, page 4
- Verifying SSH, page 4

Configuring SSH Server

Note The SSH client feature runs in user EXEC mode and has no specific configuration on the router.

Note The SSH commands are optional and are disabled when the SSH server is disabled.

To enable and configure a Cisco Router for SSH, you can configure SSH parameters. If you do not configure SSH parameters, the default values will be used.

To configure SSH server, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip ssh {[timeout seconds ] | [authentication-retries integer ]}`	(Required) Configures SSH control variables on your router. • You can specify the timeout in seconds, not to exceed 120 seconds. The default is 120. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes. • You can also specify the number of authentication retries, not to exceed 5 authentication retries. The default is 3.

Verifying SSH

To verify that the SSH server is enabled and view the version and configuration data for your SSH connection, use the **show ip ssh**command. The following example shows that SSH is enabled:

```
Router# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following example shows that SSH is disabled:

```
Router# show ip ssh
%SSH has not been enabled
```

To verify the status of your SSH server connections, use the **show ssh** command. The following example shows the SSH server connections on the router when SSH is enabled:

```
Router# show ssh
Connection      Version     Encryption    State    Username
    0    1.5    3DES    Session Started        guest
```

The following example shows that SSH is disabled:

```
Router# show ssh
%No SSH server connections running.
```

Troubleshooting Tips

- If your SSH configuration commands are rejected as illegal commands, you have not successfully generated a RSA key pair for your router. Make sure you have specified a host name and domain. Then use the **crypto key generate rsa**command to generate a RSA key pair and enable the SSH server.
- When configuring the RSA key pair, you might encounter the following error messages:
  - No hostname specified

You must configure a host name for the router using the **hostname** global configuration command. For more information, see “Prerequisites for Configuring SSH, page 1.”

- ◦ No domain specified

You must configure a host domain for the router using the **ip domain-name** global configuration command. For more information, see “Prerequisites for Configuring SSH, page 1.”

- The number of allowable SSH connections is limited to the maximum number of vtys configured for the router. Each SSH connection will use a vty resource.
- SSH uses either local security or the security protocol that is configured through AAA on your router for user authentication. When configuring AAA, you must ensure that AAA is disabled on the console for user authentication. AAA authorization is disabled on the console by default. If AAA authorization is enabled on the console, disable it by configuring the **no aaa authorization console** command during the AAA configuration stage.

Monitoring and Maintaining SSH

To monitor and maintain your SSH connections, use the following commands in user EXEC mode:

Command	Purpose
`Router# show ip ssh`	Displays the version and configuration data for SSH.
`Router# show ssh`	Displays the status of SSH server connections.

SSH Configuration Examples

This section provides the following configuration example showing output from the **show running configuration** EXEC command on a Cisco ASR1000 Series Aggregation Services Router.

- SSH on a Cisco ASR1000 Series Router Example, page 6

Note The **crypto key generate rsa** command is not displayed in the **show running configuration** output.

- SSH on a Cisco ASR1000 Series Router Example, page 6

SSH on a Cisco ASR1000 Series Router Example

In the following example, SSH is configured on a Cisco ASR1000 series router with a timeout that is not to exceed 60 seconds, and no more than 2 authentication retries. Also, before configuring the SSH server feature on the router, TACACS+ is specified as the method of authentication.

```
hostname RouterASR1K
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password enableasr1kpw
username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter the ssh commands.
ip ssh time-out 60
ip ssh authentication-retries 2
ip route 192.168.1.0 255.255.255.0 10.1.10.1
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1
map-list atm
ip 10.1.10.1 atm-vc 7 broadcast
no cdp run
tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco
line con 0
exec-timeout 0 0
login authentication aaa7200kw
transport input none
line aux 0
line vty 0 4
password enableasr1kpw
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	*Cisco IOS Security Command Reference*

Related Topic	Document Title
AAA configuration	The following chapters of the *Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2: • Configuring Authentication • Configuring Authorization • Configuring Accounting
IPSec configuration	*Configuring Security for VPNs with IPsec*

Standards

Standard	Title
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Secure Shell

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Configuring Secure Shell

Feature Name	Releases	Feature Configuration Information
Secure Shell SSH Version 1 Integrated Client	Cisco IOS XE Release 2.1	The SSH Version 1 Integrated Client feature is an application running over the SSH protocol to provide device authentication and encryption. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
Secure Shell SSH Version 1 Server Support	Cisco IOS XE Release 2.1	The SSH Version 1 Server Support feature enables a SSH client to make a secure, encrypted connection to a Cisco router. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 Series Routers.