Configuring SSH File Transfer Protocol

Secure Shell (SSH) includes support for SSH File Transfer Protocol (SFTP), which is a new standard file transfer protocol introduced in SSHv2. This feature provides a secure and authenticated method for copying device configuration or device image files.

Prerequisites for SSH File Transfer Protocol

- SSH must be enabled.
- The **ip ssh source-interface** *interface-type interface-number* command must be configured.

Restrictions for SSH File Transfer Protocol

- The SFTP server is not supported.
- SFTP boot is not supported.
- The **sftp** option in the **install add** command is not supported.

Information About SSH Support over IPv6

SSH File Transfer Protocol Overview

The SFTP client functionality is provided as part of the SSH component and is always enabled on the corresponding device. Therefore, any SFTP server user with the appropriate permission can copy files to and from the device.

An SFTP client is VRF-aware; you can configure the secure FTP client to use the virtual routing and forwarding (VRF) associated with a particular source interface during connection attempts.

How to Configure SSH File Transfer Protocol

The following sections provide information about the various tasks that comprise an SFTP configuration.

Configuring SFTP

Perform the following steps:

Before you begin

To configure a Cisco device for SFTP client-side functionality, the **ip ssh source-interface** *interface-type interface-number* command must be configured first.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip ssh source-interface** *interface-type interface-number* **Example:** `Device(config)# ip ssh source-interface GigabitEthernet 1/0/1`	Defines the source IP for the SSH session.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show running-config** **Example:** `Device# show running-config`	(Optional) Displays the SFTP client-side functionality.
Step 6	**debug ip sftp** **Example:** `Device# debug ip sftp`	(Optional) Enables SFTP debugging.

Configuring SFTP Username Password

To configure a username and password for SFTP, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sftp username***username* **Example:** `Device# ip sftp username cisco`	Defines the username.
Step 4	**ip sftp password***password* **Example:** `Device# ip sftp password 0 cisco`	Defines the password. Specify the encryption level. • 0 – Unencrypted password. • 0 – Encrypted password. • Line – Clear text password
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Performing an SFTP Copy Operation

SFTP copy takes the IP or hostname of the corresponding server if Domain Name System (DNS) is configured. To perform SFTP copy operations, use the following commands in privileged EXEC mode:

Command	Purpose
Device# **copy ios-file-system:file sftp://user:pwd@server-ip//filepath** Or Device# **copy ios-file-system: sftp:**	Copies a file from the local Cisco IOS file system to the server. Specify the username, password, IP address, and filepath of the server.
Device# **copy sftp://user:pwd@server-ip //filepath ios-file-system:file** Or Device# **copy sftp: ios-file-system:**	Copies the file from the server to the local Cisco IOS file system. Specify the username, password, IP address, and filepath of the server.

Configuration Examples for SSH Support over IPv6

Example: Configuring SSH File Transfer Protocol

The following example shows how to configure the client-side functionality of SFTP:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh source-interface gigabitethernet 1/0/1
Device(config)# exit
```

Additional References for SSH File Transfer Protocol

Related Documents

Related Topic	Document Title
Secure Shell Version 1 and 2 Support	*Security Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for SSH File Transfer Protocol

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.10.1	SSH File Transfer Protocol	SSH includes support for SFTP, a new standard file transfer protocol introduced in SSHv2.
Cisco IOS XE Cupertino 17.9.1	SSH File Transfer Protocol	This feature was implemented on C9200CX-12P-2X2G, C9200CX-8P-2X2G, and C9200CX-12T-2X2G models of the Cisco Catalyst 9200CX Series Switches, which were introduced in this release.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to Cisco Feature Navigator.