CHAPTER 5

Configuring SSHv2 and Telnet

This chapter describes how to configure Secure Shell Protocol version 2 (SSHv2) and Telnet on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as Cisco CG-OS router).

This chapter includes the following sections:

- Information About SSHv2 and Telnet, page 5-1
- Prerequisites, page 5-3
- Guidelines and Limitations, page 5-3
- Default Settings, page 5-3
- Configuring SSHv2, page 5-3
- Configuring Telnet, page 5-9
- Verifying the SSHv2 and Telnet Configuration, page 5-11
- Configuration Example, page 5-11

Information About SSHv2 and Telnet

This section includes the following topics:

- SSHv2 Server, page 5-1
- SSHv2 Client, page 5-2
- SSHv2 Server Keys, page 5-2
- SSHv2 Authentication Using Digital Certificates, page 5-2
- Telnet Server, page 5-3

SSHv2 Server

You can use the SSHv2 server to enable an SSH client to make a secure, encrypted connection to the Cisco CG-OS router. SSHv2 uses strong encryption for authentication. The SSHv2 server in the Cisco CG-OS software can interoperate with publicly and commercially available SSHv2 clients. The user authentication mechanisms supported for SSHv2 are RADIUS, TACACS+, and the use of locally stored usernames and passwords on the Cisco CG-OS router.
SSHv2 Client

The SSHv2 client feature is an application that runs over the SSHv2 protocol to provide device authentication and encryption. The SSHv2 client enables the Cisco CG-OS router to make a secure, encrypted connection to any other device that runs the SSHv2 server. This connection provides an encrypted outbound connection. With authentication and encryption, the SSHv2 client allows for a secure communication over an insecure network.

The SSHv2 client in Cisco CG-OS works with publicly and commercially available SSHv2 servers.

SSHv2 Server Keys

SSHv2 requires server keys for secure communications to the Cisco CG-OS router. You can use SSHv2 server keys for the following SSHv2 options:

- SSHv2 version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSHv2 version 2 using the Digital System Algorithm (DSA)

Be sure to have an SSHv2 server key-pair with the appropriate version before enabling the SSHv2 service. You can generate the SSHv2 server key-pair according to the SSHv2 client version used. The SSHv2 service accepts two types of key-pairs for use by SSHv2:

- The `dsa` option generates the DSA key-pair for the SSHv2 protocol.
- The `rsa` option generates the RSA key-pair for the SSHv2 protocol.

By default, Cisco CG-OS generates an RSA key using 1024 bits.

SSHv2 supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)

⚠️ Caution

If you delete all of the SSHv2 keys, you cannot start the SSHv2 services.

SSHv2 Authentication Using Digital Certificates

SSHv2 authentication provides X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that ensures the origin and integrity of a message. It contains encryption keys for secured communications and is signed by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through query or notification. Verification of certificates is successful if the certificates are from any of the trusted CAs.

You can configure your device for either SSHv2 authentication using an X.509 certificate or SSHv2 authentication using a Public Key Certificate, but not both. If either of them is configured and the authentication fails, you are prompted for a password.

For more information on CAs and digital certificates, see Chapter 6, “Configuring PKI.”
Telnet Server

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

By default, the Telnet server is disabled on the Cisco CG-OS router.

Prerequisites

Configure IP on a Layer 3 interface, out-of-band on the mgmt 0 interface, or inband on an Ethernet interface.

Guidelines and Limitations

Cisco CG-OS supports only SSH version 2 (SSHv2).

You can configure the Cisco CG-OS router with either SSHv2 authentication using an X.509 certificate or SSHv2 authentication using a Public Key Certificate, but not both. Regardless of which authentication method is in use, the Cisco CG-OS router prompts the user for a password when authentication fails.

Cisco CG-OS supports a maximum of 60 concurrent SSHv2 and Telnet sessions.

Default Settings

Table 5-1 lists the default settings for SSHv2 and Telnet parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSHv2 server</td>
<td>Enabled</td>
</tr>
<tr>
<td>SSHv2 server key</td>
<td>RSA key generated with 1024 bits</td>
</tr>
<tr>
<td>RSA key bits for generation</td>
<td>1024</td>
</tr>
<tr>
<td>Telnet server</td>
<td>Disabled</td>
</tr>
<tr>
<td>Telnet port number</td>
<td>23</td>
</tr>
</tbody>
</table>

Configuring SSHv2

This section includes the following sections:

- Generating SSHv2 Server Keys, page 5-4
- Specifying the SSHv2 Public Keys for User Accounts, page 5-4
- Starting SSHv2 Sessions, page 5-6
- Clearing SSHv2 Hosts, page 5-7
- Disabling the SSHv2 Server, page 5-7
Generating SSHv2 Server Keys

You can generate an SSHv2 server key based on your security requirements. The default SSHv2 server key is an RSA key that the Cisco CG-OS router generates using 1024 bits.

BEFORE YOU BEGIN

Ensure that you have met the prerequisites for SSHv2 summarized under Prerequisites.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 no feature ssh</td>
<td>Disables SSHv2. By default, SSHv2 is enabled</td>
</tr>
<tr>
<td></td>
<td>on the Cisco CG-OS router.</td>
</tr>
<tr>
<td>Step 3 ssh key {dsa [force]</td>
<td>rsa [bits [force]]}</td>
</tr>
<tr>
<td></td>
<td>dsa—generates the DSA key-pair for the SSHv2</td>
</tr>
<tr>
<td></td>
<td>protocol.</td>
</tr>
<tr>
<td></td>
<td>rsa—generates the RSA key-pair for the SSHv2</td>
</tr>
<tr>
<td></td>
<td>protocol.</td>
</tr>
<tr>
<td></td>
<td>(Optional) The bits argument is the number</td>
</tr>
<tr>
<td></td>
<td>of bits used to generate the key. The range</td>
</tr>
<tr>
<td></td>
<td>is from 768 to 2048 and the default value</td>
</tr>
<tr>
<td></td>
<td>is 1024.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Use the force keyword to replace</td>
</tr>
<tr>
<td></td>
<td>an existing key.</td>
</tr>
<tr>
<td>Step 4 feature ssh</td>
<td>Enables SSHv2.</td>
</tr>
<tr>
<td>Step 5 show ssh key</td>
<td>(Optional) Displays the SSHv2 server keys.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Copies the running configuration</td>
</tr>
<tr>
<td></td>
<td>to the startup configuration.</td>
</tr>
</tbody>
</table>

EXAMPLE

This example shows how to generate a SSHv2 server key on the Cisco CG-OS router.

```
router# configure terminal
router(config)# no feature ssh
router(config)# ssh key rsa 2048
router(config)# feature ssh
router(config)# copy running-config startup-config
```

Specifying the SSHv2 Public Keys for User Accounts

You can configure an SSHv2 public key to log in using an SSHv2 client without being prompted for a password. You can specify the SSHv2 public key in one of these formats:
Specifying the SSHv2 Public Keys in OpenSSH Format

You can specify the SSHv2 public keys in OpenSSH format for user accounts.

BEFORE YOU BEGIN

Generate an SSHv2 public key in OpenSSH format.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>username username sshkey ssh-key Configures the SSHv2 public key in OpenSSH format.</td>
</tr>
<tr>
<td>Step 3</td>
<td>show user-account (Optional) Displays the user account configuration.</td>
</tr>
<tr>
<td>Step 4</td>
<td>copy running-config startup-config (Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

EXAMPLE

This example shows how to specify SSHv2 public keys for user accounts.

```
router# configure terminal
router(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABAIAy19oF6QaZ19G+3f1XswK3OiW4H7YyOyuA5Orv7gsEPjh0BYmsI6PAVKui1nIf/DQhum+1JNqJP/eLowb7+ub0+1VlRXXY/G+1LN1QW3g9igG30c6k6+xVn+NjN1B7ihvpVh7dLdMOnXHYshXmSih3UD/vKyziEh5S4Tplx8=
router(config)# copy running-config startup-config
```

Specifying the SSHv2 Public Keys in IETF SECSH Format

You can specify the SSHv2 public keys in IETF SECSH format for user accounts.

BEFORE YOU BEGIN

Generate an SSHv2 public key in IETF SCSCH format.
Chapter 5  Configuring SSHv2 and Telnet

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>copy server-file bootflash:filename</strong></td>
</tr>
<tr>
<td></td>
<td>Downloads the file containing the SSHv2 key in IETF SECSH format from a server. The server can be FTP, secure copy (SCP), secure FTP (SFTP), or TFTP.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only a network-admin or vdc-admin can perform this task.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>username username sshkey file bootflash:filename</strong></td>
</tr>
<tr>
<td></td>
<td>Configures the SSHv2 public key in IETF SECSH format.</td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>show user-account</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Displays the user account configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

EXAMPLE

This example shows how to specify the SSHv2 public keys in IETF SECSH format.

```
router# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
router(config)# configure terminal
router(config)# username User1 sshkey file bootflash:secsh_file.pub
router(config)# copy running-config startup-config
```

Starting SSHv2 Sessions

You can start SSHv2 sessions using IPv4 or IPv6 to connect to remote devices from the Cisco CG-OS router.

**Note**

Cisco CG-OS supports a maximum of 60 concurrent SSHv2 and Telnet sessions.

BEFORE YOU BEGIN

Obtain the hostname for the remote device and, if needed, the username on the remote device. Enable the SSHv2 server on the remote device.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>**ssh [username@][ipv4-address</td>
</tr>
<tr>
<td></td>
<td>Creates an SSHv2 IPv4 session to a remote device using IPv4.</td>
</tr>
<tr>
<td></td>
<td>**ssh6 [username@][ipv6-address</td>
</tr>
<tr>
<td></td>
<td>Creates an SSHv2 IPv6 session to a remote device using IPv6.</td>
</tr>
</tbody>
</table>
EXAMPLE

This example shows how to create an SSHv2 IPv4 session to a remote device.
```
router# ssh 10.10.1.1
```
This example shows how to how to create an SSHv2 IPv6 session to a remote device.
```
router# ssh6 HostA
```

Clearing SSHv2 Hosts

When you download a file from a server using SCP or SFTP, or when you start an SSHv2 session from the Cisco CG-OS router to a remote host, you establish a trusted SSHv2 relationship with that server. You can clear the list of trusted SSHv2 servers for your user account.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ssh hosts</td>
<td>Clears the SSHv2 host sessions.</td>
</tr>
</tbody>
</table>

Disabling the SSHv2 Server

By default, the SSHv2 server is enabled on the Cisco CG-OS router. You can disable the SSHv2 server to prevent SSHv2 access to the Cisco CG-OS router.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no feature ssh</td>
<td>Disables SSH.</td>
</tr>
</tbody>
</table>

Note

To reenable SSHv2, you must first generate an SSHv2 server key. (See Generating SSHv2 Server Keys, page 5-4.)

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>no feature ssh</td>
<td>Disables the SSHv2 server. Feature is enabled by default.</td>
</tr>
<tr>
<td>3</td>
<td>show ssh server</td>
<td>(Optional) Displays the SSHv2 server configuration.</td>
</tr>
<tr>
<td>4</td>
<td>copy running-config startup-config</td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>
EXAMPLE

This example shows how to disable SSHv2 on the Cisco CG-OS router.

```
router# configure terminal
router(config)# no feature ssh
router(config)# copy running-config startup-config
```

Deleting SSHv2 Server Keys

BEFORE YOU BEGIN

Disable the SSHv2 server. (See Disabling the SSHv2 Server, page 5-7.)

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 no feature ssh</td>
<td>Disables the SSHv2 server.</td>
</tr>
<tr>
<td>Step 3 no ssh key [dsa</td>
<td>Deletes the SSHv2 server key. The default is to delete all the SSHv2 keys.</td>
</tr>
<tr>
<td></td>
<td>rsa]</td>
</tr>
<tr>
<td>Step 4 show ssh key</td>
<td>(Optional) Displays the SSHv2 server key configuration.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

EXAMPLE

This example shows how to delete SSHv2 server keys.

```
router# configure terminal
router(config)# no feature ssh
router(config)# no ssh key rsa
router(config)# copy running-config startup-config
```

Clearing SSHv2 Sessions

You can clear SSHv2 sessions from the Cisco CG-OS router.

BEFORE YOU BEGIN

No prerequisites.
Chapter 5  Configuring SSHv2 and Telnet

Configuring Telnet

This section includes the following topics:

- Enabling the Telnet Server, page 5-9
- Starting Telnet Sessions to Remote Devices, page 5-10
- Clearing Telnet Sessions, page 5-10

Enabling the Telnet Server

You can enable the Telnet server on the Cisco CG-OS router. By default, the Telnet server is disabled.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>feature telnet</td>
<td>Enables the Telnet server. The default is disabled.</td>
</tr>
<tr>
<td>show telnet server</td>
<td>(Optional) Displays the Telnet server configuration.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Copies the running configuration to the startup configuration.</td>
</tr>
</tbody>
</table>

EXAMPLE

This example shows how to enable Telnet on the Cisco CG-OS router.

```
router# configure terminal
router(config)# feature telnet
```
Starting Telnet Sessions to Remote Devices

You can start Telnet sessions to connect to remote devices from the Cisco CG-OS router. You can start Telnet sessions by using either IPv4 or IPv6.

**Note**
Cisco CG-OS supports a maximum of 60 concurrent SSHv2 and Telnet sessions.

**BEFORE YOU BEGIN**
Obtain the hostname or IP address for the remote device and, if needed, the username on the remote device.
Enable the Telnet server on the Cisco CG-OS router. (See Enabling the Telnet Server, page 5-9.)
Enable the Telnet server on the remote device.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  telnet {ipv4-address | host-name} [port-number]       | Starts a Telnet session to a remote device using IPv4. The default port number is 23. The range is from 1 to 65535. |
| telnet6 {ipv6-address | host-name} [port-number]       | Starts a Telnet session to a remote device using IPv6. The default port number is 23. The range is from 1 to 65535. |

**EXAMPLE**

This example shows how to configure a Telnet session to a remote device that is using IPv4.

```
router# telnet 10.10.1.1
```

This example shows how to configure a Telnet session to a remote device that is using IPv6.

```
router# telnet 2001:0DB8::ABCD:1 management
```

Clearing Telnet Sessions

You can clear Telnet sessions from the Cisco CG-OS router.

**BEFORE YOU BEGIN**
Telnet server must be enabled on the Cisco CG-OS router.
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show users</td>
<td>Displays user session information.</td>
</tr>
<tr>
<td>clear line vty-line</td>
<td>Clears a user Telnet session.</td>
</tr>
</tbody>
</table>

EXAMPLE

This example shows how to clear a Telnet session.

```
router# show users
router(config)# clear line pts/12
```

Verifying the SSHv2 and Telnet Configuration

To display the SSHv2 and Telnet configuration information, enter any or all of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ssh key [dsa</td>
<td>rsa]</td>
</tr>
<tr>
<td>show running-config security [all]</td>
<td>Displays the SSHv2 and user account configuration in the running configuration. The all keyword displays the default values for the SSHv2 and user accounts.</td>
</tr>
<tr>
<td>show ssh server</td>
<td>Displays the SSHv2 server configuration.</td>
</tr>
<tr>
<td>show telnet server</td>
<td>Displays the Telnet server configuration.</td>
</tr>
</tbody>
</table>

Configuration Example

```
configure terminal
no feature ssh
ssh key rsa
    generating rsa key(1024 bits)...  
    generated rsa key
feature ssh
show ssh key
    rsa Keys generated: Tues Jan 29 00:10:39 2013
    ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAWbF55oapPHNDBnpXUTw6+/OdHoLZJKz+rMza99n2U0ChzZG4svRWhuJ4PeDWl0e5yE3g3E03pJDzmt923s1Nv5aSga60K361r39HmXL6VppRv1XQFlbwn4na+H1d3Q0hD+uWHe0tka2u0aXliEzn4HVX0jGHFhoNE=
    bitcount:1024
    ****************************************
    could not retrieve dsa key information
    ****************************************
```
username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIBwAAAIEAy19oF6QaZl9G+3f1XswK3oiW4H7YyUyuA50rv7gsEPjh0B4Ym6i6PAVKui1nIf/
DQhum+1JNgjJf/eLowb7ubO+1VKRXYFy/G+1JNjQW3ig9igG30c6k6+XVn+NjnT187hvpVh7dLo30XwOnXH2shXsSjH
3UD/vKzsiEh5S46p1x8=
copy running-config startup-config