Configuring Secure Shell

Last Updated: July 04, 2011

The Secure Shell (SSH) feature is an application and a protocol that provides 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. Two versions of SSH are 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 feature module.

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

- Finding Feature Information, page 1
- Prerequisites for Configuring SSH, page 2
- Restrictions for Configuring SSH, page 2
- Information About Secure Shell, page 2
- How to Configure SSH, page 3
- Configuration Examples for SSH, page 6
- Additional References, page 11
- Feature Information for Configuring Secure Shell, page 12

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

Perform the following tasks before configuring SSH:

- Download the required image on the router. The SSH server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image from Cisco IOS Release 12.1(1)T or a later release; the SSH client requires an IPsec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T or a later release.) See the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information on downloading a software image.
- Configure a hostname and host domain for your router by using the **hostname** and **ip domain-name** commands in global configuration mode.
- Generate a Rivest, Shamir and Adleman (RSA) key pair for your router. This key pair automatically enables SSH and remote authentication when the **crypto key generate rsa** command is entered in global configuration mode.

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 authentication, authorization, and accounting (AAA). For more information, see the Configuring Authentication Configuring Authorization and Configuring Accounting feature modules for more information.

Restrictions for Configuring SSH

SSH has the following restrictions:

- The SSH server and SSH client are supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- 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

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

- SSH Server, page 3
- SSH Integrated Client, page 3
- RSA Authentication Support, page 3

SSH Server

The SSH Server feature enables an 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 software authentication. The SSH server in Cisco IOS software works with publicly and commercially available SSH clients.

SSH Integrated Client

The SSH Integrated Client feature is an application thats runs 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 that is 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 secure communication over an insecure network.

The SSH client in Cisco IOS software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of 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 usernames and passwords.

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

RSA Authentication Support

RSA authentication available in SSH clients is not supported on the SSH server for Cisco IOS software by default. See the " Configuring a Router for SSH Version 2 Using Private Public Key Pairs" section of the "Secure Shell Version 2 Support" chapter for the procedure to configure RSA authentication support.

How to Configure SSH

Note Hereafter, unless otherwise noted, the term "SSH" denotes "SSH Version 1" only.

- Configuring an SSH Server, page 3
- Invoking an SSH Client, page 5

Configuring an SSH Server

Perform the following steps to configure an SSH server. This task helps you to enable the Cisco router for SSH.

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. If SSH parameters are not configured, then the default values are used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh** {**timeout** *seconds* | **authentication-retries** *integer*}
4.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *integer*} **Example:** `Router(config) # ip ssh timeout 30`	Configures SSH control parameters on your router. • Select one of the SSH control variables. • The *seconds* argument specifies 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, five vtys are defined (0-4); therefore five terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.

Command or Action	Purpose
Step 4	• The *integer* argument specifies the number of authentication retries, not to exceed five authentication retries. The default is three. **Note** This command can also be used to establish the number of password prompts provided to the user. The number is the lower of the following two values: • ◦ Value proposed by the client using the **ssh -o numberofpasswordprompt** command. ◦ Value configured on the router using the **ip ssh authentication-retries** *integer*command, plus one.

Invoking an SSH Client

Perform this task to invoke an SSH client.

SUMMARY STEPS

1. **enable**
2. **ssh -l** *username* **-vrf** *vrf-name ip-address*

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** `Router> enable`	(Optional) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 **ssh -l** *username* **-vrf** *vrf-name ip-address* **Example:** `Router# ssh -l user1 -vrf vrf1 192.0.2.1`	(Optional) Invokes the Cisco IOS SSH client to connect to an IP host or address in the specified virtual routing and forwarding (VRF) instance.

• Troubleshooting Tips, page 5

Troubleshooting Tips

- If your SSH configuration commands are rejected as illegal commands, you have not successfully generated an RSA key pair for your router. Make sure that you have specified a hostname and domain. Then use the **crypto key generate rsa**command to generate an 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 hostname for the router using the **hostname** global configuration command. See the IPsec and Quality of Service feature module for more information.

- ◦ No domain specified

You must configure a host domain for the router using the **ip domain-name** global configuration command. See the IPsec and Quality of Service feature module for more information.

- The number of allowable SSH connections is limited to the maximum number of vtys configured for the router. Each SSH connection uses 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.

Configuration Examples for SSH

This section provides the following configuration examples, which are output from the show running-config EXEC command on a Cisco 7200, Cisco 7500, and Cisco 12000 routers.

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

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

- Example SSH on a Cisco 7200 Series Router, page 6
- Example SSH on a Cisco 7500 Series Router, page 7
- Example SSH on a Cisco 12000 Series Router, page 9
- Example Verifying SSH, page 10

Example SSH on a Cisco 7200 Series Router

In the following example, SSH is configured on a Cisco 7200 with a timeout that is not to exceed 60 seconds and no more than 2 authentication retries. Before the SSH server feature is configured on the router, TACACS+ is specified as the method of authentication.

```
hostname Router72K
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password password
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 timeout 60
ip ssh authentication-retries 2
controller E1 2/0
controller E1 2/1
```

```
interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no keepalive
no cdp enable
interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable
interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable
no ip classless
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 password
end
```

Example SSH on a Cisco 7500 Series Router

In the following example, SSH is configured on a Cisco 7500 with a timeout that is not to exceed 60 seconds and no more than 5 authentication retries. Before the SSH server feature is configured on the router, RADIUS is specified as the method of authentication.

```
hostname Router75K
aaa new-model
aaa authentication login default radius
aaa authentication login aaa7500kw none
enable password password

username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip cef
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 5
controller E1 3/0
channel-group 0 timeslots 1

controller E1 3/1
channel-group 0 timeslots 1
channel-group 1 timeslots 2
interface Ethernet0/0/0
```

```
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/1
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown
interface Ethernet0/0/2
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/3
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/1
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/3
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/4
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Ethernet1/5
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Serial2/0
ip address 10.1.1.2 255.0.0.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
ip classless
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
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 aaa7500kw
transport input none
line aux 0
transport input all
line vty 0 4

end
```

Example SSH on a Cisco 12000 Series Router

In the following example, SSH is configured on a Cisco 12000 with a timeout that is not to exceed 60 seconds and no more than two authentication retries. Before the SSH server feature is configured on the router, TACACS+ is specified as the method of authentication.

```
hostname Router12K
aaa new-model
aaa authentication login default tacacs+ local
aaa authentication login aaa12000kw local
enable password password

username username1 password 0 password1
username username2 password 0 password2
redundancy
main-cpu
auto-sync startup-config
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 2
interface ATM0/0
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
interface POS1/0
ip address 10.100.100.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
no keepalive
crc 16
no cdp enable

interface POS1/1
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/2
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/3
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32
```

```
interface POS2/0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
crc 16

interface Ethernet0
ip address 172.17.110.91 255.255.255.224
no ip directed-broadcast

router ospf 1
network 0.0.0.0 255.255.255.255 area 0.0.0.0
ip classless
ip route 0.0.0.0 0.0.0.0 172.17.110.65

logging trap debugging
tacacs-server host 172.17.116.138
tacacs-server key cisco

radius-server host 172.17.116.138 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa12000kw
transport input none
line aux 0
line vty 0 4

no scheduler max-task-time
no exception linecard slot 0 sqe-registers
no exception linecard slot 1 sqe-registers
no exception linecard slot 2 sqe-registers
no exception linecard slot 3 sqe-registers
no exception linecard slot 4 sqe-registers
no exception linecard slot 5 sqe-registers
no exception linecard slot 6 sqe-registers
end
```

Example Verifying SSH

To verify that the SSH server is enabled and to display 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.
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Authentication, authorization, and accounting (AAA)	• Configuring Accounting feature module • Configuring Authentication feature module • Configuring Authorization feature module
IPsec	IPsec and Quality of Service feature module
SSH Version 2	Secure Shell Version 2 Support feature module
Downloading a software image	*Cisco IOS Configuration Fundamentals Configuration Guide*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards 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.	--

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 Information
Secure Shell	12.0(5)S	The Secure Shell (SSH) feature is an application and a protocol that provides 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. Two versions of SSH are available: SSH Version 1 and SSH Version 2. This document describes SSH Version 1.

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.