Secure Shell Version 1 Support

This feature module describes the Secure Shell server feature. It includes information on the benefits of the new feature, supported platforms, related documents, and so forth.

This document includes the following sections:

Feature Overview

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS.

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 an inbound Telnet connection. The SSH server in Cisco IOS will work with publicly and commercially available SSH clients.

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

Benefits

Additional Security

Before SSH, security was limited to Telnet security. SSH allows strong encryption to be used with Cisco IOS authentication.

Restrictions

SSH has the following restrictions:

- RSA authentication available in SSH clients is not supported in the SSH server for Cisco IOS.
- User ID and Password authentication only.
- Supported on DES (56-bit) data encryption and Triple DES (168-bit) data encryption software images only. In the DES (56-bit) software images, DES is the only encryption algorithm available. In the Triple DES software images, both DES and Triple DES encryption are available.
- Execution shell is the only application supported.

Caution Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images to be installed outside the United States require an export license. Customer orders might be denied or subject to delay due to United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Related Documents

For related information on the SSH server feature, refer to the following documents:

- Cisco IOS Release 12.0 *Security Configuration Guide*
- Cisco IOS Release 12.0 *Security Command Reference*
- Release Notes for Cisco 7000 Family for Cisco IOS Release 12.0 S
- Release Notes for Cisco 12000 Series Gigabit Switch Routers for Cisco IOS Release 12.0 S

Supported Platforms

- Cisco 7200 series routers
- Cisco 7500 series routers
- Cisco 12000 series Gigabit Switch Routers (GSR)

Supported Standards, MIBs, and RFCs

MIBs

No new or modified MIBs are supported by this feature.

For descriptions of supported MIBs and how to use MIBs, see Cisco’s MIB web site on CCO at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

No new or modified RFCs are supported by this feature.

Standards

No new or modified standards are supported by this feature.

Prerequisites

- Before configuring the SSH server, you must have an encryption software image that supports the SSH server feature downloaded on to your router. For more information on downloading a software image, see the following publications:
  - "Loading and Maintaining System Images and Microcode" chapter of the Cisco IOS Release 12.0 *Configuration Fundamentals Configuration Guide*
  - "System Image and Microcode Commands" chapter of the Cisco IOS Release 12.0 *Configuration Fundamentals Command Reference*
- Before configuring the SSH server, you must specify a host name and domain, then generate a RSA key-pair for the router. When you generate an RSA key-pair for the router, you automatically enable SSH. When you delete the RSA key-pair, you automatically disable the SSH server. For more information, see "Configuration Tasks."
- Before configuring the SSH server, you must configure user authentication for local or remote access. You can configure authentication with or without AAA. For more information refer to the "Configuring Authentication" chapter in the Cisco IOS Release 12.0 *Security Configuration Guide* and the "Authentication Commands" chapter in the Cisco IOS Release 12.0 *Security Command Reference*.
- The SSH configuration commands are optional and are disabled when the SSH server is disabled.

Configuration Tasks

See the following sections for SSH configuration tasks. Each task in the list indicates if it is optional or required:

- Configuring SSH Server (Required)
- Verifying SSH (Optional)
- Troubleshooting Tips (Optional)

Configuring SSH Server

To enable and configure a Cisco router for SSH, perform the following tasks in global configuration mode:

- Configure a host name and domain on your router (Required)
- Generate a RSA key-pair (Required)
- Configure SSH parameters (Optional)

Step	Command	Purpose
1	Router(config)# **hostname** *hostname*	Enter the **hostname** global configuration command to configure a host name for your router.
2	Router(config)# **ip domain-name** *domainname*	Enter the **ip domain-name** global configuration command to configure a host domain for your router.
3	Router(config)# **crypto key generate rsa**	Enter the **crypto key generate rsa** global configuration command to enable the SSH server for local and remote authentication on the router. The recommended minimum modulus size is 1024 bits. **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.
4	Router(config)# **ip ssh {[time-out** *seconds***]} | [authentication-retries** *integer***]}**	(Optional) Enter the **ip ssh** global configuration command to configure 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 defaults is 3.

Verifying SSH

To verify that the SSH server is enabled, enter **show ip ssh** from the EXEC prompt. If SSH server is not enabled, the command will generate an error message.

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 "Configuration Tasks."
  - "No domain specified"

    You must configure a host domain for the router using the **ip domain-name** global configuration command. For more information, see "Configuration Tasks."
- 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 the console is not running under AAA by applying a keyword in the global configuration mode to disable AAA on the console.

Configuration Examples

The following examples are output from the **show-running config** global configuration command on a Cisco 7200, Cisco 7500, and Cisco 12000. The SSH configuration commands are bold.

- Cisco 7200 Series Router Configuration
- Cisco 7500 Series Router Configuration
- Cisco 12000 Gigabit Switch Router Configuration

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

Cisco 7200 Series Router Configuration

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. Also, before configuring the SSH server feature onto the router, TACACS+ is specified as the method of authentication.

```
version 12.0
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service udp-small-servers
service tcp-small-servers

hostname cisco7200

boot buffersize 150000
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password enable7200pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
ip ssh time-out 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 enable7200pw

end
```

Cisco 7500 Series Router Configuration

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. Also, before configuring the SSH server feature onto the router, RADIUS is specified as the method of authentication.

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers

hostname cisco7500

aaa new-model
aaa authentication login default radius
aaa authentication login aaa7500kw none
enable password enable7500pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
ip subnet-zero
no ip cef
no ip domain-lookup
ip domain-name cisco.com
ip ssh time-out 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
```

Cisco 12000 Gigabit Switch Router Configuration

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 2 authentication retries. Also, before configuring the SSH server feature onto the router, TACACS+ is specified as the method of authentication.

```
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

hostname cisco12000

boot system flash slot0:gsr-tpgen-mz.082098
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa12000kw none
enable password enable12000pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
redundancy
main-cpu
  auto-sync startup-config
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
ip ssh time-out 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 aaa12000pw
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
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- ip ssh
- show ip ssh
- disconnect ssh

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

> *command* **|** {**begin** | **include** | **exclude**} *regular-expression*

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression “PeakRate” appears:

> **show atm vc | begin PeakRate**

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

ip ssh

To configure SSH control parameters on your router, use the **ip ssh** global configuration command. Use the **no** form of this command to restore the default value.

[no] ip ssh {[time-out *seconds***]} | [authentication-retries** *integer***]}**

Syntax Description

time-out	(Optional) The time interval that the router waits for the SSH client to respond. 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.
authentication-retries	(Optional) The number of attempts after which the interface is reset.
seconds	The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120.
integer	The number of retries, with a maximum of 5 authentication-retries. The default is 3.

Defaults

120 seconds for the timeout timer.

3 authentication-retries.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa** command.

Examples

The following examples configure SSH control parameters on your router:

```
Router(config)# ip ssh time-out
Router(config)# ip ssh authentication-retires 3
```

show ip ssh

To display your router's SSH connections, use the **show ip ssh** privileged EXEC command.

show ip ssh

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

You must enable the SSH server before using this command. If the SSH server is not enabled, this command will generate an error message.

Examples

The following is sample output from the **show ip ssh** command. The number of connections displayed is the same as the number of VTYs used. For example, if “0” connections are displayed, “0” VTYs are defined. By default, there are 5 VTYs defined for 5 possible terminal sessions:

```
Router# show ip ssh
Connection      Version     Encryption     State   Username
    0            1.5            3DES          4    guest
```

disconnect ssh

To terminate a SSH connection on your router, use the **disconnect ssh** privileged EXEC command.

disconnect ssh [vty] *session-id*

Syntax Description

vty	(Optional) Virtual terminal for remote console access.
session-id	The session-id is the number of connections displayed in the **show ip ssh** command output.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was first introduced.

Usage Guidelines

- The **clear line vty** *n* command, where *n* is the connection number displayed in the **show ip ssh** command output, may be used instead of the **disconnect ssh** command.
- When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

Examples

The following example terminates SSH connection number 1:

```
Router# disconnect ssh 1
```

Related Commands

Command	Description
clear line vty *n*	Returns a terminal line to idle state using the privileged EXEC command.

Debug Commands

This section documents the new **debug** command related to the SSH server.

debug ip ssh

To display debug messages for SSH, use the **debug ip ssh** EXEC command. Use the **no** form of the command to disable debugging output.

[**no**] **debug ip ssh**

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging for SSH is not enabled.

Command History

Release	Modification
12.0(5)S	This command was first introduced.

Usage Guidelines

Use the **debug ssh** command to ensure normal operation of the SSH server.

Examples

The following example shows the SSH debugging output:

```
Router# debug ssh
00:53:46: SSH0: starting SSH control process
00:53:46: SSH0: Exchanging versions - SSH-1.5-Cisco-1.25

00:53:46: SSH0: client version is - SSH-1.5-1.2.25
00:53:46: SSH0: SSH_SMSG_PUBLIC_KEY message sent
00:53:46: SSH0: SSH_CMSG_SESSION_KEY message received
00:53:47: SSH0: keys exchanged and encryption on
00:53:47: SSH0: authentication request for userid guest
00:53:47: SSH0: authentication successful for jcisco
00:53:47: SSH0: starting exec shell
```

Glossary

AAA—authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

authentication, authorization, and accounting—See AAA.

IP Security Protocol—See IPSec.

IPSec—IP Security Protocol. 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 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.

Secure Shell—See SSH.

SSH—Secure Shell Protocol. A protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.

TACACS+—Terminal Access Controller Access Control System plus. A security protocol that provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.

TCP—Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission.

Terminal Access Controller Access Control System Plus—See TACACS+.

Transmission Control Protocol—See TCP.

RADIUS—Remote Authentication Dial-In User Service. A distributed client/server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Remote Authentication Dial-In User Service—See RADIUS.