Configuring the Cisco Security Packet Analyzer 2400 Series Appliances

This chapter describes how to configure the Cisco Security Packet Analyzer 2400 series appliances to establish network connectivity, configure IP parameters, and how to perform other required administrative tasks using the Packet Analyzer command line interface (CLI). This chapter also provides information about how to get started with the Packet Analyzer graphical user interface (GUI) and how to perform various system management tasks.

This chapter contains the following sections:

For more advanced Packet Analyzer configuration information, use the Packet Analyzer web server interface or see the *Network Analysis Module Command Reference*.

Logging In For the First Time

After you turn power on and boot the Cisco Security Packet Analyzer 2400 series appliance for the first time, the login prompt displays on the attached console. When shipped from the factory, the root user is preconfigured on the Cisco Security Packet Analyzer 2400 series appliance. The default password for the root user is *root*.

Note You must change the user root password during the first login session.

The root user has access to the root (read/write) level of Packet Analyzer and can enter Packet Analyzer command-line interface (CLI) commands.

To log in to the Cisco Security Packet Analyzer 2400 series appliance for the first time, open a console session or a serial session with the Cisco Security Packet Analyzer appliance.

Note After your initial login, you can enable **telnet** and **ssh** connections to the Packet Analyzer appliance.

Step 1 When the Packet Analyzer login prompt appears, type **root** and press **Enter**.

```
secpa.localdomain login: root
```

Step 2 When the password prompt appears, type **root** and press **Enter**.

After you enter the ID and password, you will be prompted to change the root password.

```
secpa2400-209.localdomain login: root
Password: <secpa1>
Last login: Mon Aug 20 08:28:34 2012 from sjc-vpn2-1516.cisco.com on pts/1

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

System_Alert! Default password has not been changed!
Please enter a new root user password.
Enter new password:
```

Step 3 Enter the new password for the root user, then enter it a second time.

```
Confirm new password:
Successfully changed password for user 'root'
```

We recommend that you make a record of the password, and store this information in a secure location. You should change this password regularly in accordance with your site's password security policies. See Changing the Root Password, page 3-2.

Changing the Root Password

This section describes how to change the root user password after the initial login session. To change the root password:

Step 1 Open a console session or serial session with the Cisco Security Packet Analyzer appliance.

Step 2 When prompted for a username, enter **root**.

The Cisco Security Packet Analyzer 2400 appliance ships from the factory with default settings for user **root** with a password of **root**.

Step 3 When prompted, enter the password for user root.

After you log in as the root user, you have read and write access to the root level of the Cisco Security Packet Analyzer appliance, and you can enter and perform CLI commands.

```
root@hostname#
```

Step 4 Enter the following command to change the root user password.

password root

```
New password:
Confirm password:
```

Step 5 Enter the new password for user root and confirm it.

We recommend that you make a record of the password and store this information in a secure location. You should change this password regularly in accordance with your site's password security policies.

Step 6 Type **exit** to end the session and log out.

Examples

This section provides the following examples:

- Changing the Packet Analyzer Root Password: Example, page 3-3
- Verifying the Packet Analyzer Root Password: Example, page 3-3

Changing the Packet Analyzer Root Password: Example

```
root@secpa2400-209.localdomain# password root
Enter new password:
Confirm new password:
Successfully changed password for user 'root'
```

Verifying the Packet Analyzer Root Password: Example

```
nam1.company.com login: root
Password: <secpa1>
Terminal type: vt100

Cisco Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

root@nam1.company.com#
root@nam1.company.com# exit
```

Resetting the Packet Analyzer Root Password to the Default Value

For information about how to reset the Packet Analyzer root password to the default value, see the *Cisco Prime Network Analysis Module Software User Guide*.

Establishing Network Connectivity

This section describes how to configure a Cisco Security Packet Analyzer 2400 appliance to configure IP parameters in IPv4 environment to establish network connectivity.

Log in to a Cisco Security Packet Analyzer 2400 appliance from the management console and enter the following CLI commands with the appropriate information for your site:

Step 1 Use the **ip address** command to configure the Cisco Security Packet Analyzer appliance IP address. The syntax for this command is as follows:

ip address *ip-address subnet-mask*

Example

```
root@localhost# ip address 172.20.104.126 255.255.255.248
```

Step 2 Use the **ip gateway** command to configure the Cisco Security Packet Analyzer appliance default gateway address. The syntax for this command is as follows:

ip gateway *ip-address*

Example

```
root@localhost# ip gateway 172.20.104.123
```

Step 3 You can use the **exsession** command to enable remote login to the Cisco Security Packet Analyzer appliance using either Telnet or SSH. The syntax for this (optional) command is as follows:

exsession on *(for Telnet)*

or

exsession on ssh *(for SSH)*

Examples

To configure the Cisco Security Packet Analyzer appliance to enable Telnet access:

```
root@localhost# exsession on
```

To configure the Cisco Security Packet Analyzer appliance to enable SSH access:

```
root@localhost# exsession on ssh
```

Step 4 You can use the **ip domain** command to configure the Cisco Security Packet Analyzer appliance system domain name. The syntax for this (optional) command is as follows:

ip domain *name*

Example

```
root@localhost# ip domain your_company.com
```

Step 5 You can use the **ip host** command to configure the Cisco Security Packet Analyzer appliance system hostname.

The syntax for this command is as follows:

ip host *name*

Example

```
root@localhost# ip host secpa_machine
```

Step 6 You might (optionally) want to use the **ip nameserver** command to configure one or more name servers for the Cisco Security Packet Analyzer appliance.

The syntax for this command is as follows:

ip nameserver *ip-address [ip-address] [ip-address}*

Examples

```
root@localhost# ip nameserver 172.20.104.10
root@localhost# ip nameserver 172.20.104.10  172.20.104.20  172.20.104.30
```

Checking Your Configuration

After you finish configuring the Cisco Security Packet Analyzer appliance for network connectivity, it is a good idea to check your connectivity and verify the IP parameters you have just configured for the Cisco Security Packet Analyzer appliance.

Step 1 Use the **ping** command to check connectivity between the Cisco Security Packet Analyzer appliance and a network device.

The syntax for this command is as follows:

ping *{hostname | ip-address}*

Examples

```
root@localhost# ping secpa_machine.your_company.com
root@localhost# ping 172.20.104.10
```

The following is an example of the **ping** command showing successful connectivity:

```
root@secpa_machine.your_company.com# ping 172.20.104.10
PING 172.20.104.10 (172.20.104.10) 56(84) bytes of data.
64 bytes from 172.20.104.10: icmp_seq=1 ttl=254 time=1.27 ms
64 bytes from 172.20.104.10: icmp_seq=2 ttl=254 time=1.13 ms
64 bytes from 172.20.104.10: icmp_seq=3 ttl=254 time=1.04 ms
64 bytes from 172.20.104.10: icmp_seq=4 ttl=254 time=1.08 ms
64 bytes from 172.20.104.10: icmp_seq=5 ttl=254 time=1.11 ms

--- 172.20.104.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.043/1.129/1.278/0.090 ms
root@secpa_machine.your_company.com#
```

Step 2 Use the **show ip** command to verify that you have configured the Cisco Security Packet Analyzer appliance IP parameters the way you want them.

The syntax for this command is as follows:

show ip

```
root@localhost# show ip root@nam1.company.com# show ip
```

The following is an example of the **show ip** command output that shows a configured Cisco Security Packet Analyzer appliance:

```
root@secpa-2400-96.cisco.com# show ip

==== IP/DNS Configuration ====
IPv4 Address/Netmask:    172.20.124.96 / 255.255.255.0
IPv4 Default Gateway:    172.20.124.47
IPv4 Broadcast:          172.20.124.255
IPv6 Address:            2001:20:1:100::96/64
IPv6 Default Gateway:    2001:20:1:100::1
Host Name:               appliance-2404-96.cisco.com
Nameserver(s):           171.70.168.183


==== Remote Access & Authentication ====
HTTP:                    Enabled (on port 80)
HTTPS:                   Disabled
SSH:                     Enabled (on port 22)
Telnet:                  Enabled (on port 23)
TACACS+:                 Disabled


==== File Sharing Services ====
SMB:                     Disabled
SFTP:                    Disabled
```

Enabling the Cisco Security Packet Analyzer Web Server

This section describes how to enable the Cisco Security Packet Analyzer web server and browser-based access to the Packet Analyzer graphical user interface (GUI).

Note You can enable the Packet Analyzer to function as an HTTP server or an HTTPS secure server, but not as both simultaneously.

To enable the Packet Analyzer web server and provide browser-based access, confirm that your web browser supports your Packet Analyzer software release.

Note For a list of supported browsers, see the Cisco Security Packet Analyzer software release notes.

To enable the Packet Analyzer web server:

Step 1 Open a Telnet or SSH session to the Cisco Security Packet Analyzer appliance and at the password prompt, enter your password.

telnet {ip-address | hostname}

or

ssh {ip-address | hostname}

Step 2 Enter one of the following commands to enable either an HTTP server or an HTTPS secure server:

To enable the Packet Analyzer HTTP web server:

ip http server enable

To enable the Packet Analyzer HTTPS secure web server:

ip http secure server enable

The Packet Analyzer requests a web administrator user name.

```
Enabling HTTP server...

No web users are configured.
Please enter a web administrator user name [admin]: <CR>
```

The Packet Analyzer web server requires at least one properly-configured web administrator. If the Packet Analyzer does not prompt you for a web username and password, then at least one web administrator was previously configured.

Step 3 Enter the username of the web administrator. Otherwise, press **Enter** to use the default web administrator username *admin*.

The Packet Analyzer requests a password for the web administrator, then requests the password to be entered again to ensure accuracy.

```
New password: <adminpswd>

Confirm password: <adminpswd>
```

Step 4 Enter the password for the web administrator and confirm it.

Note Because this document is available to the public by way of Cisco.com, it is a good idea to change this and all default passwords as soon as possible.

Step 5 To check the Packet Analyzer web server functionality, launch an approved internet browser and enter the IP address or host and domain name in the browser address field.

Note For a list of supported browsers, see the Cisco Security Packet Analyzer software release notes.

If the Cisco Security Packet Analyzer 2400 series appliance web server is properly configured, you should access the Packet Analyzer login window.

At this point, the only user able to log in to the Packet Analyzer web server is the administrative user you configured when you enabled the web server.

Verifying System Status

To verify the status of an installation, upgrade, or downgrade or to troubleshoot problems, use commands from those listed in Table 3-1, Common Diagnostic and Show Commands.

Note

- The tables in these sections show only common managed device and network module commands.
  - To view a complete list of available commands, type **?** at the prompt (Example: `user@secpa_host.domain# ?`).
  - To view a complete list of command keyword options, type **?** at the end of the command (Example: `secpa_host.domain# ip ?`).
- The tables group commands by the configuration mode in which they are available. If the same command is available in more than one mode, it might act differently in each mode.

Note Many **show** commands include the keyword option to display diagnostic output on your screen or to pipe it to a file or a URL.

Table 3-1 Common Diagnostic and Show Commands

Command	Purpose
clear access-log	Clear web access log.
clear captured-data-files	Delete all captured files in Packet Analyzer local drive.
clear monitoring-data	Delete all monitoring data on Packet Analyzer.
clear system-alerts	Clear system alerts.
clear system-passwords	Restore default CLI passwords of application image.
ping	Pings a specified IP address or hostname to check network connectivity.
show access-log	Displays the web access log.
show application	Displays the protocol grouping information.
show audit-trail	Displays the web GUI logins and CLI access settings.
show autocreate-data-source	Displays the data source autocreation settings.
show cdb	Displays information about a CDB file.
show cdp settings	Displays the CDP settings.
show certificate	Displays installed certificate.
show certificate-request	Displays certificate signing request.
show clock	Displays the current date and time.

Table 3-1 Common Diagnostic and Show Commands (continued)

Command	Purpose
show configuration	Displays the current bootloader configuration as entered using the **configure** command.
show data-source	Displays the data sources.
show date	Displays the current date and time.
show debug	Displays the debug information.
show device	Displays the remote devices.
show email	Displays EMail settings.
show entity	Displays the entity MIB information.
show flow-cache-sizes	Displays the Packet Analyzer internal cache sizes.
show ftp	Displays the FTP settings for schedule reports.
show hosts	Displays the hosts entries.
show inventory	Displays the system inventory information.
show ip	Displays the IP parameters.
show local-storage all	Displays all physical disks and virtual drives.
show local-storage physical	Displays all physical disks.
show local-storage progress	Displays progress of drive rebuilds.
show local-storage virtual	Displays all virtual drives.
show log	Displays the Packet Analyzer config, patch, report, and upgrade logs
show memory	Displays the amount of installed memory, amount available, and the amount currently used by the system.
show monitor	Displays the configured collections.
show patches	Displays any installed patches.
show preferences	Displays the Packet Analyzer web interface preferences.
show protocol-feature	Displays the parsing protocol feature settings.
show remote-storage	Displays the remote storage settings for storing capture data.
show snmp	Displays the SNMP parameters.
show syslog-settings	Displays the Packet Analyzer syslog settings.
show system-alerts	Displays Packet Analyzer failures and problems.
show tech-support	Displays general information about the host router that is useful to Cisco technical support for problem diagnosis.
show time	Displays the Packet Analyzer system time settings.
show trap-dest	Displays the Packet Analyzer trap destination.
show version	Displays information about the loaded router, software or network module bootloader version, and also hardware and device information.
show waas	Displays WAAS devices and data sources.

Table 3-1 Common Diagnostic and Show Commands (continued)

Command	Purpose
show web-publication	Displays web publication settings.
show web-users	Displays a list of current local web users.

Configuring a Monitored Device

After you connect an output interface of a monitored (or managed) device to the monitoring ports of the Cisco Security Packet Analyzer 2400 series appliance, you must also configure the monitored device to send data to that interface. You do this in two steps:

- Configuring a Monitored Device Interface
- Span the port of the monitored device to use the Cisco Security Packet Analyzer 2400 series appliance as a destination port

Configuring a Monitored Device Interface

At the monitored device, configure the connection to the Cisco Security Packet Analyzer 2400 series appliance as a trunk port, but use the no negotiate option. Using the no negotiate option on the monitored device, precludes the switch or router from performing dynamic trunk protocol (DTP) with the appliance monitoring port.

The following example shows how to configure a switch port connected to the appliance monitoring port as Te 7/29.

From the monitored device command line, enter a CLI command like the following:

show run interface ethernet 4/37

```
n7k-4# show run int ethernet 4/37
!Command: show running-config interface Ethernet4/37
!Time: Mon Apr 27 09:49:03 2015

version 7.2(0)D1(1)

interface Ethernet4/37
  description "Connected to secpa data port"
  switchport
  switchport monitor
  mtu 9216
```

Creating a SPAN Session

A SPAN session is required to SPAN the monitored device's traffic to the port connected to the monitoring port of the appliance. You can create a SPAN session using the monitored device's CLI or using the Packet Analyzer appliance GUI.

For information about how to use the Packet Analyzer GUI to set up the SPAN session, see the *Cisco Security Packet Analyzer User Guide*.

Opening and Closing a Telnet or SSH Session to the Packet Analyzer

This procedure opens and closes a Telnet or SSH session to the Packet Analyzer. This procedure is not commonly performed, because you would typically use the Packet Analyzer GUI to monitor and maintain the Packet Analyzer. If, however, you cannot access the Packet Analyzer GUI, you might want to use Telnet or SSH to troubleshoot from the Packet Analyzer CLI.

If your Cisco Security Packet Analyzer 2400 series appliance is not properly configured for Telnet or SSH access (see the following Prerequisites, page 3-11 section), you can open a Telnet session to the managed device to which the Cisco Security Packet Analyzer 2400 series appliance is connected, then open a Packet Analyzer console session from the managed device.

Prerequisites

- Configure the Packet Analyzer system IP address. Optionally, set the Packet Analyzer system hostname.
- Verify Packet Analyzer network connectivity by performing one of the following ping tests:
  - From a host beyond the gateway, ping the Packet Analyzer system IP address.
  - From the Packet Analyzer CLI, ping the Packet Analyzer system default gateway.

Telnet Prerequisites

- Enter the **exsession on** Packet Analyzer CLI command.

SSH Prerequisites

- Enter the **exsession on ssh** Packet Analyzer CLI command.

Summary Steps

1. **telnet** {*ip-address* | *hostname*}
   or
   ssh {*ip-address* | *hostname*}
2. At the login prompt, enter **root**.
3. At the password prompt, enter your password.
   or
   If you have not changed the password from the factory-set default, enter **root** as the root password.
4. Perform the tasks that you need to perform in the Packet Analyzer CLI. When you want to end the Telnet or SSH session to the Packet Analyzer and return to the Cisco IOS CLI, complete Step 5 and Step 6.
5. **exit**
6. **logout**

Detailed Steps

	Command or Action	Purpose

Step 1	**telnet** {*ip-address* | *hostname*}
	or
	ssh {*ip-address* | *hostname*}
	
	Example:
	`host.domain# telnet 10.20.30.40`
	
	Example:
	`host.domain# ssh 10.20.30.40`
		Logs in to a host that supports Telnet.
		or
		Starts an encrypted session with a remote networking device.
		• Use the Packet Analyzer system IP address or Packet Analyzer system hostname.

Step 2	At the login prompt, enter **root**. **Example:** `login: root`	Accesses the root (read/write) level of Packet Analyzer.
Step 3	At the password prompt, enter your password. or If you have not changed the password from the factory-set default, enter **root** as the root password. **Example:** `Password: root`	
Step 4	Perform the tasks that you need to perform in the Packet Analyzer CLI. When you want to end the Telnet or SSH session to the Packet Analyzer and return to the Cisco IOS CLI, complete Step 5 and Step 6.	For help using Packet Analyzer CLI commands.

Step 5	**exit**
	
	Example:
	`root@localhost(sub-custom-filter-capture)# exit`
	`root@localhost#`
		Leaves a subcommand mode.
		• Return to command mode.

Step 6	**logout**
	
	Example:
	`root@localhost# logout`
	
	`Connection closed by foreign host.`
		Logs out of the Packet Analyzer system.

Examples

Opening and Closing a Telnet Session to the Packet Analyzer Using the Packet Analyzer System IP Address

```
secpa_host> telnet 172.20.105.215
Trying 172.20.105.215 ... Open

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
```

```
Copyright (c) 2012-2016 by Cisco Systems, Inc.

login: root
Password: <password>
Terminal type: vt100

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

WARNING! Default password has not been changed!
root@secpa.company.com#
root@secpa.company.com# logout

[Connection to 172.20.105.215 closed by foreign host]
secpa_host>
```

Opening and Closing an SSH Session to the Packet Analyzer Using the Packet Analyzer System Hostname

```
host [/home/user] ssh -l root@namappl
root@namappl's password: <password>
Terminal type: vt100

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

WARNING! Default password has not been changed!
root@secpa.company.com#
root@secpa.company.com# logout

Connection to secpa closed.
host [/home/user]
```

Setting up the CIMC

The Cisco Integrated Management Controller (CIMC) is a built-in feature of Cisco UCS servers that provides a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server remotely. The Cisco Security Packet Analyzer 2400 series appliances appliance are based on the Cisco UCS server platform, and thus include the CIMC functionality.

While setting up the CIMC is not strictly necessary to use the Packet Analyzer, certain administrative and troubleshooting tasks can only be performed via the CIMC. Therefore, it is highly recommended to configure the CIMC with an IP address so that it can be accessed if needed.

To configure an IP address for the CIMC, reboot the Cisco Security Packet Analyzer appliance and press F8 when prompted to enter the "Cisco IMC Configuration Utility". Set the "NIC mode" to "Shared LOM", and configure the IP and VLAN parameters as appropriate. For more details on the CIMC configuration process, see the *Cisco UCS C240 M3 Server Installation and Service Guide*.

You can also setup a dedicated CIMC connection using the UCS management port labeled M.

Note The UCS management port labeled M is different from Packet Analyzer management port LAN1.

Setting up Serial Console Connection

There are two ways to connect to the Packet Analyzer serial console:

- Serial over LAN (SoL)–Allows access to the Packet Analyzer serial console through the web-based GUI or SSH-based CLI of CIMC. This access method is configured by default.
- Physical external serial console connector (RJ-45)–Allows access to the Packet Analyzer serial console through a direct serial cable or terminal server. See section Setting up Serial Console Access through External RJ-45 Port, page 3-14 for details.

Packet Analyzer supports two serial console ports: com0 and com1. The Packet Analyzer CLI can be accessed through either of these ports. However, only the com0 port provides full output and interactivity during the bootup process. The two serial console options (SoL or RJ-45 connector) cannot use com0 at the same time, so you should assign com0 to the option you would customarily use within your environment. By default, the Packet Analyzer is configured with SoL on com0, so if SoL is your preferred method of access, then you need not do anything more. If you prefer to assign com0 to the RJ-45 serial port, then follow the steps in section Setting up Serial Console Access through External RJ-45 Port.

Setting up Serial Console Access through External RJ-45 Port

See Figure 5-2 for Serial connector (RJ-45) location.

To setup serial console access through the external RJ-45 port:

Step 1 Log into the CIMC GUI.

Step 2 Click the **Server** tab and then click **Remote Presence**.

Step 3 Click the **Serial over LAN** tab.

Step 4 If you do not want to use Serial over LAN, uncheck the **Enabled** check box. This will make the serial console accessible on com0 through the RJ-45 port. Alternatively, if you prefer to use the RJ-45 serial console primarily, but maintain Serial over LAN as a secondary method for access to the Packet Analyzer CLI, then keep Serial over LAN enabled, but change **Com Port** to com1.

Step 5 Click the **Save Changes** button.

Console access through the RJ-45 console port will be enabled. Configure your terminal emulator or terminal server to use 9600 baud/bps, 8-N-1 when connecting to the console.

In some cases, it may be necessary to power cycle the Packet Analyzer appliance before the serial console works. From the CIMC GUI, click the **Server** tab and click **Summary**, and then click **Power Cycle Server**.

Shutting Down and Starting Up the Appliance

To shut down a Cisco Security Packet Analyzer 2400 series appliance, issue the Packet Analyzer CLI **shutdown** command.

The Cisco Security Packet Analyzer 2400 series appliance reboots after you press the Power button. You can also switch on the server through the CIMC web interface.