Contents

Preface
Who Should Use This Guide................................................................. 10
Summary of Contents........................................................................ 11
Appendices ....................................................................................... 11
Related Documentation.................................................................... 12
More Information............................................................................. 14
Feedback......................................................................................... 15

Chapter 1
Introduction
Overview.......................................................................................... 18
SecurePlatform Hardware Requirements ............................................ 19
SecurePlatform Pro.......................................................................... 20

Chapter 2
Preparing to Install SecurePlatform
Preparing the SecurePlatform Machine............................................. 22
Hardware Compatibility Testing Tool.............................................. 23
  Introduction to the Hardware Compatibility Testing Tool............ 23
  Booting from the CD.................................................................... 24
  Using the Hardware Compatibility Testing Tool....................... 24
BIOS Security Configuration Recommendations......................... 25
Installing Products on SecurePlatform............................................ 26

Chapter 3
Configuration
Using the Command Line................................................................. 28
  First Time Setup Using the Command Line......................... 28
  Using sysconfig......................................................................... 29
Check Point Products Configuration............................................... 31
Using the Web Interface................................................................. 32
  First Time Setup Using the Web Interface............................ 32
Web Interface Options..................................................................... 32
  Status 33
  Network 33
  Device 35
  Product Configuration 42
First Time Reboot and Login.......................................................... 45

Chapter 4
Administration
Managing Your SecurePlatform System........................................... 48
  Connecting to SecurePlatform by Using Secure Shell............ 48
  User Management...................................................................... 49
    Standard Mode 49
    Expert Mode 49
Dynamic Routing ................................................................. 107
To enable dynamic routing 108
To Configure Dynamic Routing 109
Backward Compatibility Support 109
Supported Protocols 109
Enabling and Disabling Dynamic Routing Support 109
Configuring Dynamic Routing Protocols 110
Tracing and Logging Options 110
Backup and Restore 110
Command Line Interface ....................................................... 111
Overview 111
Command Line Editing and Completion 111
Context-Sensitive Help 111
Command History 111
Disabling/Enabling CLI Tracing 112

Appendix A

Installation on Computers without Floppy or CDROM Drives
General Procedure ................................................................. 114
Client Setup ............................................................................. 114
Server Setup ............................................................................. 115
Required Packages ............................................................... 115
PXELINUX Configuration Files 116
DHCP Daemon Setup ........................................................... 116
TFTP and FTP Daemon Setup ............................................... 117
Hosting Installation Files ........................................................ 118
Preface

In This Chapter

Who Should Use This Guide
Summary of Contents
Related Documentation
More Information
Feedback
Who Should Use This Guide

Who Should Use This Guide

This guide is intended for administrators responsible for maintaining network security within an enterprise, including policy management and user support.

This guide assumes a basic understanding of

- System administration.
- The underlying operating system.
- Internet protocols (IP, TCP, UDP etc.).
Summary of Contents

This guide covers the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Introduction”</td>
<td>This chapter covers the two “flavors” of SecurePlatform, and hardware requirements</td>
</tr>
<tr>
<td>Chapter 2, “Preparing to Install SecurePlatform”</td>
<td>This chapter covers everything you need to do before installing SecurePlatform</td>
</tr>
<tr>
<td>Chapter 3, “Configuration”</td>
<td>This chapter covers using the command line interface, the web interface, and what happens when you log in for the first time</td>
</tr>
<tr>
<td>Chapter 4, “Administration”</td>
<td>This chapter covers the various aspects of SecurePlatform administration</td>
</tr>
<tr>
<td>Chapter 5, “SecurePlatform Pro Advanced Routing Suite”</td>
<td>This chapter covers SecurePlatform’s support for dynamic routing protocols</td>
</tr>
</tbody>
</table>

Appendices

This guide contains the following appendices:

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A, “Installation on Computers without Floppy or CDROM Drives”</td>
<td>This chapter covers alternative means of installing SecurePlatform</td>
</tr>
</tbody>
</table>
Related Documentation

This release includes the following documentation

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Security Installation and Upgrade Guide</td>
<td>Contains detailed installation instructions for Check Point network security products. Explains the available upgrade paths from versions R60-65 to the current version.</td>
</tr>
<tr>
<td>High-End Installation and Upgrade Guide</td>
<td>Contains detailed installation instructions for the Provider-1 and VSX products, including hardware and software requirements and licensing requirements. Explains all upgrade paths for Check Point products specifically geared towards upgrading to the current version.</td>
</tr>
<tr>
<td>Firewall Administration Guide</td>
<td>Describes how to control and secure network access and VoIP traffic; how to use integrated web security capabilities; and how to optimize Application Intelligence with capabilities such as Content Vectoring Protocol (CVP) applications, URL Filtering (UFP) applications.</td>
</tr>
<tr>
<td>IPS Administration Guide</td>
<td>Describes how to use IPS to protect against attacks.</td>
</tr>
<tr>
<td>Virtual Private Networks Administration Guide</td>
<td>Describes the basic components of a VPN and provides the background for the technology that comprises the VPN infrastructure.</td>
</tr>
</tbody>
</table>
# Related Documentation

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Eventia Reporter Administration Guide</strong></td>
<td>Explains how to monitor and audit traffic, and generate detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for all events logged by Check Point Security Gateways, SecureClient and IPS.</td>
</tr>
<tr>
<td><strong>SecurePlatform/SecurePlatform Pro Administration Guide</strong></td>
<td>Explains how to install and configure SecurePlatform. This guide will also teach you how to manage your SecurePlatform machine and explains Dynamic Routing (Unicast and Multicast) protocols.</td>
</tr>
<tr>
<td><strong>Provider-1/SiteManager-1 Administration Guide</strong></td>
<td>Explains the Provider-1 security management solution. This guide provides details about a three-tier, multi-policy management architecture and a host of Network Operating Center oriented features that automate time-consuming repetitive tasks common in Network Operating Center environments.</td>
</tr>
</tbody>
</table>
More Information

- For additional technical information about Check Point products, consult Check Point's SecureKnowledge at http://support.checkpoint.com.

- To view the latest version of this document in the Check Point User Center, go to: http://support.checkpoint.com.
Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

cp_techpub_feedback@checkpoint.com
Chapter 1
Introduction

In This Chapter

Overview  page 18
SecurePlatform Hardware Requirements  page 19
SecurePlatform Pro  page 20
Thank you for using SecurePlatform. This document describes how to prepare a hardware platform for SecurePlatform, and how to configure and administer SecurePlatform.

SecurePlatform is distributed on a bootable CD ROM which includes Check Point’s product suite, that includes software blades for firewall, VPN, and many others. The SecurePlatform CD ROM can be installed on any PC with an Intel x86 compatible architecture. SecurePlatform includes a customized and hardened operating system, with no unnecessary components that could pose security risks. The system is pre-configured and optimized to perform its task as a network security device, requiring only minimal user configuration of basic elements, such as IP addresses, routes, etc.

On most systems, this installation process runs less than five minutes, resulting in a network security device ready to be deployed.

SecurePlatform allows easy configuration of your computer and networking aspects, as well as the Check Point products installed. An easy-to-use shell provides a set of commands, required for easy configuration and routine administration of a security system, including: network settings, backup and restore utilities, upgrade utility, system log viewing, control, and much more. A Web GUI enables most of the administration configuration, as well as the first time installation setup, to be performed from an easy-to-use Web interface.
SecurePlatform Hardware Requirements


For details regarding SecurePlatform on specific hardware platforms, see: http://www.checkpoint.com/services/techsupport/hcl/

For information about the recommended configuration of high-performance systems running Check Point Performance Pack, see the Check Point Performance Pack R70 Administration Guide at http://supportcontent.checkpoint.com/documentation_download?ID=8739
SecurePlatform Pro

SecurePlatform Pro is an enhanced version of SecurePlatform. SecurePlatform Pro adds advanced networking and management capabilities to SecurePlatform such as:

- Dynamic routing
- Radius authentication for SecurePlatform administrators

To install “SecurePlatform Pro” select the “SecurePlatform Pro” option during the installation.

To convert regular SecurePlatform to SecurePlatform Pro, from the expert mode command line run: “pro enable”.

Note - SecurePlatform Pro requires a separate license that must be installed on the Security Management server that manages the SecurePlatform Pro Security Gateways.

For information about RADIUS support, see: "How to Authenticate Administrators via RADIUS" on page 50

For information regarding advanced routing, see the SecurePlatform Pro & Advanced Routing Command Line Interface.

For all intents and purposes, wherever the name SecurePlatform is used, SecurePlatform Pro is implicitly included.
Chapter 2
Preparing to Install SecurePlatform

In This Chapter

Preparing the SecurePlatform Machine  page 22
Hardware Compatibility Testing Tool  page 23
BIOS Security Configuration Recommendations  page 25
Installing Products on SecurePlatform  page 26
Preparing the SecurePlatform Machine

SecurePlatform can be installed from a CD drive or from a network server.

Before you begin the SecurePlatform installation process, ensure that the following requirements are met:

- If the target computer has a CD drive, make sure that the system BIOS is set to reboot from this drive as the first boot option (this BIOS Setup Feature is usually named Boot Sequence).

- If your target computer cannot boot from a CD drive, or if you wish to install using a remote file server, refer to the instructions in the Internet Security Products Installation and Upgrade Guide at http://supportcontent.checkpoint.com/documentation_download?ID=8753

⚠️ Warning - The installation procedure erases all hard disks, so the former operating system cannot be recovered.

>Note - SecurePlatform can be installed on a computer without a keyboard or VGA display by using a serial console attached to a serial port.
Hardware Compatibility Testing Tool

In This Section

Introduction to the Hardware Compatibility Testing Tool page 23
Booting from the CD page 24
Using the Hardware Compatibility Testing Tool page 24

Introduction to the Hardware Compatibility Testing Tool

The Hardware Compatibility Testing Tool enables you to determine whether SecurePlatform is supported on a specific hardware platform.

The utility is available for download as a CD ISO image (hw.iso). The ISO image can be burned on the blank CD-R or on the CD-RW media, using a CD-burning tool.

Note - You must specify that you are burning “CD image” and not single file.

Run the Hardware Compatibility Testing Tool by booting from CD.

The tool detects all hardware components on the platform, checks whether they are supported, and displays its conclusions: whether SecurePlatform can be installed on the machine (supported I/O devices found, support mass storage device was found), and the number of supported and unsupported Ethernet controllers detected.

It is possible to view detailed information on all the devices found on the machine. You can also save detailed information on a diskette, on TFTP server, or dump it via the serial port. This information can be submitted to Check Point Support in order to add support for unsupported devices.

SecurePlatform requires the following hardware:

• I/O Device (either Keyboard & Monitor, or Serial console).
• mass storage device
• at least one supported Ethernet Controller (If SecurePlatform is to be configured as a Check Point Security Gateway, more than one controller is needed)
Booting from the CD

The tool makes no modifications to the tested hardware platform, so it is safe to use.

**Booting from the CD**

Run the Hardware Compatibility Testing Tool by booting from the CD that contains it.

If no keyboard and monitor are connected to the hardware platform, the serial console can be used to perform the hardware detection.

To boot from the CD:

1. Configure the BIOS of the machine to boot from the CD drive.
2. Insert the CD into the drive.
3. Boot the machine.

**Using the Hardware Compatibility Testing Tool**

The hardware tool automatically tests the hardware for compatibility.

*Note* - A simple, “naïve” detection tool is included on the boot diskette. If for some reason, the complete detection tool is unavailable (e.g., the CDR drive is not supported), you can still use the simple tool to get some information on your hardware. The simple tool is available from the ‘Installation Method’ screen, by pressing the **Produce Hardware** button.

When it finishes, the tool displays a summary page with the following information:

- statement whether the Platform is suitable for installing SecurePlatform
- number of supported and unsupported mass storage devices found
- number of supported and unsupported Ethernet Controllers found

Additional information can be obtained by pressing the **Devices** button. The devices information window lists all the devices, found on the machine (grouped according to functionality).

Use the arrow keys to navigate through the list.

Pressing **Enter** on a specific device displays detailed information about that device.

The detailed information can be saved to a diskette, to a TFTP Server, or dumped through the Serial Console. This action can be required in cases where some of the devices are not supported.
BIOS Security Configuration Recommendations

The following are BIOS configuration recommendations:

- Disable the “boot from floppy” option in the system BIOS, to avoid unauthorized booting from a diskette and changing system configuration.
- Apply a BIOS password to avoid changing the BIOS configuration. Make sure you memorize the password, or keep it in a safe place.
Installing Products on SecurePlatform

Installing Products on SecurePlatform

For details of how to install Check Point products on SecurePlatform, refer to the Check Point Internet Security Products Installation and Upgrade Guide:
http://supportcontent.checkpoint.com/documentation_download?ID=8753
Chapter 3

Configuration

In This Chapter

Using the Command Line  page 28
Using the Web Interface  page 32
First Time Reboot and Login  page 45

SecurePlatform enables easy configuration of your computer and networking setup, and the Check Point products installed on them.
Using the Command Line

This section describes the `sysconfig` application, which provides an interactive menu system for all configuration aspects. Configuration can also be done using command line utilities provided by the SecurePlatform Shell. The SecurePlatform Shell is discussed in “SecurePlatform Shell” on page 54.

First Time Setup Using the Command Line

After the installation from the CD has been completed, and the computer has been rebooted, a first time setup is required in order to:

- configure the network settings
- apply the license
- select which products will be installed
- perform the initial setup, if selected

Perform the first time setup, as follows:

1. Run the `sysconfig` command from the console to configure SecurePlatform, using a text interface.
2. The command line setup wizard begins, and guides you through the first-time configuration.
3. Select “n” to proceed to the next menu, or “q” to exit the Wizard, and press Enter.
4. If you selected “n” and pressed Enter, the Network Configuration menu options are displayed. They are:
   - Host Name (Set/Show Host Name)
   - Domain Name (Set/Show Domain Name)
   - Domain Name Servers (Add/Remove/Show Domain Name Servers)
   - Network Connections (Add/Configure/Remove/Show Connection)
   - Routing (Set/Show Default Gateway)
5. You must configure the following:
   • the computer's name
   • the domain name, and up to three DNS servers
   • the computer's network interfaces
   • the default gateway

6. Enter the desired option number and press Enter.
   The Choose an action menu operation options are displayed.

7. Enter the desired operation option number and press Enter. (Select “e” and press Enter to return to the previous menu.)

8. When you have completed the Network Configuration, select n and press Enter to proceed to the next menu, Time and Date Configuration. (Select p and press Enter to return to the previous menu, or select q and press Enter to exit the Wizard.)

   In the Time and Date Configuration menu you can enter the current date and time, as well as setting the time zone.

   Note - This concludes the SecurePlatform operating system installation. For detailed installation instructions for a specific product, refer to the relevant documentation for that product.

Using sysconfig

Once you have performed the first time setup, via the command line setup wizard, you can use sysconfig to modify your configuration.

To run sysconfig, login to SecurePlatform and enter sysconfig at the prompt.

The sysconfig main menu lists various configuration items, (note that all configuration items must be defined). We recommend step by step configuration, by addressing each menu item in sequence, one after the other.

Select a menu item by typing the relevant number and pressing Enter. Selecting a main menu option displays an additional menu for setting or viewing various configuration items. To return to the main menu, select the menu item Done. To quit, select Exit from the main menu.

When selecting a set option, sysconfig prompts you to enter all relevant configuration parameters. As soon as all the parameters are completed, the change is applied.
Using sysconfig

Note - Entering e at any point during sysconfig takes you one menu level up.

Table 3-1 Sysconfig Configuration Options

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Inside Each Menu Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Host Name</td>
<td>Set or show host name.</td>
</tr>
<tr>
<td>2 Domain Name</td>
<td>Set or show domain name.</td>
</tr>
<tr>
<td>3 Domain Name Servers</td>
<td>Add or remove domain name servers, or show configured domain name servers.</td>
</tr>
<tr>
<td>4 Time &amp; Date</td>
<td>Set the time zone, date and local time, or show the date and time settings.</td>
</tr>
<tr>
<td>5 Network Connections</td>
<td>Add or remove connections, configure network connections, or show configuration of network connections.</td>
</tr>
<tr>
<td>6 Routing</td>
<td>Add network and route, add new host, set default gateway, delete route, or show routing configuration.</td>
</tr>
<tr>
<td>7 DHCP Server Configuration</td>
<td>Configure SecurePlatform DHCP Server.</td>
</tr>
<tr>
<td>8 DHCP Relay Configuration</td>
<td>Setup DHCP Relay.</td>
</tr>
<tr>
<td>9 Export Setup</td>
<td>Exports Check Point environment.</td>
</tr>
<tr>
<td>10 Products Installation</td>
<td>Installs Check Point products (cpconfig). For more information, see the product installation instructions.</td>
</tr>
<tr>
<td>11 Products Configuration</td>
<td>Configure Check Point products (cpconfig). For more information, see “Check Point Products Configuration” on page 31.</td>
</tr>
</tbody>
</table>
Check Point Products Configuration

- To configure installed Check Point products, run the `cpconfig` application from the SecurePlatform Shell, or select the `cpconfig` option in the `sysconfig` application. For more information about configuring Check Point products, refer to the Check Point Internet Security Products Installation and Upgrade Guide. http://supportcontent.checkpoint.com/documentation_download?ID=8753

As soon as you finish the Check Point products configuration procedure as part of the first time setup, you will be asked to reboot your system. After reboot, your system will be available for use.

Note - You must run the Check Point Products Configuration procedure (`cpconfig`) in order to activate the products.

- For information on how to connect to your Security Management server, using the Check Point SmartConsole, refer to the Check Point Internet Security Products Installation and Upgrade Guide http://supportcontent.checkpoint.com/documentation_download?ID=8753

- For information on how to set up a Firewall and Address Translation policy, see the Firewall Administration Guide at http://supportcontent.checkpoint.com/documentation_download?ID=8738
Using the Web Interface

This section describes SecurePlatform's Web interface. Most of the common operations can be done by using the Web Interface.

Note - The Web interface is not accessible in the FIPS 140-2 compliant mode.

First Time Setup Using the Web Interface

After the installation from the CD has been completed, and the computer has been rebooted, a first time setup using the First-Time Configuration Wizard is required in order to:

- configure the network settings
- configure the time/date/time zone
- configure the allowed IPs of SSH and administration Web UI clients
- select which products will be installed
- set the initial configuration of installed products

For the details of each setting, see "Web Interface Options".

Web Interface Options

The initial configuration of SecurePlatform is performed using the First-Time Configuration Wizard. The SecurePlatform Web UI allows you to further configure SecurePlatform.

To connect to the SecurePlatform Web interface:

1. Initiate a connection from a browser to the administration IP address: https://<Device_IP_address>.

Note - Pop-ups must always be allowed on https://<device_IP_address>.

The login page appears.

2. Login with the system administrator login name/password and click Login.
Web Interface Options

(To log out of the Web Interface, click Close, in the top right of the page.)

The configuration options are as follows:

**Status**

The Status category provides a concise summary of the system’s functionality.

**Device Status**

This page provides a summary of the device status, and displays information, such as the machine host name, Version and Build, and Installation Type.

**Network**

This category provides the tools to specify the management parameters of your network settings, such as physical network interfaces, VLANs, Routing, DNS, and other devices.

**Connections**

This page enables you to edit the properties of existing network connections (for example, xDSL connections using PPPoE or PPTP) and to add VLANs to ethernet interface.

The Network Connections table displays all available network connections.

To configure network connections:

1. Click the specific interface link to edit the properties of a specific connection.
2. Select the specific interface and click Delete to delete a selected connection.

**Note** - You can disable an interface, by selecting the specific interface, and clicking the Down button. Loopback and Ethernet connection cannot be deleted.

3. To add a connection, Click New and select the connection type from the drop-down list. Click Apply
4. Click Refresh to refresh the table (in case the configuration was changed while you were on this page).
Web Interface Options

Routing

This page enables you to manage the routing table on your device. You can add a static or default route, or delete them.

Note - You cannot edit an existing route. To modify a specific route, delete it and create a new route in its place. Be careful not to delete a route that allows you connect to the device.

To delete a route:

- Select the specific route, and click Delete.

To configure routing:

On the Routing Table page, click New. The Add Route drop-down box is displayed.

The options are:

- Route
- Default Route

To add a new route:

1. Select Route. The Add New Route page appears.
2. On the Add New Route page, supply a:
   a. Destination IP Address
   b. Destination Netmask
   c. Interface (from the drop-down box)
   d. Gateway
   e. Metric
3. Click Apply.

To add a default route:

1. Select Default Route. The Add Default Route page appears.
2. On the Add Default Route page, supply a:
   a. Gateway
   b. Metric
   c. Click Apply.
DNS

In the DNS page, define up to three DNS servers.

Domain

In the Domain page:
- Supply a Hostname.
- Supply a Domain name.
- Select a primary interface from the drop-down box. The Hostname will be associated with the IP of this interface.

Hosts

This page enables you to configure the host's local resolving configuration. You can add a new host by clicking New, and delete an existing entry, by selecting the specific Hostname, and clicking Delete.

To add a Host:
1. Click New. The Add Host page is displayed.
2. In the Add Host page:
   - Supply a Hostname.
   - Supply a Host IP Address
3. Click Apply.

Device

The device category enables you to control the device itself. It contains the following topics:
- Control
- Date and Time
- Backup
- Upgrade
- Web Server
- Device Administrators
- Web and SSH Clients
- Administrator Security
Web Interface Options

Control
This page provides diagnostics information about all the processes that are running on the machine. For each Process, the User, PID, Parent PID, %CPU, % Memory and Command are displayed. You can use the Device Control drop-down list to Start, Restart, or Stop any of the Check Point products. In addition, you can Shutdown the device, or Reboot it, or download a diagnostic file (cpinfo output) useful for support.

You can refresh the information displayed in the page by clicking Refresh.

You can save the currently viewed diagnostics information in a file.

Date and Time
This page allows you to define the SecurePlatform's date and time, optionally using NTP.

In the Date and Time Setup page you can enter the current date and time, as well as setting the time zone. The date must be in the format: dd-Mon-yyyy (e.g. 31-Dec-2009). The time should be: HH:mm (e.g. 23:30).

NTP is used to synchronize clocks of computers on the Internet.

Click Apply to set the date and time.

Warning - If you change the date or time, and do not select Apply, the changes will not take effect.

Backup
This page allows you to configure backup settings. You can choose to configure a scheduled backup, or you can choose to perform an instantaneous backup operation. The backup data can be stored on a TFTP Server, SCP Server, or locally. In addition, you can view a Backup Log.

Note - If you use a stock TFTP Server with Unix/Linux flavors, you must create a world writable file having the same name as the proposed backup file before executing the backup. Otherwise, the backup will not succeed. It is strongly recommended that you refer to your tftp server manual, or simply to the tftp protocol, and verify that the usage of the utility is compliant with the environment that you are working in.

The SecurePlatform backup mechanism enables exporting snapshots of the entire dynamic configuration. Exported configurations can later be imported in order to restore a previous state in case of failure. The mechanism is also used for seamless upgrades of the software.
Information Backed Up

The information backed up includes:

- All settings performed by the Admin GUI
- Network configuration data
- Database of user settings (personal favorites, credentials, cookies etc.)

Two common use cases are:

- When the current configuration stops working, a previous exported configuration may be used in order to revert to a previous system state.
- Upgrading to a new SecurePlatform version. The procedure would include:
  - Backing up the configuration of the current version
  - Installing the new version
  - Importing the backed up configuration

Backup can be performed in configurable schedules.

The Backup page displays the **Current device date and time**. This field shows the current local time of the device, which may be different than the browser machine time.

Viewing the Scheduling Status

To view the Scheduling Status:

The **Scheduling Status** pane displays the following information:

- **Enabled**: backup currently enabled.
- **Backup to**: backup destination which can be one of the following: the current SecurePlatform, a TFTP Server, or an SCP Server,
- **Start at**: time to start the backup.
- **Recur every**: recurrence pattern.

Restoring the Backup

To restore the backup, run the restore shell command from the device.

The syntax is as follows:

```
restore [-h] [-d][[-tftp <ServerIP> <Filename>] | [-scp <ServerIP> <Username> <Password> <Filename>] |
```
Web Interface Options

[--file <Filename>]]

Table 3-2  restore command parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt; [&lt;Filename&gt;]</td>
<td>IP address of TFTP server, from which the configuration is restored, and the filename.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [&lt;Filename&gt;]</td>
<td>IP address of SCP server, from which the configuration is restored, the username and password used to access the SCP Server, and the filename.</td>
</tr>
<tr>
<td>--file &lt;Filename&gt;</td>
<td>Specify a filename for restore operation, performed locally.</td>
</tr>
</tbody>
</table>

When the restore command is executed by itself, without any additional flags, a menu of options is displayed. The options in the menu provide the same functionality, as the command line flags, for the restore command:

```
Choose one of the following:
-----------------------------------------------
[L]  Restore local backup package
[T]  Restore backup package from TFTP server
[S]  Restore backup package from SCP server
[R]  Remove local backup package
[Q]  Quit
-----------------------------------------------
```

Select the operation of your choice.

**Scheduling a Backup**

To schedule a backup:

1. On the **Backup** page, click **Scheduled backup**. The **Scheduled backup** page appears.
2. Select **Enable backup recurrence**.
3. Set up the backup schedule.
4. Select a device to hold the backup. The options include the current SecurePlatform, a TFTP Server (Trivial File Transfer Protocol: A version of the TCP/IP FTP protocol that has no directory or password capability), or an SCP Server (SCP is a secure FTP protocol).
5. Click **Apply**.

To execute a backup:
- Click **Backup now**.

**Viewing the Backup Log**

To view the backup log:
- Click **View backup log**. The **Backup Log** page appears. You will see the Device Date and Time, Location (the device to which the backup has been sent), Location IP Address, Backup Status and Details.
Web Interface Options

**Upgrade**

To upgrade your device:

1. Select the upgrade package file.
2. Click **Upload package to device**.
3. Select either **Safe Upgrade**, or **Double-Safe Upgrade**.
   
   If you selected **Double-Safe Upgrade**, your browser will automatically try to perform the first login immediately after the upgrade, within the time interval that you set. To enable that, you should not close the **Upgrade** page, and not browse to any other page. Otherwise, you will have to login manually, before the above interval expires. If you do not login manually within the above interval, the system will interpret this as a loss of connectivity and reset to the saved state.

4. When you are done uploading the package, you can click on the "package information" link to see detailed information about the package, including version information and the MD5 checksum of the package. This checksum can be used to verify that the package is correct.

5. Click **Start Upgrade**.
   
   The **Upgrade Status** pane provides information such as **Action**, **Start Time**, **Status** and **Details**.

**Web Server**

This page allows you to configure the Administration Web server listening IP and port.

1. Supply the port.
2. You can select an address from the drop-down list, instead of **All**. In that case, the Web server will only listen on that IP.
3. Click **Apply**.
Device Administrators

This page allows you to create a Device Administrator, and download a One Time Login Key.

If no Administrator has been configured, you can add an Administrator. This Administrator has Read/Write Permissions.

On a Security management server, only one administrator can be defined. To add more administrators, use SmartDashboard.

To create a Device Administrator:
2. Provide a name and a password for the Device Administrator.
3. Select an Authentication Scheme from the drop-down list.
4. Click Apply.
5. A One Time Login Key is required in case you forget your password. To download a One Time Login Key, click Download.
   The Login Key Challenge page is displayed.
6. Supply a challenge-question and answer to protect your Login Key from unauthorized usage.
7. Click OK.
8. Save this file in a safe place.

Web and SSH Clients

In the Web/SSH Clients page, a list of configured client IPs is displayed. Only the configured client IPs are permitted to access SecurePlatform and SSH services. You can add or remove a Web/SSH client.

To remove a Web/SSH client:
- Select the specific Web/SSH client and click Remove.

To add a Web/SSH client:
1. In the Web/SSH Clients page, click Add. The Add Web/SSH Client page is displayed.
2. You can add the IP address, resolvable name, or Network of the Web client.

   **Note** - The Hostname can also contain a wildcard, or the word 'any', which enables a connection from any Web/SSH Client.

3. Click **Apply**.

**Administrator Security**

In the **Administrator Security** window, you can configure the Administrator Security parameters.

To configure Administrator Security parameters:

1. Set the **Administrator Session Timeout** value.
2. In the **Administrator Login Restrictions** section, enable and set the **Lock Administrator's account after <x> login failures**.
3. Set the **Unlock Administrator's account after <y> minutes**.
4. Click **Apply**.

**Product Configuration**

The products category enables you to define which products are installed on the device (**Products** page) as well as to apply licenses to these products (**Licenses** page).
 Administrators

This page allows you to create a Security Management server Administrator.

If no Administrator has been configured, you can add an Administrator. This Administrator has Read/Write Permissions.

Only one Security Management server administrator can be defined. To add more administrators, use SmartDashboard.

To create a Device Administrator:
2. Provide a name and a password for the Device Administrator.
3. Select an Authentication Scheme from the drop-down list.
4. Click Apply.

GUI Clients

The Security Management GUI Clients page lists the type, hostname/IP address and netmask of the configured GUI Clients, and enables you to add additional GUI Clients or remove them. To delete a GUI Client, select the specific GUI Client and click Remove. In order to add a new GUI client, click Add. In the Add GUI Client page, you can enter either a hostname, or a network. The Hostname can also contain a Wildcard, an IP address range, or the word 'any', which enables a connection from any GUI Client. Click Apply.

Certificate Authority

The certificate authority is the entity that issues certificates for the Security Management server, Check Point Security Gateways, users and other trusted entities such as OPSEC applications used in the system.

The Certificate Authority page lists key parameters of the Security Management server Certificate Authority. These are:
- Certificate Authority Status
- Security Management server DN
- Fingerprint

Clicking Reset retrieves the current parameter values.
**Licenses**

Use the *Licenses* page to apply a license for the products that you have installed.

To apply a license:

1. You can click the **Check Point User Center** link to obtain a license from the User Center.
2. Click **New**.
3. Enter the **IP Address**, **Expiration Date**, **Features**, and **Signature Key**.
4. You can also copy the license string into the clipboard, and click **Paste License** to copy all the information into the fields.
5. Click **Apply** when done.

**Note** - License can also be applied by using SmartUpdate.

**Products**

This page enables you to check which products are already installed on the machine.
First Time Reboot and Login

As soon as the system reboots, after installation, the SecurePlatform Boot Loader screen appears.

**Note** - The Boot Loader appears on the console, connected to the computer. The console can be a monitor and keyboard attached to the computer, or a serial console attached to the first serial port (com1).

The Boot Loader offers a selection of boot options. By default, if there is no user intervention, the first option will be selected after a few seconds. For now, allow this option to run. Detailed information about the Boot Loader can be found in “SecurePlatform Boot Loader” on page 103.

As soon as the reboot finishes, the login prompt appears.
First Time Reboot and Login
Chapter 4
Administration

In This Chapter

- Managing Your SecurePlatform System  page 48
- SecurePlatform Shell  page 54
- SNMP Support  page 92
- Check Point Dynamic Routing  page 98
- SecurePlatform Boot Loader  page 103

This chapter discusses how to manage the SecurePlatform system, how to use the SecurePlatform’s shell commands, and how to configure SNMP for use with SecurePlatform. In addition, the Dynamic Routing and Boot Loader features are discussed.
Managing Your SecurePlatform System

In This Section

- Connecting to SecurePlatform by Using Secure Shell
- User Management
- SecurePlatform Administrators
- FIPS 140-2 Compliant Systems
- Using TFTP
- Backup and Restore

This section provides information on how to manage your SecurePlatform system, using the SecurePlatform Command Shell.

The Command Shell provides a set of commands required for configuration, administration and diagnostics of various system aspects. To manage Firewall and Address Translation policies and QoS policies, use SmartConsole.

Connecting to SecurePlatform by Using Secure Shell

SecurePlatform provides an SSH service, which allows secured, authenticated and encrypted access to the SecurePlatform system.

SSH (or Secure SHEll) is a protocol for creating a secure connection between two systems. In the SSH protocol, the client machine initiates a connection with a server machine. The following safeguards are provided by SSH:

- After an initial connection, the client can verify that it is connecting to the same server during subsequent sessions.
- The client can transmit its authentication information to the server, such as a username and password, in an encrypted format.
- All data, sent and received, during the connection is transferred using strong encryption, making it extremely difficult to decrypt and read.

The SSH service runs, by default. In addition, access to the SSH service is limited to the same IPs that have been allowed access to the Web UI. Granular control of machines that are allowed access to the SecurePlatform system, using SSH, can be set, using the security policy.
SSH login is allowed using the Standard Mode account user name and password, only. SCP service and client files can be copied to and from SecurePlatform, using SCP client software. Access to SCP is controlled, by editing /etc/scpusers.

User Management

SecurePlatform Shell includes two permission levels (Modes): Standard and Expert.

**Standard Mode**

This is the default mode, when logging in to a SecurePlatform system. In Standard Mode, the SecurePlatform Shell provides a set of commands, required for easy configuration and routine administration of a SecurePlatform system. Most system commands are not supported in this Mode. Standard mode commands are listed in “SecurePlatform Shell” on page 54.

Standard Mode displays the following prompt: `[hostname]#`, where hostname is the host name of the machine.

**Expert Mode**

The Expert Mode provides full system root permissions and a full system shell. Switching from Standard Mode to Expert Mode requires a password. The first time you switch to Expert mode you will be asked to select a password. Until then, the password is the same as the one that you set for Standard Mode.

You need to enter the first replacement password that you used when logging in as the admin user. Any sequential administrator password change will not update the expert password that you must enter at the first-time expert user password change. To exit Expert Mode, run the command `exit`.

Expert Mode displays the following prompt: `[Expert@hostname]#`, where hostname is the host name of the machine.

**Warning** - Expert Mode should be used with caution. The flexibility of an open shell, with a root permission, exposes the system to the possibility of administrative errors.

**Note** - An Expert user must first login as a Standard user, and only then enter the `expert` command to access Expert Mode. Until you change passwords, the Expert password is the same password that you set for Standard Mode, i.e. you need to enter the first replacement password that you used when logging in as the admin user. Any sequential admin password change will not update the expert password that you must enter at the first-time expert user password change.
SecurePlatform Administrators

SecurePlatform supports multiple administrator access to the regular shell. This can be used to audit configuration changes performed by administrators. Every such change is logged to the system's syslog mechanism, with the username of the administrator, as a tag.

To configure another administrator from the cpshell, use the following command:

```
adduser [-x EXTERNAL_AUTH] <user name>
```

Note - Only SecurePlatform Pro supports RADIUS authentication for SecurePlatform Administrators.

You will be asked to enter and confirm a password for the administrator. The password must conform to the following complexity requirements:

- at least 6 characters, in length
- a mixture of alphabetic and numeric characters
- at least four different characters
- does not use simple dictionary words, or common strings such as “qwerty”

To delete an administrator from the cpshell, use the following command:

```
deluser <name>
```

You can also define additional administrators through the Web GUI.

How to Authenticate Administrators via RADIUS

All Administrators must be authenticated by one of the supported authentication methods. As well as being authenticated through the internal database, Administrators may also be authenticated via RADIUS. SecurePlatform administrators can be authenticated using the RADIUS server in two ways:

- By configuring the local user authentication via the RADIUS server. In this case it is necessary to define all users that will be authenticated by the RADIUS server on every SecurePlatform machine, and it is NOT required to define any RADIUS groups.
- By defining the list of RADIUS groups. All users that belong to the RADIUS groups defined on SecurePlatform will be able to authenticate and perform login.
The option utilizing RADIUS groups allows more flexibility, by eliminating the need to define all RADIUS users on each SecurePlatform machine.

There is a special RADIUS group called **any**. When this group is present in the group list, ALL users defined on the RADIUS server will be able to log into the SecurePlatform machine.

To authenticate an Administrator via RADIUS, you must:

1. Verify that a RADIUS server is configured. If a RADIUS server is not configured, add one by using the following command:
   
   ```
   radius servers add <server[:port]> <secret> <timeout> <label>
   ```

2. Verify that at least one of the following is correct:

   A. The user that you want to authenticate via the RADIUS server is configured on SecurePlatform, as using the RADIUS authentication method. You can define local users that authenticate via RADIUS by using the following command:

   ```
   radius users add <username>
   ```

   B. At least one RADIUS group is configured, and the user defined on the RADIUS server belongs to that group. You can define RADIUS groups by using the following command line:

   ```
   radius groups add <groupname>
   ```

3. Define the Administrator as a RADIUS user, by using the following command:

   ```
   radius users add <username>
   ```

You can use the following commands to monitor and modify your RADIUS configuration.

To control RADIUS servers:

- `radius servers show`
- `radius servers add <server[:port]> <secret> <timeout>`
- `radius servers del <server[:port]>`

To control RADIUS user groups:

- `radius groups show`
- `radius groups add <groupname>`
- `radius groups del <groupname>`
To control local RADIUS users:

- `radius users show`
- `radius users add <username>`
- `radius users del <username>`

**FIPS 140-2 Compliant Systems**

The Federal Information Processing Standard (FIPS) 140-2 imposes certain restrictions on the operation of SecurePlatform. Administrators whose systems are FIPS 140-2 compliant, must configure their systems as follows:

Run the following command from cpshell:

```
fips on
```

This command does the following:

1. Adds an integrity check that verifies the integrity of all executables, scripts and configuration files, before connecting the system to the network.

2. Enforces the policy of locking accounts of administrators who have exceeded the threshold of unsuccessful login attempts (see “Lockout of Administrator Accounts” on page 52).

3. Removes the Web GUI daemon, thus disabling the Web GUI.

4. Removes the Check Point Remote Installation daemon, thus disabling SmartUpdate.

5. Configures the Check Point Security Gateway's default filter to “drop all incoming”.

**Lockout of Administrator Accounts**

The account of an administrator, who attempts to logon unsuccessfully, three times in one minute, is locked for 60 minutes. This feature is configurable using the `lockout` command.

**Using TFTP**

The Trivial File Transfer Protocol (TFTP) provides an easy way for transferring files to and from SecurePlatform. SecurePlatform mechanisms that can utilize TFTP include:
Backup and Restore

- **Backup / Restore Utilities**
- **Patch Utility**—used for software updates
- **Diag Utility**—used for obtaining various diagnostics information

**Note** - Freeware and Shareware TFTP servers are readily available on the Internet.

Follow the vendor instructions on how to setup the TFTP server, and make sure that you configure the server to allow both reception and transmission of files.

**Warning** - TFTP is not an encrypted, or authenticated protocol. Make sure that you run the TFTP server on your internal network only.

**Backup and Restore**

SecurePlatform provides both command line, or Web GUI, capability for conducting backups of your system settings and products configuration.

The **backup** utility can store backups either locally on the SecurePlatform machine hard drive or to an FTP server, TFTP server or SCP server. You can perform backups on request, or according to a predefined schedule.

Backup files are kept in tar gzipped format (.tgz). Backup files, saved locally, are kept in /var/CPbackup/backups.

The **restore** command line utility is used for restoring SecurePlatform settings, and/or Product configuration from backup files.

**Note** - Only administrators with Expert permission can directly access directories of a SecurePlatform system. You will need the Expert password to execute the restore command.

For more information about the **backup** and **restore** utilities, see “backup” on page 61, and “restore” on page 65.
SecurePlatform Shell

In This Section

Command Shell ........................................ page 54
Management Commands ................................. page 56
Documentation Commands ............................... page 57
Date and Time Commands ................................. page 57
System Commands ........................................ page 60
Snapshot Image Management ............................ page 68
System Diagnostic Commands ......................... page 70
Check Point Commands ................................ page 73
Network Diagnostics Commands ....................... page 73
Network Configuration Commands ..................... page 79
Dynamic Routing Commands ............................ page 89
User and Administrator Commands .................... page 90

This section includes a complete listing of SecurePlatform’s shell commands. These commands are required for configuration, administration and diagnostics of various system aspects.

Note - All commands are case sensitive.

Command Shell

Command Set

To display a list of available commands, enter `?` or `help` at the command prompt. Many commands provide short usage instructions by running the command with the parameter `--help`, or with no parameters.
Command Line Editing

SecurePlatform Command Shell uses command line editing conventions. You can scroll through previously entered commands with the up or down arrow keys. When you reach a command you wish to use, you can edit it or click the Enter key to start it. The audit command is used to display history of commands entered at the command prompt (see “audit” on page 60):

Table 4-1 Command Line Editing Keys

<table>
<thead>
<tr>
<th>Key</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right Arrow/^f</td>
<td>Move cursor right</td>
</tr>
<tr>
<td>Left Arrow/^b</td>
<td>Move cursor left</td>
</tr>
<tr>
<td>Home/^a</td>
<td>Move cursor to beginning of line</td>
</tr>
<tr>
<td>End/^e</td>
<td>Move cursor to end of line</td>
</tr>
<tr>
<td>Backspace/^h</td>
<td>Delete last char</td>
</tr>
<tr>
<td>^d</td>
<td>Delete char on cursor</td>
</tr>
<tr>
<td>^u</td>
<td>Delete line</td>
</tr>
<tr>
<td>^w</td>
<td>Delete word to the left</td>
</tr>
<tr>
<td>^k</td>
<td>Delete from cursor to end of line</td>
</tr>
<tr>
<td>Up arrow/^p</td>
<td>View previous command</td>
</tr>
<tr>
<td>Down arrow/^n</td>
<td>View next command</td>
</tr>
</tbody>
</table>

Command Output

Some command output may be displayed on more than one screen. By default, the Command Shell will display one screen, and prompt: -More-. Click any key to continue to display the rest of the command output.

The More functionality can be turned on or off, using the scroll command.
Management Commands

In This Section

exit\hspace{1em}page 56

Expert Mode\hspace{1em}page 56

passwd\hspace{1em}page 56

exit

Exit the current Mode:

- In Standard Mode, exit the shell (logout of the SecurePlatform system)
- In Expert Mode, exit to Standard Mode

Syntax

```
exit
```

Expert Mode

Switch from Standard Mode to Expert Mode.

Syntax

```
expert
```

Description

After entering the `expert`, command supply the expert password. After password verification, you will be transferred into expert mode.

passwd

Changing the password can be performed in both modes. Changing the password in Standard Mode changes the login password. Changing the password in Expert Mode changes the Expert Mode and Boot Loader password. During the first transfer to Expert Mode, you will be required to enter your Standard Mode password, i.e. you need to enter the first replacement password that you used when logging in as the admin user. Any sequential admin password change will not update the expert password that you must enter at the first-time expert user password change. Change the Expert Mode password. After the Expert Mode password is changed, the new password must be used to obtain Expert Mode access.
Documentation Commands

**Syntax**

```
passwd
```

**Documentation Commands**

**help**

List the available commands and their respective descriptions.

**Syntax**

```
help
```

**Date and Time Commands**

**In This Section**

- date  page 57
- time  page 58
- timezone  page 58
- ntp  page 59
- ntpstop  page 59
- ntpstart  page 60

**date**

Show or set the system's date. Changing the date or time affects the hardware clock.
Date and Time Commands

Syntax

date [MM-DD-YYYY]

Parameters

Table 4-2  Date Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM-DD-YYYY</td>
<td>The date to be set, first two digits (MM) are the month [01..12], next two digits (DD) are the day of month [01..31], and last four digits (YYYY) are the year</td>
</tr>
</tbody>
</table>

**time**

Show or set the system’s time. Changing the date or time affects the hardware clock.

Syntax

time [HH:MM]

Parameters

Table 4-3  Time Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH:MM</td>
<td>The time to be set, first two digits (HH) are the hour [00..23], last two digits (MM) are the minute [00..59]</td>
</tr>
</tbody>
</table>

**timezone**

Set the system’s time zone.
Date and Time Commands

**Syntax**

```bash
timezone [-show | --help]
```

**Parameters**

Table 4-4  Time Zone Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>if no parameters are entered, an interactive mode of time zone selection is displayed</td>
</tr>
<tr>
<td>-show</td>
<td>show currently selected time zone</td>
</tr>
<tr>
<td>--help</td>
<td>show usage message</td>
</tr>
</tbody>
</table>

**ntp**

Configure and start the Network Time Protocol polling client.

**Syntax**

```bash
ntp <MD5_secret> <interval> <server1> [<server2> [<server3>]]
ntp -n <interval> <server1> [<server2> [<server3>]]
```

**Parameters**

Table 4-5  ntp Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5_secret</td>
<td>pre-shared secret used to authenticate against the NTP server; use &quot;-n&quot; when authentication is not required.</td>
</tr>
<tr>
<td>interval</td>
<td>polling interval, in seconds</td>
</tr>
<tr>
<td>server[1,2,3]</td>
<td>IP address or resolvable name of NTP server</td>
</tr>
</tbody>
</table>

**ntpstop**

Stop polling the NTP server.
System Commands

**Syntax**

```plaintext
ntpstart
```

**ntpstart**

Start polling the NTP server.

**Syntax**

```plaintext
ntpstart
```

System Commands

In This Section

- **audit**  page 60
- **backup**  page 61
- **patch**  page 64
- **restore**  page 65
- **shutdown**  page 66
- **ver**  page 67

**audit**

Display or edit commands, entered in the shell for a specific session. The audit is not kept between sessions.
System Commands

Syntax

```latex
audit setlines <number_of_lines>
audit show <number_of_lines>
audit clear <number_of_lines>
```

Parameters

Table 4-6 Audit Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>lines &lt;number_of_lines&gt;</td>
<td>restrict the length of the command history that can be shown to &lt;number_of_lines&gt;</td>
</tr>
<tr>
<td>show &lt;number_of_lines&gt;</td>
<td>show &lt;number_of_lines&gt; recent commands entered</td>
</tr>
<tr>
<td>clear</td>
<td>clear command history</td>
</tr>
</tbody>
</table>

backup

Backup the system configuration. You can also copy backup files to a number of scp and tftp servers for improved robustness of backup. The backup command, run by itself, without any additional flags, will use default backup settings and will perform a local backup.

Syntax

```latex
backup [-h] [-d] [-I] [--purge DAYS] [--sched [on hh:mm <-m DayOfMonth> | <-w DaysOfWeek> | off] [--tftp <ServerIP> [-path <Path>] [<Filename>]] [--scp <ServerIP> <Username> <Password> [-path <Path>] [<Filename>]] [--ftp <ServerIP> <Username> <Password> [-path <Path>] [<Filename>]] [--file [-path <Path>] [<Filename>]]
```
### Parameters

**Table 4-7: Backup Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>-l</td>
<td>flag enables backup of the Check Point Security Gateway log (By default, logs are not backed up.)</td>
</tr>
<tr>
<td>-p or --purge</td>
<td>delete old backups from previous backup attempts</td>
</tr>
<tr>
<td>[--sched [on hh:mm &lt;-m DayOfMonth&gt;</td>
<td>&lt;-w DaysOfWeek&gt;]</td>
</tr>
<tr>
<td></td>
<td>• On - specify time and day of week, or day of month</td>
</tr>
<tr>
<td></td>
<td>• Off - disable schedule</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt; [-path &lt;Path&gt;][&lt;Filename&gt;]</td>
<td>List of IP addresses of TFTP servers, to which the configuration will be backed up, and optionally the filename.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt;[-path &lt;Path&gt;] [&lt;Filename&gt;]</td>
<td>List of IP addresses of SCP servers, to which the configuration will be backed up, the username and password used to access the SCP Server, and optionally the filename.</td>
</tr>
<tr>
<td>--ftp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [-path &lt;Path&gt;] [&lt;Filename&gt;]</td>
<td>List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.</td>
</tr>
<tr>
<td>--file [-path &lt;Path&gt;] &lt;Filename&gt;</td>
<td>When the backup is performed locally, specify an optional filename</td>
</tr>
</tbody>
</table>

**Note** - If a Filename is not specified, a default name will be provided with the following format: `backup_hostname.domain-name_day of month_month_year_hour_minutes.tgz` for example:`backup_gateway1.mydomain.com_13_11_2003_12_47.tgz`
Examples

backup -file -path /tmp filename (will put the backup file in (local) /tmp and name it filename)

backup

-tftp <ip1> -path tmp
-tftp <ip2> -path var file1
-scp <ip3> username1 password1 -path /bin file2
-file file3
--scp <ip4> username2 password2 file4
--scp <ip5> username3 password3 -path mybackup

The backup file be saved on:

1. tftp server with ip1, the backup file will be saved in the tmp directory (under the tftp server default directory – usually /tftproot) with the default file name – backup_SystemName_TimStamp.tgz
2. tftp server with ip2, the backup file will be saved on var (under the tftp server default directory – usually /tftproot) as file1
3. scp server with ip3, the backup file will be saved on /bin as file2
4. locally on the default directory (/var/CPbackup/backups) as file3
5. scp server with ip4 on the username2 home directory as file4
6. scp server with ip5 on ~username3/mybackup/ with the default backup file name
System Commands

**reboot**

Restart the system.

**Syntax**

```
reboot
```

**patch**

Apply an upgrade or hotfix file.

*Note* - See the Release Notes for information about when to replace the patch utility with a more recent version.
System Commands

**restore**

Restore the system configuration.

**Syntax**

```
patch add scp <ip_address> <patch_name> [password (in expert mode)]
patch add tftp <ip_address> <patch_name>
patch add cd <patch_name>
patch add <full_patch_path>
patch log
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>install a new patch</td>
</tr>
<tr>
<td>log</td>
<td>list all patches installed</td>
</tr>
<tr>
<td>scp</td>
<td>install from SCP</td>
</tr>
<tr>
<td>cd</td>
<td>install from CD</td>
</tr>
<tr>
<td>tftp</td>
<td>install from TFTP server</td>
</tr>
<tr>
<td>ip</td>
<td>IP address of the tftp server containing the patch</td>
</tr>
<tr>
<td>patch_name</td>
<td>the name of the patch to be installed</td>
</tr>
<tr>
<td>password</td>
<td>password, in expert mode</td>
</tr>
<tr>
<td>full_patch_path</td>
<td>the full path for the patch file (for example,</td>
</tr>
<tr>
<td></td>
<td>/var/tmp/mypatch.tgz)</td>
</tr>
</tbody>
</table>

**Syntax**

```
```
Parameters

Table 4-9

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt;</td>
<td>IP address of TFTP server, from which the configuration is restored, and the filename.</td>
</tr>
<tr>
<td>[&lt;Filename&gt;]</td>
<td></td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [Filename&gt;]</td>
<td>IP address of SCP server, from which the configuration is restored, the username and password used to access the SCP Server, and the filename.</td>
</tr>
<tr>
<td>--ftp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [-path &lt;Pat&gt;] [Filename]</td>
<td>List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.</td>
</tr>
<tr>
<td>--file &lt;Filename&gt;</td>
<td>Specify a filename for restore operation, performed locally.</td>
</tr>
</tbody>
</table>

When the restore command is executed by itself, without any additional flags, a menu of options is displayed. The options in the menu provide the same functionality, as the command line flags, for the restore command.

Choose one of the following:

---

[L]  Restore local backup package
[T]  Restore backup package from TFTP server
[S]  Restore backup package from SCP server
[V]  Restore backup package from FTP server
[R]  Remove local backup package
[Q]  Quit

---

Select the operation of your choice.

**shutdown**

Shut down the system.
System Commands

Syntax

shutdown

**ver**

Display the SecurePlatform system's version.

Syntax

ver
Snapshot Image Management

In This Section

Revert
Snapshot

Commands to take a snapshot of the entire system and to restore the system, from
the snapshot, are available. The system can be restored at any time, and at boot
time the administrator is given the option of booting from any of the available
snapshots. This feature greatly reduces the risks of configuration changes.

The snapshot and revert commands can use an TFTP server, a SCP Server or and
FTP server to store snapshots. Alternatively, snapshots can be stored locally.

Note - The amount of time it takes to perform a snapshot or revert depends on the amount
of data (for example, logs) that is stored or restored. For example, it may take between 90
to 120 minutes to perform a snapshot or revert for Security Management server, Log Server,
Provider-1, etc.

Revert

Reboot the system from a snapshot file. The revert command, run by itself, without
any additional flags, will use default backup settings, and will reboot the system
from a local snapshot.

revert [-h] [-d] [--tftp <ServerIP> <Filename>]
[--scp <ServerIP> <Username> <Password> <Filename>
[--ftp <ServerIP> <Username> <Password> <Filename>
[--file <Filename>]]
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt; &lt;Filename&gt;</td>
<td>IP address of the TFTP server, from which the snapshot is rebooted, as well as the filename of the snapshot.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; &lt;Filename&gt;</td>
<td>IP address of the SCP server, from which the snapshot is rebooted, the username and password used to access the SCP Server, and the filename of the snapshot.</td>
</tr>
<tr>
<td>--ftp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [-path &lt;Path&gt;] [Filename]</td>
<td>List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.</td>
</tr>
<tr>
<td>--file &lt;Filename&gt;</td>
<td>When the snapshot is made locally, specify a filename</td>
</tr>
</tbody>
</table>

The revert command functionality can also be accessed from the **Snapshot image management** boot option.

**Snapshot**

This command creates a snapshot file. The snapshot command, run by itself, without any additional flags, will use default backup settings and will create a local snapshot.

**Syntax**

```
```
Parameters

Table 4-11  Snapshot Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>obtain usage</td>
</tr>
<tr>
<td>-d</td>
<td>debug flag</td>
</tr>
<tr>
<td>--tftp &lt;ServerIP&gt; &lt;Filename&gt;</td>
<td>IP address of the TFTP server, from which the snapshot is made, as well as the filename of the snapshot.</td>
</tr>
<tr>
<td>--scp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; &lt;Filename&gt;</td>
<td>IP address of the SCP server, from which the snapshot is made, the username and password used to access the SCP Server, and the filename of the snapshot.</td>
</tr>
<tr>
<td>--ftp &lt;ServerIP&gt; &lt;Username&gt; &lt;Password&gt; [-path &lt;Pat&gt;] [&lt;Filename&gt;]</td>
<td>List of IP addresses of FTP servers, to which the configuration will be backed up, the username and password used to access the FTP Server, and optionally, the filename.</td>
</tr>
<tr>
<td>--file &lt;Filename&gt;</td>
<td>When the snapshot is made locally, specify a filename</td>
</tr>
</tbody>
</table>

System Diagnostic Commands

In This Section

- diag
- log
- top

**diag**

Display or send the system’s diagnostic information (**diag** files).
System Diagnostic Commands

Syntax

```
diag <log_file_name> tftp <tftp_host_ip_address>
```

Parameters

Table 4-12  Diag Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>log_file_name</td>
<td>name of the logfile to be sent</td>
</tr>
<tr>
<td>tftp</td>
<td>use tftp to upload the diagnostic information (other upload methods can be added in the future)</td>
</tr>
<tr>
<td>tftp_host_ip_address</td>
<td>IP address of the host, that is to receive the diagnostic information</td>
</tr>
</tbody>
</table>

**log**

Shows the list of available log files, applies log rotation parameters, shows the index of the log file in the list, and selects the number of lines of the log to display.
System Diagnostic Commands

### Syntax

```
log --help
log list
log limit <log-index><max-size><backlog-copies>
log unlimit <log-index>
log show <log-index> [<lines>]
```

### Parameters

Table 4-13  Log Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>show the list of available log files</td>
</tr>
<tr>
<td>limit</td>
<td>apply log rotation parameters</td>
</tr>
<tr>
<td>unlimit</td>
<td>remove log size limitations</td>
</tr>
<tr>
<td>log-index</td>
<td>show the index of the log file, in the list</td>
</tr>
<tr>
<td>max-size</td>
<td>show the size of the log file, in bytes</td>
</tr>
<tr>
<td>backlog-copies</td>
<td>list the number of backlog copies of the log file</td>
</tr>
<tr>
<td>lines</td>
<td>select the number of lines of the log to display</td>
</tr>
</tbody>
</table>

### top

Display the top 15 processes on the system and periodically updates this information. Raw CPU percentage is used to rank the processes.

### Syntax

```
top
```
Check Point Commands

For information about Check Point commands, see the Command Line Interface R70 Reference Guide http://supportcontent.checkpoint.com/documentation_download?ID=8713

Network Diagnostics Commands

In This Section

ping page 73
traceroute page 76
netstat page 77

ping

send ICMP ECHO_REQUEST packets to network hosts.

Syntax

```
```
## Network Diagnostics Commands

### Parameters

Table 4-14 ping Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c count</td>
<td>Stop after sending (and receiving) count ECHO_RESPONSE packets.</td>
</tr>
<tr>
<td>-d</td>
<td>Set the SO_DEBUG option for the socket being used.</td>
</tr>
<tr>
<td>-f</td>
<td>Flood ping. Outputs packets as fast as they come back, or one hundred times per second, whichever is greater. For every ECHO_REQUEST sent, a period &quot;.&quot; is printed, while for every ECHO_REPLY received, a backspace is printed. This provides a rapid display of how many packets are being dropped. Only the super-user may use this option. This can place a very heavy load on a network and should be used with caution.</td>
</tr>
<tr>
<td>-i wait</td>
<td>Wait: wait i seconds between sending each packet. The default is to wait for one second between each packet. This option is incompatible with the -f option.</td>
</tr>
<tr>
<td>-l</td>
<td>Preload: if preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior. Only the super-user may use this option.</td>
</tr>
<tr>
<td>-n</td>
<td>Numeric output only. No attempt will be made to lookup symbolic names for host addresses.</td>
</tr>
<tr>
<td>-p pattern</td>
<td>You may specify up to 16 &quot;pad&quot; bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, &quot;-p ff&quot; will direct the sent packet to be filled with a series of ones (&quot;1&quot;).</td>
</tr>
<tr>
<td>-q</td>
<td>Quiet output. Nothing is displayed except the summary lines at the time of startup and finish.</td>
</tr>
<tr>
<td>-R</td>
<td>Record route. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.</td>
</tr>
</tbody>
</table>
Table 4-14 ping Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r</td>
<td>Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.</td>
</tr>
<tr>
<td>-s packetsize</td>
<td>Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes, when combined with the 8 bytes of ICMP header data.</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose (detailed) output. Lists ICMP packets (other than ECHO_RESPONSE) that are received.</td>
</tr>
</tbody>
</table>
Network Diagnostics Commands

**traceroute**

Tracking the route a packet follows (or finding the miscreant gateway that is discarding your packets) can be difficult. Tracert uses the IP protocol ‘time to live’ field and attempts to elicit an **ICMP TIME EXCEEDED** response from each gateway along the path to a designated host.

**Syntax**

```
traceroute [ -dFInrvx ] [ -f first_ttl ] [ -g gateway ] [ -i iface ]
[ -m max_ttl ] [ -p port ] [ -q nqueries ] [ -s src_addr ] [ -t tos ]
[ -w waittime ] host [ packetlen ]
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f first_ttl</td>
<td>Set the initial time-to-live, used in the first outgoing probe packet.</td>
</tr>
<tr>
<td>-F</td>
<td>Set the &quot;don't fragment&quot; bit.</td>
</tr>
<tr>
<td>-d</td>
<td>Enable socket level debugging.</td>
</tr>
<tr>
<td>-g gateway</td>
<td>Gateway: specify a loose source route gateway (8 maximum).</td>
</tr>
<tr>
<td>-i iface</td>
<td>iface: specify a network interface, to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do this.)</td>
</tr>
<tr>
<td>-I</td>
<td>Use ICMP ECHO instead of UDP datagrams.</td>
</tr>
<tr>
<td>-m max_ttl</td>
<td>Set the max time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).</td>
</tr>
<tr>
<td>-n</td>
<td>Print hop addresses numerically, rather than symbolically and numerically (saves a name server address-to-name lookup, for each gateway found on the path).</td>
</tr>
<tr>
<td>-p port</td>
<td>Set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an <strong>ICMP PORT UNREACHABLE</strong> message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range.</td>
</tr>
<tr>
<td>-q nqueries</td>
<td>Number of queries to run.</td>
</tr>
</tbody>
</table>
Network Diagnostics Commands

**netstat**
Show network statistics.

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r</td>
<td>Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.</td>
</tr>
<tr>
<td>-s</td>
<td>Use the following IP address (which usually is given as an IP number, not a hostname) as the source address in out-going probe packets. On multi-homed hosts (those with more than one IP address), this option can be used to force the source address to be something, other than the IP address of the interface that the probe packet is sent on. If the IP address is not one of this machine's interface addresses, an error is returned and nothing is sent. (See the -i flag for another way to do this.)</td>
</tr>
<tr>
<td>-t tos</td>
<td>Set the type-of-service in probe packets to the following value (default zero). The value must be a decimal integer in the range 0 to 255. This option can be used to see if different types-of-service result in different paths. (If you are not running 4.4bsd, this may be irrelevant, since the normal network services like telnet and ftp don't let you control the TOS. Not all values of TOS are legal or meaningful, see the IP spec for definitions. Useful values are probably &quot;-t 16&quot; (low delay) and &quot;-t 8&quot; (high throughput).</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose (detailed) output. Received ICMP packets other than TIME_EXCEEDED and UNREACHABLES are listed.</td>
</tr>
<tr>
<td>-w</td>
<td>Set the time (in seconds) to wait for a response to a probe (default is 5 seconds).</td>
</tr>
<tr>
<td>-x</td>
<td>Toggle checksums. Normally, this prevents traceroute from calculating checksums. In some cases, the operating system can overwrite parts of the outgoing packet, but not recalculate the checksum (In some cases, the default is not to calculate checksums. Using -x causes checksums to be calculated). Checksums are usually required for the last hop, when using ICMP ECHO probes (-I).</td>
</tr>
</tbody>
</table>

**Table 4-15**  traceroute Parameters (continued)
### Network Diagnostics Commands

**Syntax**

```bash
netstat [-veenCFl] [<Af>] -r
netstat (-V|--version|-h|--help)
netstat [-vnNcaeol] [<Socket> ...]
netstat ( [-veenN] -i | [-cnNe] -M | -s )
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
<th>extended meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r</td>
<td>route</td>
<td>display routing table</td>
</tr>
<tr>
<td>-i</td>
<td>interfaces</td>
<td>display interface table</td>
</tr>
<tr>
<td>-g</td>
<td>groups</td>
<td>display multicast group memberships</td>
</tr>
<tr>
<td>-s</td>
<td>statistics</td>
<td>display networking statistics (like SNMP)</td>
</tr>
<tr>
<td>-M</td>
<td>masquerade</td>
<td>display masqueraded connections</td>
</tr>
<tr>
<td>-v</td>
<td>verbose</td>
<td>be verbose (detailed)</td>
</tr>
<tr>
<td>-n</td>
<td>numeric</td>
<td>do not resolve names</td>
</tr>
<tr>
<td>-N</td>
<td>symbolic</td>
<td>resolve hardware names</td>
</tr>
<tr>
<td>-e</td>
<td>extend</td>
<td>display other/more information</td>
</tr>
<tr>
<td>-p</td>
<td>programs</td>
<td>display PID/Program name for sockets</td>
</tr>
<tr>
<td>-c</td>
<td>continuous</td>
<td>continuous listing</td>
</tr>
<tr>
<td>-l</td>
<td>listening</td>
<td>display listening server sockets</td>
</tr>
<tr>
<td>-a</td>
<td>all, listening</td>
<td>display all sockets (default: connected)</td>
</tr>
<tr>
<td>-o</td>
<td>timers</td>
<td>display timers</td>
</tr>
<tr>
<td>-F</td>
<td>fib</td>
<td>display Forwarding Information Base (default)</td>
</tr>
<tr>
<td>-C</td>
<td>cache</td>
<td>display routing cache, instead of FIB</td>
</tr>
<tr>
<td>&lt;Socket&gt;</td>
<td></td>
<td>Type of socket, may be one of the following:</td>
</tr>
<tr>
<td>-A &lt;AF&gt;,</td>
<td>af &lt;AF&gt;</td>
<td>Address family, may be one of the following: inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25) netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)</td>
</tr>
</tbody>
</table>
Network Configuration Commands

In This Section

arp
addarp
delarp
hosts
ifconfig
vconfig
route
hostname
domainname
dns
sysconfig
webui

**arp**

arp manipulates the kernel’s ARP cache in various ways. The primary options are clearing an address mapping entry and manually setting one up. For debugging purposes, the ARP program also allows a complete dump of the ARP cache.

**Syntax**

```bash
arp [-vn] [-H type] [-i if] -a [hostname]
arp [-v] [-i if] -d hostname [pub]
arp [-v] [-H type] [-i if] -s hostname hw_addr [temp]
arp [-v] [-H type] [-i if] -s hostname hw_addr [netmask nm] pub
arp [-v] [-H type] [-i if] -Ds hostname ifa [netmask nm] pub
arp [-vnD] [-H type] [-i if] -f [filename]
```
Network Configuration Commands

**addarp**

addarp adds a persistent ARP entry (one that will survive re-boot).

**Syntax**

```
addarp <hostname> <hwaddr>
```

**delarp**

delarp removes ARP entries created by addarp.

**Syntax**

```
delarp <hostname> <MAC>
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
<th>Extended Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>verbose</td>
<td>Tell the user the details of what is going on.</td>
</tr>
<tr>
<td>-n</td>
<td>numeric</td>
<td>Shows numerical addresses instead of trying to determine symbolic host, port or user names.</td>
</tr>
<tr>
<td>-H type,</td>
<td>hw-type</td>
<td>When setting, or reading the ARP cache, this optional parameter tells arp which class of entries it should check for. The default value of this parameter is ether (i.e. hardware code 0x01 for IEEE 802.3 10Mbps Ethernet). Other values might include network technologies such as ARCnet (arcnet), PROnet (pronet), AX.25 (ax25) and NET/ROM (netrom).</td>
</tr>
<tr>
<td>-a [hostname]</td>
<td>display [hostname]</td>
<td>Shows the entries of the specified hosts. If the hostname parameter is not used, all entries will be displayed.</td>
</tr>
<tr>
<td>-d hostname</td>
<td>delete hostname</td>
<td>Remove any entry for the specified host. This can be used if the indicated host is brought down, for example.</td>
</tr>
</tbody>
</table>
Network Configuration Commands

Table 4-17  arp Parameters (continued)

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
<th>extended meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-D</td>
<td>use-device</td>
<td>Use the interface ifa's hardware address.</td>
</tr>
<tr>
<td>-i If</td>
<td>device If</td>
<td>Select an interface. When dumping the ARP cache, only entries matching the specified interface will be printed. When setting a permanent, or temp ARP, entry this interface will be associated with the entry. If this option is not used, the kernel will guess, based on the routing table. For public entries, the specified interface is the interface, on which ARP requests will be answered.</td>
</tr>
<tr>
<td>-f filename</td>
<td>file filename</td>
<td>Similar to the -s option, only this time the address info is taken from file filename set up. The name of the data file is very often /etc/ethers. If no filename is specified /etc/ethers is used as default.</td>
</tr>
</tbody>
</table>
Network Configuration Commands

**hosts**

Show, set or remove hostname to IP-address mappings.

**Syntax**

```
hosts add <IP-ADDRESS> <host1> [host2] ...
hosts remove <IP_ADDRESS> <host1> [host2] ...
hosts
```

**Parameters**

<table>
<thead>
<tr>
<th>Table 4-18</th>
<th>hosts Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hosts</strong></td>
<td><strong>parameter</strong></td>
</tr>
<tr>
<td>Running hosts, with no parameters, displays the current host names to IP mappings.</td>
<td></td>
</tr>
<tr>
<td><strong>add</strong></td>
<td>IP-ADDRESS</td>
</tr>
<tr>
<td></td>
<td>host1, host2...</td>
</tr>
<tr>
<td><strong>remove</strong></td>
<td>IP-ADDRESS</td>
</tr>
<tr>
<td></td>
<td>host1, host2...</td>
</tr>
</tbody>
</table>

**ifconfig**

Show, configure or store network interfaces settings.
Network Configuration Commands

Syntax

```
ifconfig [-a] [-i] [-v] [-s] <interface> [[<AF>] <address>]
(add <address>[/<prefixlen>])
(del <address>[/<prefixlen>])
([-broadcast {[<address>]}] [-pointopoint {[<address>]}]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>] [metric <NN>] [mtu <NN>]
([-]trailers) [(-]arp) [(-]allmulti]
[multicast] [(-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
([-]dynamic]
[up|down]
[=-save]
```

Table 4-19  ifConfig Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The name of the interface. This is usually a driver name, followed by a unit number, for example eth0 for the first Ethernet interface.</td>
</tr>
<tr>
<td>up</td>
<td>This flag causes the interface to be activated. It is implicitly specified if an address is assigned to the interface.</td>
</tr>
<tr>
<td>down</td>
<td>This flag causes the driver, for this interface, to be shut down.</td>
</tr>
<tr>
<td>[-]arp</td>
<td>Enable or disable the use of the ARP protocol, on this interface.</td>
</tr>
<tr>
<td>[-]promisc</td>
<td>Enable or disable the promiscuous mode of the interface. If selected, all packets on the network will be received by the interface.</td>
</tr>
<tr>
<td>[-]allmulti</td>
<td>Enable or disable all-multicast mode. If selected, all multicast packets on the network will be received by the interface.</td>
</tr>
<tr>
<td>metric N</td>
<td>This parameter sets the interface metric.</td>
</tr>
<tr>
<td>mtu N</td>
<td>This parameter sets the Maximum Transfer Unit (MTU) of an interface.</td>
</tr>
<tr>
<td>dstaddr addr</td>
<td>Set the remote IP address for a point-to-point link (such as PPP). This keyword is now obsolete; use the point-to-point keyword instead.</td>
</tr>
<tr>
<td>netmask addr</td>
<td>Set the IP network mask, for this interface. This value defaults to the usual class A, B or C network mask (as derived from the interface IP address), but it can be set to any value.</td>
</tr>
</tbody>
</table>
## Network Configuration Commands

### Table 4-19  ifConfig Parameters (continued)

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>irq addr</td>
<td>Set the interrupt line used by this device. Not all devices can dynamically change their IRQ setting.</td>
</tr>
<tr>
<td>io_addr addr</td>
<td>Set the start address in I/O space for this device.</td>
</tr>
<tr>
<td>mem_start addr</td>
<td>Set the start address for shared memory used by this device. Only a few devices need this parameter set.</td>
</tr>
<tr>
<td>media type</td>
<td>Set the physical port, or medium type, to be used by the device. Not all devices can change this setting, and those that can vary in what values they support. Typical values for type 10base2 (thin Ethernet), 10baseT (twisted-pair 10Mbps Ethernet), AUI (external transceiver) and so on. The special, medium type of auto can be used to tell the driver to auto-sense the media. Not all drivers support this feature.</td>
</tr>
<tr>
<td>[-]broadcast [addr]</td>
<td>If the address argument is given, set the protocol broadcast address for this interface. Otherwise, set (or clear) the IFF_BROADCAST flag for the interface.</td>
</tr>
<tr>
<td>[-]pointopoint [addr]</td>
<td>This keyword enables the point-to-point mode of an interface, meaning that it is a direct link between two machines, with nobody else listening on it. If the address argument is also given, set the protocol address of the other side of the link, just like the obsolete dstaddr keyword does. Otherwise, set or clear the IFF_POINTOPOINT flag for the interface.</td>
</tr>
<tr>
<td>hw class address</td>
<td>Set the hardware address of this interface, if the device driver supports this operation. The keyword must be followed by the name of the hardware class and the printable ASCII equivalent of the hardware address. Hardware classes currently supported include: ether (Ethernet), ax25 (AMPR AX.25), ARCnet and netrom (AMPR NET/ROM).</td>
</tr>
<tr>
<td>multicast</td>
<td>Set the multicast flag on the interface. This should not normally be needed, as the drivers set the flag correctly themselves.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address to be assigned to this interface.</td>
</tr>
<tr>
<td>txqueuelen length</td>
<td>Set the length of the transmit queue of the device. It is useful to set this to small values, for slower devices with a high latency (modem links, ISDN), to prevent fast bulk transfers from disturbing interactive traffic, like telnet, too much.</td>
</tr>
<tr>
<td>--save</td>
<td>Saves the interface IP configuration. Not available when UTM-1 is installed.</td>
</tr>
</tbody>
</table>
**vconfig**

Configure virtual LAN interfaces.

**Syntax**

```
vconfig add [interface-name] [vlan_id]
vconfig rem [vlan-name]
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>The name of the Ethernet card that hosts the VLAN.</td>
</tr>
<tr>
<td>vlan_id</td>
<td>The identifier (0-4095) of the VLAN.</td>
</tr>
<tr>
<td>skb_priority</td>
<td>The priority in the socket buffer (sk_buff).</td>
</tr>
<tr>
<td>vlan_qos</td>
<td>The 3 bit priority field in the VLAN header.</td>
</tr>
<tr>
<td>name-type</td>
<td>One of:</td>
</tr>
<tr>
<td></td>
<td>• VLAN_PLUS_VID (e.g. vlan0005),</td>
</tr>
<tr>
<td></td>
<td>• VLAN_PLUS_VID_NO_PAD (e.g. vlan5),</td>
</tr>
<tr>
<td></td>
<td>• DEV_PLUS_VID (e.g. eth0.0005),</td>
</tr>
<tr>
<td></td>
<td>• DEV_PLUS_VID_NO_PAD (e.g. eth0.5)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bind-type</th>
<th>One of:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• PER_DEVICE  # Allows vlan 5 on eth0 and eth1 to be unique</td>
</tr>
<tr>
<td></td>
<td>• PER_KERNEL # Forces vlan 5 to be unique across all devices</td>
</tr>
</tbody>
</table>

| flag-num      | Either 0 or 1 (REORDER_HDR). If set, the VLAN device will move the Ethernet header around to make it look exactly like a real Ethernet device. |

**route**

Show, configure or save the routing entries.
Network Configuration Commands

Syntax

```
route [-nNvee] [-FC] [<AF>] List kernel routing tables
route [-v] [-FC] {add|del|flush} ... Modify routing table for AF.
route {-h|--help} [<AF>] Detailed usage syntax for specified AF.
route {-V|--version} Display version/author and exit.
route --save
```

Table 4-21  route Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
<th>extended meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>verbose</td>
<td>be verbose (detailed)</td>
</tr>
<tr>
<td>-n</td>
<td>numeric</td>
<td>do not resolve names</td>
</tr>
<tr>
<td>-N</td>
<td>symbolic</td>
<td>resolve hardware names</td>
</tr>
<tr>
<td>-e</td>
<td>extend</td>
<td>display other or more information</td>
</tr>
<tr>
<td>-F</td>
<td>fib</td>
<td>display Forwarding Information Base (default)</td>
</tr>
<tr>
<td>-C</td>
<td>cache</td>
<td>display routing cache, instead of FIB</td>
</tr>
<tr>
<td>-A &lt;AF&gt;</td>
<td>af &lt;AF&gt;</td>
<td>Address family, may be one of the following: inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)</td>
</tr>
</tbody>
</table>

netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)

save  Save the routing configuration

hostname

Show or set the system’s host name.
Network Configuration Commands

**Syntax**

```
hostname [--help]
hostname <host>
hostname <host> <external_ip_address>
```

**Table 4-22**  hostname Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>show host name</td>
<td>show host name</td>
</tr>
<tr>
<td>host</td>
<td>new host name</td>
</tr>
<tr>
<td>external_ip_address</td>
<td>IP address of the interface to be assigned</td>
</tr>
<tr>
<td>help</td>
<td>show usage message</td>
</tr>
</tbody>
</table>

**domainname**

Show or set the system’s domain name.

**Syntax**

```
domainname [<domain>]`

**Parameters**

**Table 4-23**  domainname Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>Show domainname</td>
</tr>
<tr>
<td></td>
<td>Set domainname to domain</td>
</tr>
</tbody>
</table>

**dns**

Add, remove, or show the Domain Name resolving servers.
Network Configuration Commands

**Syntax**

dns [add|del <ip_of_nameserver>]

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>show DNS servers configured</td>
</tr>
<tr>
<td>add</td>
<td>add new nameserver</td>
</tr>
<tr>
<td>del</td>
<td>delete existing nameserver</td>
</tr>
<tr>
<td>&lt;ip_of_nameserver&gt;</td>
<td>IP address of the nameserver</td>
</tr>
</tbody>
</table>

**sysconfig**

Interactive script to set networking and security of the system.

**Syntax**

sysconfig

**webui**

webui configures the port the SecurePlatform HTTPS web server uses for the management interface.

**Syntax**

webui enable [https_port]
webui disable

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable [https_port]</td>
<td>enable the Web GUI on port https_port</td>
</tr>
<tr>
<td>disable</td>
<td>disable the Web GUI</td>
</tr>
</tbody>
</table>
Dynamic Routing Commands

Only SecurePlatform Pro supports Dynamic Routing Commands.

Router

Configures Check Point Dynamic Routing.

Syntax

```
router [enable | config | disable]
```

Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable Dynamic Routing</td>
</tr>
<tr>
<td>config</td>
<td>invokes the Dynamic Routing CLI (For more information, refer to “Command Line Interface” on page 101.)</td>
</tr>
<tr>
<td>disable</td>
<td>disable Dynamic Routing</td>
</tr>
</tbody>
</table>
User and Administrator Commands

In This Section

adduser  page 90
deluser  page 90
showusers  page 90
lockout  page 91
unlockuser  page 91
checkuserlock  page 91

**adduser**

adduser adds a SecurePlatform administrator. (SecurePlatform supports RADIUS authentication for SecurePlatform administrators.)

**Syntax**

```
adduser [-x EXTERNAL_AUTH] <user name>
```

**deluser**

deluser deletes a SecurePlatform administrator.

**Syntax**

```
deluser <user name>
```

**showusers**

showusers displays all SecurePlatform administrators.

**Syntax**

```
showusers
```
User and Administrator Commands

**lockout**

Lock out a SecurePlatform administrator.

**Syntax**

```
lockout enable <attempts> <lock_period>
lockout disable
lockout show
```

**Parameters**

Table 4-27  lockout Parameters

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable attempts</td>
<td>Activate lockout after a specified number of unsuccessful attempts to login, and lock the account for lock_period minutes.</td>
</tr>
<tr>
<td>lock_period</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td>Disable the lockout feature.</td>
</tr>
<tr>
<td>show</td>
<td>Display the current settings of the lockout feature.</td>
</tr>
</tbody>
</table>

**unlockuser**

Unlock a locked administrator (see “lockout” on page 91).

**Syntax**

```
unlockuser <username>
```

**checkuserlock**

Display the lockout status of a SecurePlatform administrator (whether or not the administrator is locked out).

**Syntax**

```
checkuserlock <username>
```
SNMP Support

SNMP Support

In This Section

Configuring the SNMP Agent page 92
SNMP Monitoring page 93

SNMP support is based on the Net-SNMP open source package, and provides the following features:

- Support for full OS-MIB-II.
- Monitoring of Check Point status Information (AMON) through SNMP.
- SNMP V.2 and V.3 Support.

Configuring the SNMP Agent

For basic SNMP configuration use the `snmp` command in the restricted shell, as follows:

```
snmp service enable [<portnumber>]
snmp service stat
snmp service disable
snmp user add noauthuser <username> [oidbase <OID>]
snmp user add authuser <username> pass <passphrase> [priv <privacyphrase>] [oidbase <OID>]
snmp user del [<username>]
snmp user show [<username>]
```
**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp service enable</code></td>
<td>starts SNMP agent daemon listening on the specified UDP port.</td>
</tr>
<tr>
<td><code>snmp service disable</code></td>
<td>stops the SNMP agent daemon.</td>
</tr>
<tr>
<td><code>snmp service stat</code></td>
<td>displays service status.</td>
</tr>
<tr>
<td><code>snmp user</code></td>
<td>adds an SNMP v3 user to the agent. Authentication and encryption passwords can be specified for the user. Additionally, the user's access can be restricted to the specified OID sub-tree.</td>
</tr>
<tr>
<td><code>snmp user delete</code></td>
<td>deletes a user. SNMP v1 and v2 users can also be deleted using this command.</td>
</tr>
<tr>
<td><code>snmp user show</code></td>
<td>displays a list of existing users.</td>
</tr>
<tr>
<td><code>snmp user show</code> [&lt;username&gt;]</td>
<td>displays the specified user's (or all users') details: access level information and OID subtree restriction.</td>
</tr>
</tbody>
</table>

**SNMP Monitoring**

In This Section

- Introduction to SNMP Monitor  page 93
- SNMP Monitor Configuration Guidelines  page 94
- Commands used by SNMP Monitor  page 94
- Configuring SNMP Monitoring and Traps  page 96

**Introduction to SNMP Monitor**

Check Point `snmpmonitor` is a daemon, running on SecurePlatform, designed to monitor SNMP OIDs and to send SNMP traps at regular intervals to a trap sink server for as long as the OID value is in breach of a configurable threshold. A clear trap is sent when the OID value is back within threshold boundaries.

The `snmpmonitor` daemon integrates with the default SecurePlatform net-snmp / Agentx components that are part of the standard Check Point SecurePlatform installation.
**SNMP Monitor Configuration Guidelines**

For each OID that you wish to monitor, a monitoring rule must be defined in the `/etc/snmp/snmpd.conf` file. The following parameters are required for each monitoring rule:

1. The OID to monitor.
3. A threshold value: either an integer (not enclosed within double quotes "") or a string (enclosed within double quotes ").
4. A polling interval (in seconds).
5. A message (e.g. "HA sync link 1 down", "Internet VLAN down", "Low REAL memory", etc.).

General configuration guidelines are:

- All configuration is performed in the `/etc/snmp/snmpd.conf` file.
- Double quotes are required for enclosing string values.
- Single quotes are not supported for enclosing string values but may be used inside string values.
- Lines that start with `#` are ignored.
- All lines that do not start with `snmp monitor` daemon commands are ignored.

**Commands used by SNMP Monitor**

**cp_monitor**

The `cp_monitor` command defines a single monitoring rule.

```
.cp_monitor <OID> <Operator> <Threshold> <Frequency> <Message>
```
Once the expression `<oid> <operator> <threshold>` evaluates to true, traps are sent until the expression evaluates back to false. At that point one or more clear traps are sent to indicate that the OID value has fallen back within acceptable boundaries.

**Table 4-29  cp_monitor parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>Use standard OID notation. OID types supported are: Integer, String.</td>
</tr>
<tr>
<td>Operator</td>
<td>For OIDs of type Integer: Use one of: !, &lt;, &gt;, ==. For OIDs of type String: Use one of: !=, ==.</td>
</tr>
<tr>
<td>Threshold</td>
<td>For OIDs of type Integer: an integer value. For OIDs of type String: a string enclosed within double quotes **</td>
</tr>
<tr>
<td>Frequency</td>
<td>Integer value representing polling interval in seconds. The daemon polls each monitored OID at the given interval. If a trap should fire it is then fired.</td>
</tr>
<tr>
<td>Message</td>
<td>A textual message to describe the trap (sent as part of the trap), must be enclosed within double quotes **.</td>
</tr>
</tbody>
</table>

**Example:**

```
cp_monitor 1.3.6.1.4.1.2021.4.6.0 < 2000 5 "memAvailReal"
cp_monitor 1.3.6.1.4.1.2620.1.5.6.0 != "active" 5 "Cluster State"
```

To verify correctness of OID used in a `cp_monitor` line make sure the equivalent `snmpget` command returns a value. For example, if attempting to configure the above example `cp_monitor "memAvailReal"` line, then the following `snmpget` command should return a value:

```
"snmpget -v 2c -c public localhost 1.3.6.1.4.1.2021.4.6.0"
```

**cp_cleartrap**

The optional `cp_cleartrap` command can instruct the daemon about the number of clear traps to send and the interval between each. That is, once a rule's OID value falls back to being within configured threshold.

```
cp_cleartrap <interval> <retries>
```
SNMP Monitoring

Default values are: 3 packets at 10 seconds intervals.

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>A number indicating time between clear trap packets, in seconds.</td>
</tr>
<tr>
<td>Retries</td>
<td>A number indicating number of clear trap packets to send.</td>
</tr>
</tbody>
</table>

**trap2sink**

The `trap2sink` command designates a host that receives traps.

```
trap2sink <sink-server>[:<port>] <community>
```

The `snmpmo, .nitor` daemon requires a `trap2sink` command to exist inside the `/etc/snmp/snmpd.conf` file. The `trap2sink` command is required (as opposed to the `trapsink` command) because the `snmpmonitor` daemon sends SNMP version 2c traps. Note this command is part of the net-snmp syntax.

**Table 4-31 trap_2_sink parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>sink-server</td>
<td>A sink server for which traps are sent.</td>
</tr>
<tr>
<td>port</td>
<td>An optional (UDP) port number on which the server listens, the default is port 162.</td>
</tr>
<tr>
<td>community</td>
<td>An SNMP community</td>
</tr>
</tbody>
</table>

Example:

```
trap2sink 10.10.10.10 public
trap2sink 10.10.10.10:1610 MyCommunity
```

**Configuring SNMP Monitoring and Traps**

To configure SNMP monitoring and traps:
1. Edit the `/etc/snmp/snmpd.conf` configuration file and define the SNMP monitoring rules and the trap server. The following is an example configuration file:

```
trap2sink 10.10.10.10 public
cp_cleartrap 10 2
proc syslogd 1 1
disk /var 20%
cp_monitor 1.3.6.1.2.1.2.1.8.1 == 2 60 "link 1 down"
cp_monitor prErrorFlag.1 != "0" 60 "process monitor"
cp_monitor dskErrorFlag.1 != 0 60 "disk monitor"
cp_monitor 1.3.6.1.4.1.2021.10.1.5.1 > 100 60 "CPU load 1 min"
cp_monitor 1.3.6.1.4.1.2021.10.1.5.2 > 90 60 "CPU load 5 min"
cp_monitor 1.3.6.1.4.1.2021.4.4.0 < 2000 60 "memAvailSwap"
cp_monitor 1.3.6.1.4.1.2021.4.6.0 < 2000 60 "memAvailReal"
cp_monitor 1.3.6.1.4.1.2620.1.5.6.0 != "active" 20 "Cluster State"
cp_monitor 1.3.6.1.4.1.2620.1.1.25.3.0 > 50000 20 "Firewall connections"
cp_monitor 1.3.6.1.2.1.25.2.3.1.6.6 > 60000 60 "/opt hrStorageUsed"
```

2. At the SecurePlatform command prompt, start the `snmp` service:

```
snmp service enable
```
Check Point Dynamic Routing

In This Section

Supported Features page 98
Command Line Interface page 101

Check Point now supports Dynamic Routing (Unicast and Multicast) protocols, as an integral part of SecurePlatform. Configuration is done via an "Industry-Standard" Command-Line-Interface that is integrated into the SecurePlatform Shell. Other administration tasks, such as log viewing, are performed via the standard SecurePlatform tools. This chapter discusses the integration of SecurePlatform and Dynamic Routing.

Supported Features

In This Section:

Supported Protocols page 98
Enabling and Disabling Dynamic Routing Support page 99
Tracing and Logging Options page 99
Status Monitoring via SNMP page 100
Backup and Restore page 100

This section discusses several key features supported by Check Point Dynamic Routing.

Supported Protocols

The following protocols are supported by Check Point Dynamic Routing:

- Unicast
  - RIP-1
  - RIP-2
  - OSPF
  - BGP
- Multicast
Supported Features

- PIM-DM
- PIM-SM
- IGMP

**Enabling and Disabling Dynamic Routing Support**

The `router` CLI command is essential for using and configuring Check Point Dynamic Routing:

The `router` command syntax and parameter description are provided below:

```
router
```

Configures Check Point Dynamic Routing.

**Syntax**

```
router [enable | config | disable]
```

**Parameters**

<table>
<thead>
<tr>
<th>parameter</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable Dynamic Routing</td>
</tr>
<tr>
<td>config</td>
<td>invokes the Dynamic Routing CLI (For more information, refer to “Command Line Interface” on page 101.)</td>
</tr>
<tr>
<td>disable</td>
<td>disable Dynamic Routing</td>
</tr>
</tbody>
</table>

The Check Point Dynamic Routing state is preserved during the reboot operation, for example if it was Enabled before the reboot, it remains Enabled after the reboot.

**Note** - The Dynamic Routing configuration, however, is not preserved during the reboot operation. Only the last configuration, saved via the CLI, is preserved during the reboot.

**Tracing and Logging Options**

Check Point Dynamic Routing's tracing options can be configured at many levels. Tracing options include the file specifications and global and protocol-specific tracing options. The trace files can later be viewed by using the Log Switch mechanism.
Supported Features

The Dynamic Routing logging messages are stored in 'routing_messages' and can be viewed using the standard SecurePlatform logging mechanism.

For more detailed information, refer to “log” on page 71.

**Status Monitoring via SNMP**

Check Point Dynamic Routing supports SNMP, via the RFC 1227 SMUX interface. It is enabled by default. Use a standard SNMP client to retrieve the Dynamic Routing status information, via SNMP.

Only SNMP version 1 is supported, and all MIB variables are read-only. For more detailed information, refer to “SNMP Support” on page 92.

**Backup and Restore**

The SecurePlatform mechanism stores and restores the Dynamic Routing configuration, as well. This is also true, if you use the snapshot and revert commands.

**Note** - The Dynamic Routing configuration is stored as part of the system configuration. For more detailed information, refer to “Backup and Restore” on page 53.
Command Line Interface

In This Section:

- Overview page 101
- Command Line Editing and Completion page 101
- Context-Sensitive Help page 101
- Command History page 101
- Disabling/Enabling CLI Tracing page 102

Overview

Check Point Dynamic Routing utilizes industry standard commands for configuration. The basic features of the CLI include the following:

- Command line editing and completion
- Context-sensitive help
- Command history
- Disabling/Enabling CLI Tracing

Command Line Editing and Completion

At any point when typing a command line, you can hit the Tab key to either complete the current command, or show a list of possible completions.

Context-Sensitive Help

Type "?" immediately after any command to obtain context-sensitive help about the last command that you typed. Type "?" after any set of commands to obtain a list of options that can be used in the command.

Command History

All commands entered during a CLI session are saved in a command history. The history can be toggled on and off.
Disabling/Enabling CLI Tracing

The CLI provides a flexible tracing mechanism. Events to be traced are divided into several classes, each of which can be traced individually. Classes can be traced to any or to all three of the following locations: the terminal, a file, or the underlying system's tracing system (i.e., syslog).
SecurePlatform Boot Loader

In This Section

Booting in Maintenance Mode  page 103
Customizing the Boot Process  page 104
Snapshot Image Management  page 104

Each time the SecurePlatform machine is booted the boot loader screen is displayed. The boot loader offers a selection of boot options and allows customization of the boot process, including the possibility to boot from a snapshot image (if one is present).

By default, if there is no user intervention, the boot loader will select the boot option selected last time (or the default option, if no option was ever selected).

Booting in maintenance mode and customizing the boot process require a password. The password is the system's Expert mode password.

Tip - The first time that you switch to Expert mode you will be asked to select a password. Until then, it is the same as the Standard password, i.e. you need to enter the first replacement password that you used when logging in as the admin user. Any sequential admin password change will not update the expert password that you must enter at the first-time expert user password change.

Warning - Changing the boot options and customizing the boot process requires a high level of understanding of system administration and Linux.

Booting in Maintenance Mode

Maintenance Mode should be used in rare system emergencies, such as when there is a problem rebooting the system, or the Standard admin password is lost. To reboot in this mode, position the selection bar on “SecurePlatform with Application Intelligence [Maintenance Mode]” and click Enter. You will be asked to enter a password.

Selecting the Maintenance Mode boot option will boot your SecurePlatform in a special mode, known on Unix systems as “single-user mode”. In this mode, your computer boots to runlevel 1. Your local file systems will be mounted, but your network will not be activated. You will have a usable system maintenance shell.
Customizing the Boot Process

To customize the boot process, click p in order to enter a password and unlock the next set of features. The password is the Expert password that you set for your system. The following options are available:

- Click e to edit any of the boot options (position the selection bar on the relevant boot option).
- Click c to perform root level system operations.

Snapshot Image Management

At boot time, the user is given the option of switching to any of the available snapshots. For more information, see “Snapshot Image Management” on page 68.
Chapter 5

SecurePlatform Pro
Advanced Routing Suite

In This Chapter

Introduction  page 106
Check Point Advanced Routing Suite  page 107
Introduction

SecurePlatform Pro integrates support for dynamic routing. For more information regarding SecurePlatform Pro see: “SecurePlatform Pro” on page 20

Note - Advanced Routing Suite does not allow the configuration of static routes. Use standard SecurePlatform tools to maintain static routes
Check Point Advanced Routing Suite

In This Section

Supported Features ............................................. page 107
Command Line Interface ....................................... page 111

Check Point now supports Dynamic Routing (Unicast and Multicast) protocols, as an integral part of SecurePlatform Pro. Configuration is done via an "Industry-Standard" Command-Line-Interface that is integrated into the SecurePlatform Shell. Other administration tasks, such as log viewing, are performed via the standard SecurePlatform tools. This chapter discusses the integration of SecurePlatform and Dynamic Routing.

The Advanced routing suite is also supported with ClusterXL.

For more information about the Advanced Routing suite, see the Advanced Routing Suite Command Line Interface guide at http://supportcontent.checkpoint.com/documentation_download?ID=8743

Supported Features

In This Section:

Dynamic Routing ................................................ page 107
Supported Protocols ........................................... page 109
Enabling and Disabling Dynamic Routing Support ....... page 109
Configuring Dynamic Routing Protocols ................. page 110
Tracing and Logging Options ................................. page 110
Backup and Restore ........................................... page 110

Dynamic Routing

Dynamic routing is implemented in the following way:

- Each Virtual Device (Virtual System or Virtual Router) has its own routing daemon.
- Each Virtual Device on the VSX gateway has to be configured separately.
Dynamic Routing

- For a VSX cluster, each Virtual Device on the cluster members has to be configured separately. This means if you have two physical machines combined to a single cluster, the Virtual Devices on each machine have to be configured independently.

To enable dynamic routing

1. Open a Secure Shell connection to the VSX gateway. You are automatically in the default (VSX:0) context. Run `fw vsx stat -v` to view the Virtual Systems and their IDs:

   ```
   [Expert@vsx57:vs0]# vsx stat -v
   VSX Gateway Status
   ===============
   Name:                    vsx57
   Management IP Address:   172.23.3.57
   Security Policy:         Standard
   Installed at:            1May2005 15:37:36
   SIC Status:              Trust
   Number of Virtual Systems allowed by license:       100
   Virtual Systems [active / configured]:              3 / 3
   Virtual Routers and Switches [active / configured]: 0 / 0
   Virtual Devices Status
   =====================
   ID | Type & Name | Security Policy | Installed at | SIC Stat
   ----------------------|-----------------|-----------------|--------------|--------
   1 | S vsx57_vs1  | Standard        | 1May2005 15:37 | Trust
   2 | S vsx57_vs2  | Standard        | 1May2005 15:37 | Trust
   3 | S vsx57_vs3  | Standard        | 1May2005 15:37 | Trust
   Type: S - Virtual System, B - Virtual System in Bridge mode, R - Virtual Router, W - Virtual Switch.
   ```

2. Run `drouter` to either enable or disable the routing daemon on the Virtual Device.

   - `drouter enable <vs_id>` enables and starts dynamic routing for the Virtual Device
   - `drouter disable <vs_id>` stops and disables dynamic routing for the Virtual Device
   - `drouter start <vs_id>` starts dynamic routing for the Virtual Device
   - `drouter stop <vs_id>` stops dynamic routing for the Virtual Device
To Configure Dynamic Routing

1. Open the Command Line Interface to the dynamic routing application.
   - `router` starts the Advanced Routing Suite Command Line Interface.
   - `vrf-connect` is a command that determines for which Virtual Device the dynamic routing configuration applies. For example:

```
[Expert@vsx57:vs0]# router
>vrf-connect 2
localhost.localdomain-VRF-2>enable
localhost.localdomain-VRF-2#
```

Backward Compatibility Support

From current release you create and manage:
- VSX 2.0.1 objects
- VSX_NG_AI objects

Supported Protocols

The following protocols are supported by Check Point Dynamic Routing:
- Unicast
  - RIP-1
  - RIP-2
  - OSPF
  - BGP
- Multicast
  - PIM-DM
  - PIM-SM
  - IGMP

Enabling and Disabling Dynamic Routing Support

Enabling and disabling the Advanced Routing Suite is performed through `cpconfig` by selecting the relevant option.
Configuring Dynamic Routing Protocols

The following CLI command is essential for use of Check Point Dynamic Routing:

- router: Configures Check Point Dynamic Routing.

Tracing and Logging Options

Check Point Dynamic Routing's tracing options can be configured at many levels. Tracing options include the file specifications and global and protocol-specific tracing options. The trace files can later be viewed by using the Log Switch mechanism.

The Dynamic Routing logging messages are stored in 'routing_messages' and can be viewed using the standard SecurePlatform logging mechanism.

Backup and Restore

The SecurePlatform mechanism stores and restores the Dynamic Routing configuration, as well.

Note - The Dynamic Routing configuration is stored as part of the system configuration.
In This Section:

Overview page 111
Command Line Editing and Completion page 111
Context-Sensitive Help page 111
Command History page 111
Disabling/Enabling CLI Tracing page 112

Overview

Check Point Dynamic Routing utilizes industry standard commands for configuration. The basic features of the CLI include the following:

- Command line editing and completion
- Context-sensitive help
- Command history
- Disabling/Enabling CLI Tracing

Command Line Editing and Completion

At any point when typing a command line, you can hit the Tab key to either complete the current command, or show a list of possible completions.

Context-Sensitive Help

Type "?" immediately after any command to obtain context-sensitive help about the last command that you typed. Type "?" after any set of commands to obtain a list of options that can be used in the command.

Command History

All commands entered during a CLI session are saved in a command history. The history can be toggled on and off.
Disabling/Enabling CLI Tracing

The CLI provides a flexible tracing mechanism. Events to be traced are divided into several classes, each of which can be traced individually. Classes can be traced to any or to all three of the following locations: the terminal, a file, or the underlying system's tracing system (i.e., syslog).
Appendix

Installation on Computers without Floppy or CDROM Drives

In This Appendix

General Procedure  page 114
Client Setup  page 114
Server Setup  page 115

You must set up a server for network installation, and perform some client setup on the host, on which SecurePlatform is being installed.

Note - It is not recommended to use a system that was installed in this manner in a production environment. It should only be used as an Installation Server for SecurePlatform.
General Procedure

The network installation is performed as follows:

1. The client boots from the network, using the PXE network loader.
2. The client sends a broadcast request, using the BOOTP protocol.
3. The server responds to the client, by providing the client's assigned IP address and a filename (pxelinux.0 by default), to which to download the PXE boot loader.
4. The client downloads the PXE Boot Loader, using TFTP, and executes it.
5. The PXE boot loader downloads a PXE configuration file from the server, containing the names of the kernel and the ramdisk that the client requires.
6. The PXE boot loader downloads the kernel and the ramdisk.
7. The kernel is run, using ramdisk as its environment.
8. The Installer is executed.
9. At this point the installation can be configured to load files from the FTP server.

The client's requirements are minimal. Only PXE is required.

The server needs a little more configuring. You must install a DHCP daemon, a TFTP daemon, the PXE boot loader, the kernel and the ramdisk.

Client Setup

On the client machine, enable the network boot, using PXE, from the BIOS setup. (It sometimes appears as DHCP.) The procedure differs from machine to machine. Consult specific machine documentation, if necessary.
Server Setup

In This Section

Required Packages  page 115
DHCP Daemon Setup  page 116
TFTP and FTP Daemon Setup  page 117
Hosting Installation Files  page 118

The following setup details and instructions apply to a server running SecurePlatform, as its operating system. Setup on a server running a different OS may differ slightly.

Required Packages

The following packages are required for server setup:

- DHCP daemon (located on the Checkpoint CDROM and installed, by default, on SecurePlatform)
- Xinetd (/SecurePlatform/RPMS/xinetd-2.3.11-4cp.i386.rpm on the Checkpoint CDROM)
- TFTP daemon (/SecurePlatform/RPMS/tftp-server-0.32-5cp.i386.rpm)
- FTP server (/SecurePlatform/RPMS/ftpd-0.3.3-118.4cp.i386.rpm)
- TCP-Wrappers package (/SecurePlatform/RPMS/tcp_wrappers-7.6-34.4cp.i386.rpm)
- Kernel (can be found on the SecurePlatform CD at /SecurePlatform/kernel)
- Ramdisk (can be found on the SecurePlatform CD at /SecurePlatform/ramdisk-pxe)

Note - To access files on Check Point CDROM, insert the CDROM into the CDROM drive and enter the command: 

```sh
# mount/mnt/cdrom
```
PXELINUX Configuration Files

/SecurePlatform/RPMS/tftp-server-0.32-4cp.i386.rpm includes a default configuration file (located under /tftpboot/pxelinux.cfg) that will serve the kernel and ramdisk to any host. Because more than one system may be booted from the same server, the configuration file name depends on the IP address of the booting machine.

PXELINUX will search for its config file on the boot server in the following way:

1. PXELINUX will search for its config file, using its own IP address, in upper case hexadecimal, e.g. 192.0.2.91 -> C000025B.

2. If that file is not found, PXELINUX will remove one hex digit and try again. Ultimately, PXELINUX will try looking for a file named default (in lower case).

As an example, for 192.0.2.91, PXELINUX will try C000025B, C000025, C00002, C0000, C000, C00, C0, C, and default, in that order.

Assuming the kernel and ramdisk files are named kernel and ramdisk, respectively, a default configuration file, which will serve these to all clients, will look like this:

```
default bootnet
label bootnet
kernel kernel
append initrd=ramdisk lang= devfs=nomount \ramdisk_size=80024 console=tty0
```

DHCP Daemon Setup

To setup the DHCP Daemon, perform the following procedure:

1. Enter the `sysconfig` utility and enable the DHCP server.
TFTP and FTP Daemon Setup

To setup the TFTP and FTP Daemons, perform the following procedure:

1. Install `/SecurePlatform/RPMS/tcp_wrappers-7.6-34.4cp.i386.rpm` (The TCP wrappers package)
2. Install `/SecurePlatform/RPMS/xinetd-2.3.11-4cp.i386.rpm` (The xinetd package is a prerequisite for the tftp-server and ftpd.)
3. Install the TFTP Daemon RPM:
   ```
   # rpm -i /SecurePlatform/RPMS/tftp-server-0.32-5cp.i386.rpm
   ```
4. Install the FTP Daemon RPM:
   ```
   # rpm -i /SecurePlatform/RPMS/ftpd-0.3.3-118.4cp.i386.rpm
   ```
5. Force xinted to reread its configuration:
   ```
   # service xinetd restart
   ```

2. Edit the daemon’s configuration file, found at `/etc/dhcpd.conf`. The configuration file should include a subnet declaration for each subnet, the DHCP server is connected to. In addition, configuration should include a host declaration, for each host that will use this server for remote installation. A sample configuration file follows:

```plaintext
subnet 192.92.93.0 netmask 255.255.255.0 {
}host foo {
    # The client’s MAC address
    # The IP address that will be assigned to the
    # client by this server
    fixed-address 192.92.93.32;
    # The file to upload
    filename "/pxelinux.0";
}
```

TFTP and FTP Daemon Setup
Hosting Installation Files

An FTP server installed on SecurePlatform will be used to host the installation files. During the installation process, you will be asked to supply the IP of the installation server, the credentials on that server, and the path to the installation packages. Supply the IP of the SecurePlatform installation server, the Administrator’s credentials, and the path to the SecurePlatform packages.

You can also use different FTP servers, or HTTP servers, to host SecurePlatform installation files.