

Chapter

Introduction to SecurePlatform

2

Before delving into the intricacies of creating and managing Security Policies, it is beneficial to first understand the workings of Check Point SecurePlatform, Check Point's Linux-based operating system that is the framework for many Check Point products. For those familiar with Linux, this is a review. But for those with little to no Linux experience, this will be a welcome guide.

Objectives:

- Given the most current configuration, update the appropriate network interface using the sysconfig utility to change the management interface.
- Given specific instructions, perform a backup and restore of the current Gateway installation from the command line.

Key Terms:

- Check Point SecurePlatform
- Hardware Compatibility Testing Tool
- SecurePlatform Command Shell
- Secure Shell (SSH)
- Standard Mode
- Expert Mode

COPY

Introduction

Check Point SecurePlatform is distributed on a bootable CD-ROM, which includes Check Point's product suite comprised of VPN-1, Check Point QoS, SmartView Monitor, Policy Server, and UserAuthority Server. The system is preconfigured and optimized as a network-security device, requiring only minimal user configuration of IP addresses, routes, etc. SecurePlatform allows easy configuration of your computer and networking aspects, along with installed Check Point products. The Linux shell provides a convenient set of commands, including network settings, backup- and-restore utilities, an upgrade utility, and system-log viewing. As in the lab "VPN-1 Distributed Installation", a WebUI 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 and Setup

On SecurePlatform, the minimum hardware requirements for installing a VPN-1 SmartCenter Server, Security Gateway, or SmartPortal are:

- Intel Pentium III 300+ MHz or equivalent processor.
- 10 GB free disk space.
- 256 MB (512 MB recommended).
- One or more supported network-adaptor cards.
- CD-ROM drive (bootable).
- 1024 x 768 video-adaptor card.

For details regarding SecurePlatform on specific hardware platforms, see:

<http://www.checkpoint.com/services/techsupport/hcl/index.html>

Hardware Compatibility Testing Tool

The **Hardware Compatibility Testing Tool** enables you to determine whether SecurePlatform is supported on a specific hardware platform. The following describe key points for using the tool:

- The utility is available for download as a CD ISO image (**hw.iso**). The ISO image can be burned on blank CD-R or CD-RW media, using a CD-burning tool. The Hardware Compatibility Testing Tool should be run in the same way that would be used to install SecurePlatform on the hardware platform (for example, booting from CD, booting from disk, and installing through a network, etc.).
- You must specify that you are burning the CD image and not a single file.

- 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, supported mass-storage device found), and the number of supported and unsupported Ethernet controllers detected.
- The user can view detailed information on all devices found on the machine.
- The user can save the detailed information on a disk, on a TFTP server, or dump it via the serial port. This information can be submitted to Check Point Support to add support for unsupported devices.
- SecurePlatform requires the following hardware:
 - I/O device (either keyboard and monitor, or serial console)
 - Mass-storage device
 - At least one supported Ethernet controller (If SecurePlatform is to be configured as a VPN-1 Gateway, more than one controller is needed.)
 - The tool makes no modifications to the tested hardware platform, so it is safe to use.

Using the Command Line

A Linux based platform is structured as part of a UNIX directory tree. The chart below details a typical Linux structure. Files are grouped according to purpose, such as commands, data files and documentation. See http://www.comptechdoc.org/os/linux/usersguide/linux_ugfilestruct.html.

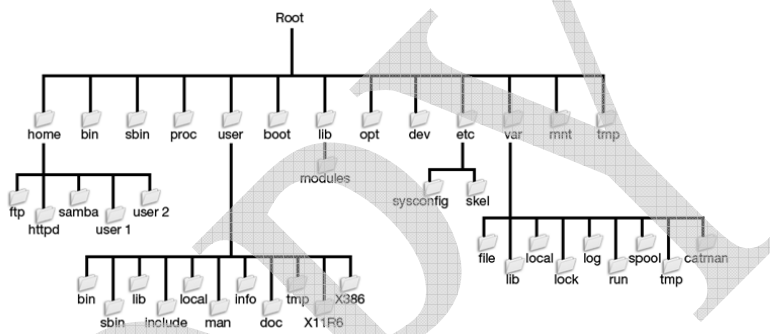


Figure 2-72: Linux File Structure

This section describes the `sysconfig`, `cpconfig`, and backup tools, which provide interactive menu systems for all configuration aspects. Configuration can also be done using command-line utilities provided by the SecurePlatform Shell. The SecurePlatform Shell is discussed in “Connecting to SecurePlatform Using Secure Shell,” on page 128.

Basic Linux Commands

sysconfig

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

- Configure the network settings.
- Apply the license.

- Select which products will be installed.
- Perform the SmartCenter initial setup, if selected.



In the lab “VPN-1 Distributed Installation”, the configuration of the Gateway was performed via the WebUI, instead of the command line. Performing the first-time configuration using the `sysconfig` utility is merely an alternative, and requires minimal interface modifications, depending on your particular network topology.

To use the `sysconfig` utility for the first time configuration, run the **`sysconfig`** command from the console to configure SecurePlatform, using a text interface. The command-line setup wizard begins, and guides you through the first-time configuration.

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`**, log in to SecurePlatform and enter **`sysconfig`** at the prompt.

If performing the first-time installation via the command-line, Check Point recommends step-by-step configuration, by addressing each menu item in sequence. 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 the user to enter all relevant configuration parameters. As soon as all parameters are completed, the change is applied.

`sysconfig` Menu Options

1. **Host Name** — Set or show hostname.
2. **Domain Name** — Set or show domain name.

3. **Domain Name Servers** — Add or remove Domain Name Servers (DNS), or show configured Domain Name Servers.
4. **Time & Date** — Set the time zone, date and local time, or show the date-and-time settings.
5. **Network Connections** — Add or remove connections, configure network connections, or show configuration of network connections.
6. **Routing** — Add network and route, add new host, set default Gateway, delete route, or show routing configuration.
7. **DHCP Server Configuration** — Configure SecurePlatform DHCP server.
8. **DHCP Relay Configuration** — Set up DHCP relay.
9. **Export Setup** — Export Check Point environment.
10. **Products Installation** — Install Check Point products (cpconfig). For more information, see the product-installation instructions.
11. **Products Configuration** — Configure Check Point products (cpconfig).

cpconfig

This command is used to run a command-line version of the Check Point Configuration Tool. This tool is used to configure or reconfigure a VPN-1 installation. The configuration options shown depend on the installed configuration and products. Among others, these options include:

- **Licenses** — Modify the necessary Check Point licenses.
- **Administrators** — Modify the Administrators authorized to connect to the SmartCenter Server via the SmartConsole.
- **GUI Clients** — Modify the list of GUI client machines from which Administrators are authorized to connect to a SmartCenter Server.

- **Certificate Authority** — Install the Certificate Authority on the SmartCenter Server in a first-time installation.
- **Key Hit Session** — Enter a random seed to be used for encryption purposes.
- **Secure Internal Communication** — Set up trust between the Gateway on which this command is being run and the SmartCenter Server
- **Fingerprint** — Display the fingerprint that will be used on first-time launch to verify the identity of the SmartCenter Server being accessed by the SmartConsole. This fingerprint is a text string derived from the SmartCenter Server's Certificate.

Backup and Restore

Backup can be performed from the command line or from the WebUI. 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 or SCP server, or locally. In addition, you can view a backup log.

The backup files are kept in tar gzip format (**.tgz**). Backup files, saved locally by default, are kept in **/var/CPbackup/backup**. The restore command-line utility is used for restoring SecurePlatform settings and/or product configuration from backup files.



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_fwoslo.oslo.cp_13_8_2007_12_47.tgz
```

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. Check Point strongly recommends 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 you are working in.

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

The following types of information can be backed up:

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

Two common-use cases are:

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

Backup can be performed in configurable schedules and run by itself. Without additional flags, Secure Platform will use default backup settings and will perform a local backup. See “System Commands,” on page 133 for syntax.

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

Viewing Scheduling Status in the WebUI

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

- **Enabled** — backup currently enabled
- **Backup to** — backup destination either the current SecurePlatform, a TFTP, or SCP server
- **Start at** — time to start the backup
- **Recur every** — recurrence pattern

Restoring the Backup via the Command Line

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>] | [--file <Filename>]]
```

Parameters

Parameter	Meaning
-h	Obtain usage
-d	Debug flag
--tftp <ServerIP> [<Filename>]	IP address of TFTP server from which the configuration is restored, and the filename

Table 2-73: restore Parameters

Parameter	Meaning
<code>--scp <ServerIP> <Username> <Password> [<Filename>]</code>	IP address of SCP server from which the configuration is restored, the username and password used to access the SCP server, and the filename
<code>--file <Filename></code>	Filename for restore operation, performed locally

Table 2-73: restore Parameters

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.

```
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

```

## Restoring Older Versions of SecurePlatform

When restoring backups of older versions of SecurePlatform, such as NG FP2 and FP3, and NG with Application Intelligence (AI), only system settings, such as routes, IP configurations, VLAN interface configurations, user accounts, hostnames, domain names, and WebUI ports will be restored. You cannot restore backups saved on newer SecurePlatform versions onto an older SecurePlatform version.

When **restore** detects that the currently installed version of Check Point products does not match the version that was stored in the backup file, the following information will be displayed,

when restoring from backups of SecurePlatform NG with AI R55 and later:

```
The following information will be restored:
 system

The following information will NOT be restored:
 cp_products

Choose one of the following:

[C] Continue.
[M] Modify which information to restore.
[Q] Quit.

Your choice:
```

If you choose to continue, only system settings will be restored.

When restoring from backups of SecurePlatform NG with AI and earlier, the following information will be shown:

```
Restoring...

Backup file was created MM-DD-YYYY-HH:MM.

The MD5 checksum of the backup file is:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Do you wish to restore this file (Y/N)?

If you choose "N", the restore operation will be
aborted.

The restore operation will replace current
configuration.

After restore you have to reboot your system.

Do you wish to proceed (Y/N)?

If you choose "N", the restore operation will be
aborted.

Restore completed successfully.

You have to reboot your system now. Reboot now (Y/N)?
```

## Scheduling a Backup in the WebUI

To schedule a backup:

1. On the **Backup** page, click **Scheduled backup**. The **Scheduled backup** page appears.
2. Check the box **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, or an SCP server.
5. Click **Apply**.



To execute an immediate backup in the WebUI, click **Backup now**.

## Viewing the Backup Log in the WebUI

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

## Generating CPInfo

**CPInfo** is a support tool that gathers into one text file a wide range of data concerning the Check Point packages in your system. When speaking with a Check Point Technical Support Engineer, you may be asked to run **CPInfo** and transmit the data to the Support Center.



This is not a restorable backup file.

To launch **CPInfo**, select **Tools > Generate CPInfo**.

1. Choose the directory to which you want to save the output file.
2. Choose between two methods to name the file:
  - based on the Service Request (SR) number the technician assigns you, or
  - a custom name that you define.
3. Optionally, you may choose to add:
  - log files to the CPInfo output
  - the registry to the CPInfo output

## Critical Check Point Directories

### *\$FWDIR/conf*

This directory contains Rule Bases, objects, and the user database.

### *\$FWDIR/bin*

Import and export tools are located under **\$FWDIR/bin/upgrade\_tools**.



Do not upgrade VPN-1, without first making a complete backup of the system. A computer backup will allow a quick restore, in case of problems.

## Log Files

The logs are displayed in SmartView Tracker. These should be logswitched regularly. The time between a logswitch will depend on how many rules are logging, the type of logging, and the amount of traffic passing through the Security Gateway. The logswitch can be configured to perform on a set schedule, using time objects. This is completed through the SmartCenter Server and log server's **General Properties**.

### *\$FWDIR/log*

**\$FWDIR/log** contains log files such as **ahttpd.log**, **aftpd.log**, and **smtpd.log**. These files contain information about each Security Server. **\$FWDIR/log** can get large quickly, depending upon the amount of network traffic passing through the Security Gateway.

## objects.C and objects\_5\_0.C

The **objects\_5\_0.C** file includes a section of properties whose values affect VPN-1 behavior. In addition, network objects, server objects, service objects, time objects, and other miscellaneous data also exist in this file. **objects\_5\_0.C** is modified when global and local properties are changed, or when the DbEdit utility is used. **objects\_5\_0.C** is used only by the SmartCenter Server. **objects\_5\_0.C** file is used to create the **objects.C** file, which is passed to the Security Gateway and

contains information required for the Gateway's operation. These files are located in the `$FWDIR/conf/` directory. `objects.C` is created when a Security Policy is installed on the Security Gateway. `objects.C` is then sent to the Gateway, along with the new Policy.

## rulebases\_5\_0.fws

The `rulebases_5_0.fws` file is located in `$FWDIR/conf`. This file contains rules and auditing information about modifications made to the Rule Base. Unlike `objects.C`, `rulebases_5_0.fws` does not appear on the Security Gateway in a distributed environment.

All created Rule Bases may be extracted from `rulebases_5_0.fws`: Select a Rule Base, then install the Security Policy on the Security Gateways. `rulebases_5_0.fws` is not modified manually, but is manipulated through SmartDashboard.

## fwauth.NDB

The `fwauth.NDB` database file contains all VPN-1 users and groups. It is located in both the `$FWDIR/conf` and `$FWDIR/database` directories. File modification is performed through SmartDashboard user administration.

## Exporting User Database Only



To export *all* VPN-1 files (your current configuration), see “Backing Up Using upgrade\_export,” on page 126.

To export users from the VPN-1 user database on the SmartCenter Server, run the `fwm dbexport` command:

```
fwm dbexport [-f file] [[-g | -u username] [-d delim]
[-a attributes]] | [-l [-p profile -s subtree
[-k isakmp shared secret]]
```

The table below lists the parameters for **fwm dbexport**:

| Parameter | Description                                                                       |
|-----------|-----------------------------------------------------------------------------------|
| <b>-f</b> | Specifies the filename and location to which the user database should be exported |
| <b>-g</b> | Specifies to export group names                                                   |
| <b>-u</b> | Exports a specific users properties                                               |
| <b>-d</b> | Specifies a delimiting character other than ;                                     |
| <b>-a</b> | Specifies special attributes                                                      |
| <b>-l</b> | LDIF option                                                                       |
| <b>-s</b> | Specifies the subtree under which all entries should be placed                    |
| <b>-p</b> | Specifies the LDAP profile that generates the LDIF file                           |
| <b>-k</b> | Account management shared-secret key                                              |

Table 2-74: fwm dbexport Parameters

The user database may need to be exported to import into another SmartCenter Server, restore from a backup, or export users, when implementing an LDAP directory server.

## Backing Up Using upgrade\_export

Before upgrading, back up your current configuration, in case the upgrade is unsuccessful. The purpose of the backup is to back up the entire configuration, and to restore it when necessary.

The backup file created contains your current system configuration (i.e., objects, rules, users, etc.), and can be used to restore your previous configuration, if the upgrade fails. Restoring returns the configuration to its original state when backed up.



If you upgrade on SecurePlatform, you do not have to back up your configuration using the Export utility. SecurePlatform provides you the option of backing up your configuration during the upgrade.

***Backing Up Manually***

To export manually, use the VPN-1 Export tool (**upgrade\_export.exe**), located in

**\$FWDIR/bin/upgrade\_tools.**

COPY

## Managing Your SecurePlatform System

This section provides information on how to manage your SecurePlatform VPN-1 system, using the SecurePlatform Command Shell. The **SecurePlatform Command Shell** provides a set of commands required for configuration, administration, and diagnostics of various system aspects.

### Connecting to SecurePlatform Using Secure Shell

SecurePlatform VPN-1 provides a **Secure Shell (SSH)** program, which allows secured, authenticated, and encrypted access to the SecurePlatform system. SSH 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 program runs by default. In addition, access to the SSH program is limited to the same IPs that have been allowed access to the WebUI. Granular control of machines that are allowed access to the SecurePlatform system using SSH can be set, using the VPN-1 Security Policy.

SSH login is allowed using the Standard Mode account username and password only. (See “Standard Mode,” on page 129.) 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 Command Shell includes two permission levels: Standard and Expert Modes.

### *Standard Mode*

This is the default mode when logging into a SecurePlatform system. In **Standard Mode**, the SecurePlatform Command 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 Command Shell,” on page 130.

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

### *Expert Mode*

**Expert Mode** provides the user with root permissions and a full system shell. Switching from Standard 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 Administrator. Any sequential administrative-password change will not update the expert password 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 hostname of the machine.



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.

An Expert Mode user must first log in as a Standard Mode user, and only then enter the **expert** command to access Expert Mode.

## SecurePlatform Command Shell

This section includes a listing of SecurePlatform's Command Shell commands. All commands are case-sensitive.

### SecurePlatform 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 a history of commands entered at the command prompt.

#### *Command-Line Editing Keys*

| Key            | Command                            |
|----------------|------------------------------------|
| RIGHT ARROW/^f | Move cursor right.                 |
| LEFT ARROW/^b  | Move cursor left.                  |
| HOME/^a        | Move cursor to beginning of line.  |
| END/^e         | Move cursor to end of line.        |
| BACKSPACE/^h   | Delete last character.             |
| ^d             | Delete character on cursor.        |
| ^u             | Delete line.                       |
| ^w             | Delete word to left.               |
| ^k             | Delete from cursor to end of line. |

Table 2-75: Command-Line Editing Keys

| Key           | Command                |
|---------------|------------------------|
| UP ARROW/^p   | View previous command. |
| DOWN ARROW/^n | View next command.     |

Table 2-75: Command-Line Editing Keys

**Command Output**

Some command output may be displayed on more than one screen. By default, the SecurePlatform Command Shell will display one screen and the prompt **-more-**. Click any key to continue to display the rest of the command output. **more** functionality can be turned on or off, using the **scroll** command.



You can also view multiple screens by holding the **SHIFT** key, and pressing **PAGE UP** or **PAGE DOWN**.

## Management Commands

| Command       | Use                                                                                                                                                                                                             | Syntax        |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <b>exit</b>   | Exit the current mode.                                                                                                                                                                                          | <b>exit</b>   |
| <b>expert</b> | Switch from Standard to Expert Mode.                                                                                                                                                                            | <b>expert</b> |
| <b>passwd</b> | 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. | <b>passwd</b> |

Table 2-76: Management Commands

## Documentation Commands

| Command          | Use                                                                                  | Syntax                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>help</b>      | List the available commands and their descriptions.                                  | <b>help or ?</b>                                                                                                                                                                                                                                                                                                                                                                       |
| <b>date</b>      | Show or set the system's date. Changing the date or time affects the hardware clock. | <b>date [MM-DD-YYYY]</b>                                                                                                                                                                                                                                                                                                                                                               |
| <b>time</b>      | Show or set the system's time. Changing the date or time affects the hardware clock. | <b>time [HH:MM]</b>                                                                                                                                                                                                                                                                                                                                                                    |
| <b>time zone</b> | Set the system's time zone.                                                          | <b>timezone [-show   --help]</b>                                                                                                                                                                                                                                                                                                                                                       |
| <b>ntp</b>       | Configure and start the NTP polling client.                                          | <b>ntp &lt;MD5_secret&gt;</b><br><b>&lt;interval&gt; &lt;server1&gt;</b><br><b>[&lt;server2&gt; [&lt;server3&gt;]]</b><br>and<br><b>ntp -n &lt;interval&gt;</b><br><b>&lt;server1&gt;</b><br><b>[&lt;server2&gt; [&lt;server3&gt;]]</b><br>... where <b>MD5_secret</b> is pre-shared secret to authenticate against the NTP server; use <b>-n</b> when authentication is not required. |
| <b>ntpstop</b>   | Stop polling the NTP server.                                                         | <b>ntpstop</b>                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ntpstart</b>  | Start polling the NTP server.                                                        | <b>ntpstart</b>                                                                                                                                                                                                                                                                                                                                                                        |

Table 2-77: Documentation Commands

## System Commands

| Command         | Use                                                                                                           | Syntax                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>audit</b>    | Display or edit commands entered in the Shell for a specific session. The audit is not kept between sessions. | <pre>audit setlines &lt;no. of lines&gt; audit show &lt;no. of lines&gt; audit clear &lt;no of lines&gt;</pre>                                                                                                                                                                                                                                         |
| <b>backup</b>   | Back up the system configuration.                                                                             | <pre>backup [-h] [-d] [-l] [--purge DAYS] [--sched [on hh:mm &lt;-m DayOfMonth&gt;   &lt;-w DaysOfWeek&gt;]   off] [[-tftp &lt;ServerIP&gt; [-path &lt;Path&gt;] [&lt;File- name&gt;]]   [--scp &lt;ServerIP&gt; &lt;User- name&gt; &lt;Password&gt; [-path &lt;Path&gt; &lt;Filename&gt;]]   [--file [-path &lt;Path&gt;] [&lt;File- name&gt;]]</pre> |
| <b>reboot</b>   | Restart the system.                                                                                           | <b>reboot</b>                                                                                                                                                                                                                                                                                                                                          |
| <b>patch</b>    | Apply an upgrade or Hotfix file.                                                                              | <pre>patch add scp &lt;ip_address&gt; &lt;patch_name&gt; [password(in expert mode)] patch add tftp &lt;ip_address&gt; &lt;patch_name&gt; patch add cd &lt;patch_name&gt; patch add &lt;full_patch_path&gt; patch log</pre>                                                                                                                             |
| <b>shutdown</b> | Shut down the system.                                                                                         | <b>shutdown</b>                                                                                                                                                                                                                                                                                                                                        |

Table 2-78: System Commands

| Command    | Use                                           | Syntax     |
|------------|-----------------------------------------------|------------|
| <b>ver</b> | Display the Secure-Platform system's version. | <b>ver</b> |

Table 2-78: System Commands

## Snapshot-Image Management

Commands to take a snapshot of the entire system and to restore the system from a snapshot are available. The system can be restored at any time, and at boot time the user 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 a TFTP or SCP server to store snapshots. Alternatively, snapshots can be stored locally.



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 a SmartCenter Server, log server, Check Point Provider-1, etc.

| Command       | Use                                                                                                                                                                                                | Syntax                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>revert</b> | Reboot the system from a snapshot file. The <b>revert</b> command, run by itself without any additional flags, will use default backup settings, and will reboot the system from a local snapshot. | <b>revert</b> [-h] [-d] [[--tftp <ServerIP> <Filename>]   --scp <ServerIP> <Username> <Password> <Filename>]   [--file <Filename>]] |

Table 2-79: snapshot and revert Commands

| Command         | Use                                                                                                                                                                               | Syntax                                                                                                                                                      |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>snapshot</b> | This command creates a snapshot file. The <b>snapshot</b> command, run by itself without any additional flags, will use default backup settings and will create a local snapshot. | <b>snapshot</b> [-h] [-d]Z<br>[[--tftp <ServerIP><br><Filename>]   [--scp<br><ServerIP> <Username><br><Password> <File-<br>name>]   [--file<br><Filename>]] |

Table 2-79: snapshot and revert Commands

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

## System-Diagnostic Commands

| Command     | Use                                                                                                                                                                    | Syntax                                                                                                                                                                                   |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>diag</b> | Display or send the system's diagnostic information ( <b>diag</b> files).                                                                                              | <b>diag</b> <log_file_name><br><b>tftp</b><br><tftp_host_ip_addresses>                                                                                                                   |
| <b>log</b>  | Show the list of available log files, apply log-rotation parameters, show the index of the log file in the list, and select the number of lines of the log to display. | <b>log --help</b><br><b>log list</b><br><b>log limit</b><br><log-index><br><max-size><backlog-copies><br><b>log unlimited</b><br><log-index><br><b>log show</b> <log-index><br>[<lines>] |

Table 2-80: System-Diagnostic Commands

| Command    | Use                                                                                                                                    | Syntax     |
|------------|----------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>top</b> | Display the top 15 processes on the system and periodically update this information. Raw CPU percentage is used to rank the processes. | <b>top</b> |

Table 2-80: System-Diagnostic Commands

## Check Point Commands

| Command        | Use                                                                                                                                                                                                                                                                                                                  | Syntax         |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <b>cpstart</b> | <b>cpstart</b> starts all Check Point applications running on a machine (other than <b>cprid</b> , which is invoked upon boot, and keeps on running independently). <b>cpstart</b> implicitly invokes <b>fwstart</b> (or any other installed Check Point product, such as <b>etmstart</b> , <b>uagstart</b> , etc.). | <b>cpstart</b> |
| <b>cpstop</b>  | <b>cpstop</b> stops all Check Point applications running on a machine (other than <b>cprid</b> , which is invoked upon boot and keeps on running independently). <b>cpstop</b> implicitly invokes <b>fwstop</b> (or any other installed Check Point product, such as <b>etmstop</b> , <b>uagstop</b> , etc.).        | <b>cpstop</b>  |

Table 2-81: Check Point Commands

| Command       | Use                                                                                                                                                                                                              | Syntax                                                                                                                                                                                                                                                                             |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>fw</b>     | <b>fw</b> provides a series of commands and tools for the Administrator to pass commands to the VPN-1 kernel that are not necessarily accessible via the GUI, i.e., <b>fw monitor</b> or <b>fw unloadlocal</b> . | <pre>fw ver [-h] fw kill [-t sig_no] procname fw putkey fw sam fw sam_policy fw fetch targets fw tab [-h] fw monitor [-h] fw ctl [args] fw lichosts fw log [-h] fw logswitch [-h target] [+ -] [oldlog] fw repairlog ... fw mergefiles fw lslogs fw fetchlogs fw unloadlocal</pre> |
| <b>cpinfo</b> | Show Check Point diagnostic information.                                                                                                                                                                         | <b>cpinfo</b> [[-v]   [-o filename]]                                                                                                                                                                                                                                               |
| <b>cpstat</b> | Display, in various formats, the status of Check Point applications on a local or nonlocal machine.                                                                                                              | <b>cpstat</b> [-h host] [-p port] [-f flavour] [-d] application_flag                                                                                                                                                                                                               |
| <b>cplic</b>  | Show, add, or remove Check Point licenses.                                                                                                                                                                       | <b>cplic</b> [put   del   print   check ]                                                                                                                                                                                                                                          |

Table 2-81: Check Point Commands

| Command                   | Use                                  | Syntax                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>cpshared_ver</code> | Show the SVN Foundation's version.   | <code>cpshared_ver</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>fwm</code>          | Execute SmartCenter Server commands. | <pre> fwm ver [-h] ... tar- gets fwm unload [opts] tar- gets fwm dbload [targets] fwm logexport [-h] ... fwm gen [-RouterType [-import]] rule-base fwm dbexport [-h] ... fwm ikencrypt &lt;key&gt; &lt;password&gt; fwm ver [-h] ... fwm load [opts] [fil- ter-file rule-base] targets fwm unload [opts] tar- gets fwm dbload [targets] fwm logexport [-h] ... fwm gen [-RouterType [-import]] rule-base fwm dbexport [-h] ... fwm ikencrypt &lt;key&gt; &lt;password&gt; fwm dbimport [-h] ... </pre> |

Table 2-81: Check Point Commands

## Network-Diagnostic Commands

| Command           | Use                                                                                                                                                                                                                                                                                                    | Syntax                                                                                                                                                                                     |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ping</b>       | Send <b>ICMP ECHO_REQUEST</b> packets to network hosts.                                                                                                                                                                                                                                                | <code>ping [-dfnqrVrR] [-c count] [-i wait] [-l preload] [-p pattern] [-s packetsize]</code>                                                                                               |
| <b>traceroute</b> | Tracking the route a packet follows (or finding the Gateway that is discarding your packets) can be difficult. <b>traceroute</b> utilizes the IP protocol <b>time to live</b> field and attempts to elicit an <b>ICMP TIME_EXCEEDED</b> response from each Gateway along the path to a designated host | <code>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 ]</code> |
| <b>netstat</b>    | Show network statistics.                                                                                                                                                                                                                                                                               | <code>netstat [-veenNcCF] [&lt;Af&gt;] -r<br/>netstat {-V --version -h --help}<br/>netstat [-vnNcaeol] [&lt;Socket&gt; ...]<br/>netstat { [-veenNac] -i   [-cnNe] -M   -s }</code>         |

Table 2-82: Network-Diagnostic Commands

## Network-Configuration Commands

| Command       | Use                                                                                                                                                                                                                             | Syntax                                                                                                                                                                                                                                                                                                                |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>arp</b>    | Manipulate 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. | <pre>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]</pre> |
| <b>addarp</b> | Add a persistent ARP entry (one that will survive reboot).                                                                                                                                                                      | <pre>addarp &lt;hostname&gt; &lt;hwaddr&gt;</pre>                                                                                                                                                                                                                                                                     |
| <b>delarp</b> | Remove ARP entries created by <b>addarp</b> .                                                                                                                                                                                   | <pre>delarp &lt;hostname&gt; &lt;MAC&gt;</pre>                                                                                                                                                                                                                                                                        |
| <b>hosts</b>  | Show, set, or remove host-name-to-IP-address mappings.                                                                                                                                                                          | <pre>hosts add &lt;IP-ADDRESS&gt; &lt;host1&gt; [&lt;host2&gt; ...] hosts remove &lt;IP_ADDRESS&gt; &lt;host1&gt; [&lt;host2&gt; ...] hosts</pre>                                                                                                                                                                     |

Table 2-83: Network-Configuration Commands

| Command         | Use                                                   | Syntax                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ifconfig</b> | Show, configure, or store network-interface settings. | <pre> ifconfig [-a] [-i] [-v] [-s] &lt;interface&gt; [[&lt;AF&gt;] &lt;address&gt;] [add &lt;address&gt;[/&lt;prefixlen&gt;]] [del &lt;address&gt;[/&lt;prefixlen&gt;]] [[-]broadcast [&lt;address&gt;]] [[-]pointpoint [&lt;address&gt;]] [netmask &lt;address&gt;] [dstaddr &lt;address&gt;] [tunnel &lt;address&gt;] [outfill &lt;NN&gt;] [keepalive &lt;NN&gt;] [hw &lt;HW&gt; &lt;address&gt;] [metric &lt;NN&gt;] [mtu &lt;NN&gt;] [[-]trailers] [[-]arp] [[-]allmulti] [multicast] [[-]promisc] [mem_start &lt;NN&gt;] [io_addr &lt;NN&gt;] [irq &lt;NN&gt;] [media &lt;type&gt;] [txqueuelen &lt;NN&gt;] [[-]dynamic] [up down] [--save] </pre> |
| <b>vconfig</b>  | Configure VLAN interfaces.                            | <pre> vconfig add [interface-name] [vlan_id] vconfig rem [vlan-name] </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 2-83: Network-Configuration Commands

| Command            | Use                                                                                       | Syntax                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>route</b>       | Show, configure, or save routing entries.                                                 | <pre>route [-nNvee] [-FC] [&lt;AF&gt;] List kernel routing tables  route [-v] [-FC] {add del flush} ... Modify routing table for AF.  route {-h --help} [&lt;AF&gt;] Detailed usage syntax for specified AF.  route {-V --version} Display version/ author and exit.  route --save</pre> |
| <b>hostname</b>    | Show or set the system's hostname.                                                        | <pre>hostname [--help] hostname &lt;host&gt; hostname &lt;host&gt; &lt;external_ip_address&gt;</pre>                                                                                                                                                                                     |
| <b>domain-name</b> | Show or set the system's domain name.                                                     | <pre>domainname [&lt;domain&gt;]</pre>                                                                                                                                                                                                                                                   |
| <b>dns</b>         | Add, remove, or show the Domain Name Servers.                                             | <pre>dns [add del &lt;ip_of_nameserver&gt;]</pre>                                                                                                                                                                                                                                        |
| <b>webui</b>       | Configure the port the SecurePlatform HTTPS Web server uses for the management interface. | <pre>webui enable [https_port] webui disable</pre>                                                                                                                                                                                                                                       |

Table 2-83: Network-Configuration Commands

## User and Administrative Commands

| Command               | Use                                                                                                            | Syntax                                                                                                |
|-----------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>adduser</b>        | Add a SecurePlatform Administrator (supports RADIUS authentication for Administrators).                        | <b>adduser</b> [-x<br><b>EXTERNAL_AUTH</b> ]<br><user name>                                           |
| <b>deluser</b>        | Delete a SecurePlatform Administrator.                                                                         | <b>deluser</b> <user name>                                                                            |
| <b>showusers</b>      | Display all SecurePlatform Administrators.                                                                     | <b>showusers</b>                                                                                      |
| <b>lockout</b>        | Lock out a SecurePlatform Administrator.                                                                       | <b>lockout enable</b><br><attempts><br><lock_period><br><b>lockout disable</b><br><b>lockout show</b> |
| <b>unlockuser</b>     | Unlock a locked Administrator.                                                                                 | <b>unlockuser</b><br><username>                                                                       |
| <b>checkuser-lock</b> | Display the lockout status of a SecurePlatform Administrator (whether or not the Administrator is locked out). | <b>checkuserlock</b><br><username>                                                                    |

Table 2-84: User and Administrative Commands

COPY