# Gaia WebUI and clish

## Administration Guide

### Early Availability

DRAFT

9 November 2011

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

© 2011 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

DRAFT

# Important Information

## Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

## Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=TBD

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the home page at the Check Point Support Center (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doShowproductpage&productTab=overview&product=TBD).

IF THE RELEASE HAS A HOME PAGE,

1. Copy the above line to just above the Revision History (use Body Text style).

2. Drag the predefined home page link object in **TechPub > Network Security > Common Content** onto the last few words of the line.

## Revision History

| Date | Description |
|---|---|
| 9 November 2011 | First release of this document |

## Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Gaia WebUI and clish Administration Guide).

DRAFT

# Contents

DRAFT

DRAFT

DRAFT

DRAFT

# Chapter 1

## Gaia Overview

Gaia is Check Point's advanced operating system for security applications that includes features and functionality from IPSO and SecurePlatform, in addition to many new enhancements. Gaia supports all Check Point appliances and open servers.

Gaiais a "hardened" operating system that prevents unauthorized access to many services and subsystems.

Gaia is designed from the ground up for modern, high-end deployments, with support for:

- IPv4 and IPv6
- 64 bit platforms
- High connection capacity
- Virtualization
- Superior high availability and load sharing (ClusterXL, VRRP, Interface Bonding)
- Dynamic routing and multicast environments (BGP, OSPF, RIP, PIM, IGMP)
- Software and hardware acceleration

Gaia includes state-of-the-art management features and operational efficiencies, such as:

- Centralized management
- Web-based GUI for nearly all system configuration and management tasks.
- Enhanced command line interface gives unmatched usability, including IPSO and SecurePlatform functionality
- Role-based administration for granular access permission
- Full logging and audit trail for all <t_ggui> and CLI actions

We recommend that you read this document carefully before using Gaia.

DRAFT

# Chapter 2

# Introduction to the WebUI

In This Chapter

## Obtaining a Configuration Lock

Only one user can have Read/Write access for Gaia configuration settings at a time. Other users can have read-only access to view configuration settings according to their permissions.

When you log in to the WebUI or the CLI when no other user is logged in, you get an exclusive configuration lock. If another CLI or WebUI session already has a configuration lock, you must remove it before you can make any changes. If you do not remove the configuration lock, you can use to WebUI or CLI with Read Only permissions.

The WebUI shows a message when another user has a configuration lock. You cannot change WebUI page configuration settings unless you first remove the configuration lock.

### Logging out

You must log out of your WebUI or CLI session before you close the browser or terminal window. This is because the configuration lock stays in effect even when you close the browser or terminal window. The lock remains if effect until another user removes the lock or the defined inactivity time-out period (default = 10 minutes) expires.

### To remove a configuration lock:

- Click the lock icon above the toolbar.
  or
- On a configuration settings page, click the **Click here to obtain lock** link.

**Note -** Only users with read/write access privileges can override a configuration lock or log in with read/write privileges.

DRAFT

# Toolbar Accessories

# The Overview Page

## Widgets

### *The System Overview Widget*

### *The Memory Monitor Widget*

### *The CPU Monitor Widget*

### *Downloading SmartConsole*

# The Configuration Tab

# The Monitoring Tab

# Using the Search Tool

DRAFT

Chapter 3

# Introduction to the Command Line Interface

This chapter gives an introduction to the Gaia command line interface (CLI).

The default shell of the CLI is called `clish`.

**To use the CLI:**

1. Connect to the platform using a command-line connection (SSH or a console) over a TCP/IP network.
2. Log on using a user name and password.
   Immediately after installation, the default user name and password, are `admin` and `admin`.

In This Chapter

DRAFT

## Saving Configuration Changes

Configuration changes you enter using the CLI are applied immediately to the running system. To ensure that these changes remain after you reboot, that is, to save your changes permanently, run `save config` at the CLI prompt.

## Commands and Features

Gaia commands are organized into features. A feature is a group of related commands.

Commands have the syntax

```
Operation feature parameter
```

The most common operations are `show`, `add`, `set`, `delete`

| The 4 main operations | Description |
|---|---|
| `set` | Sets a value in the system. |
| `show` | Shows a value or values from the system. |
| `delete` | Deletes a value from the system. |

| The 4 main operations | Description |
|---|---|
| `add` | Adds a new value to the system. |

| Other operations | Description |
|---|---|
| `save` | Saves the configuration changes made since the last save. |
| `reboot` | Reboot the system. |
| `halt` | Halts the system. |
| `quit` | Exits from the CLI. |
| `exit` | Exits from the shell. |
| `Start` | Starts a transaction. Puts the CLI into transaction mode. All changes made using commands in transaction mode are applied at once or none of the changes are applied based on the way transaction mode is terminated. |
| `commit` | Ends transaction by committing changes. |
| `rollback` | Ends transaction by discarding changes. |
| `expert` | Enter the expert shell. Allows low-level access to the system, including the file system. |
| `ver` | Shows the version of the active Gaia image |
| `revert` | Revert the database |

| To do this | Type |
|---|---|
| Show a list of all features | `show commands feature <TAB>` |
| Shows all commands that the user has permissions to run | `show commands` |
| Shows all commands for a specific feature | `show commands feature VALUE`<br>For example<br>`Gaia> show commands feature arp`<br>`add arp static ipv4-address VALUE macaddress VALUE`<br>`delete arp dynamic all`<br>`delete arp static ipv4-address VALUE`<br>`set arp table cache-size VALUE`<br>`set arp table validity-timeout VALUE`<br>`show arp dynamic all`<br>`show arp static all`<br>`show arp table cache-size`<br>`show arp table validity-timeout` |

DRAFT

| Other operations | Description |
|---|---|
| Show all the possible operations | `show commands op <SPACE> <TAB>`<br>For example<br>`Gaia> show commands op`<br><br>`save      reboot    halt      set       show      delete    add`<br>`load      start     help      history   quit      exit`<br>`commit`<br>`rollback  expert    ver       revert`<br>`Gaia> show commands op` |
| Show all commands per operation, per feature | `show commands [op VALUE] [feature VALUE]`<br>For example<br>`Gaia> show commands op show feature arp`<br>`show arp dynamic all`<br>`show arp static all`<br>`show arp table cache-size`<br>`show arp table validity-timeout`<br>`Gaia>` |

### At the `--More--` prompt:

| To do this... | Type |
|---|---|
| To see the next page. | <SPACE> |
| To see the next line. | <ENTER> |
| To exit to the CLI prompt | <Q> or <q> |

# Command Completion

You can automatically complete a command. This saves time, and can also help if you are not sure what to type next.

| Press ... | To do this... |
|---|---|
| <TAB> | Complete or fetch the keyword. For example<br>`Gaia> set in<TAB>`<br>`inactivity-timeout - Set inactivity timeout`<br>`interface          - Displays the interface related parameters`<br>`Gaia> set in` |
| <SPACE> <TAB> | Show the arguments that the command for that feature accepts. For example:<br>`Gaia> set interface <SPACE> <TAB>`<br>`eth0 eth1 lo`<br>`Gaia> set interface` |

DRAFT

| Press ... | To do this... |
|---|---|
| <ESC><ESC> | See possible command completions. For example<br>`Gaia> set inter<ESC><ESC>`<br>`set interface VALUE ipv4-address VALUE mask-length VALUE`<br>`set interface VALUE ipv4-address VALUE subnet-mask VALUE`<br>`set interface VALUE ipv6-address VALUE mask-length VALUE`<br>`set interface VALUE { comments VALUE mac-addr VALUE mtu VALUE`<br>`state VALUE speed VALUE duplex VALUE auto-negotiation VALUE }`<br>`set interface VALUE { ipv6-autoconfig VALUE }`<br>`Gaia> set inter` |
| ? | Get help on a feature or keyword. For example<br>`Gaia> set interface <?>`<br>`interface: {show/add/delete} interface "interface-name"`<br>`Gaia> set interface` |
| UP/DOWN arrow | Browse the command history |
| LEFT/RIGHT arrow | Edit command. |
| Enter | Run a command string. The cursor does not have to be at the end of the line.<br>You can usually abbreviate the command to the smallest number of unambiguous characters. |

# Command History

You can recall commands you have used before, even in previous sessions.

| Command | Description |
|---|---|
| ↓ | Recall previous command. |
| ↑ | Recall next command |
| history | Show the last 100 commands. |
| !! | Run the last command. |
| !nn | Run a specific previous command: The nn command. |
| !-nn | Run the nnth previous command. For example, entering !-3 runs the third from last command. |
| !str | Run the most recent command that starts with str. |
| !\?str\? | Run the most recent command containing str. The trailing ? may be omitted if str is followed immediately by a new line. |
| !!:s/str1/str2 | Repeat the last command, replacing str1 with str2 |

# Reusing Parts of Commands

You can combine word designators with history commands to refer to specific words used in previous commands. Words are numbered from the beginning of the line with the first word being denoted by `0`. Use a colon to separate a history command from a word designator. For example, you could enter `!!:1` to refer to the first argument in the previous command. In the command `show interfaces`, `interfaces` is word 1.

DRAFT

| Word Designator | Meaning |
|---|---|
| 0 | The operation word. |
| `n` | The `n`th word. |
| `^` | The first argument; that is, word 1. |
| `$` | The last argument. |
| `%` | The word matched by the most recent `\?str\?` search. |

Immediately after word designators, you can add a sequence of one or more of the following modifiers, each preceded by a colon:

| Modifier | Meaning |
|---|---|
| `p` | Print the new command but do not execute |
| `s/str1/str2` | Substitute `new` for the first occurence of old in the word being referred to. |
| `g` | Apply changes over the entire command. Use this modified in conjunction with `s`, as in `gs/str1/str2`. |

# Command Line Movement and Editing

You can back up in a command you are typing to correct a mistake. To edit a command, use the left and right arrow keys to move around and the Backspace key to delete characters. You can enter commands that span more than one line.

These are the keystroke combinations you can use:

| Keystroke combination | Meaning |
|---|---|
| Alt-D | Delete next word. |
| Alt-F | Go to the next word. |
| Ctrl-Alt-H | Delete the previous word. |
| Ctrl-shift_ | Repeat the previous word. |
| Ctrl-A | Move to the beginning of the line. |
| Ctrl-B | Move to the previous character. |
| Ctrl-E | Move to the end of the line. |
| Ctrl-F | Move to the next character. |
| Ctrl-H | Delete the previous character. |
| Ctrl-L | Clear the screen and show the current line at the top of the screen. |
| Ctrl-N | Next history item. |
| Ctrl-P | Previous history item. |
| Ctrl-R | Redisplay the current line. |
| Ctrl-U | Delete the current line. |

DRAFT

# Obtaining a Configuration Lock

When you use the CLI Only one user can have Read/Write access for Gaia configuration settings at a time. Other users can have read-only access to view configuration settings according to their permissions.

When you log in to the WebUI or the CLI when no other user is logged in, you get an exclusive configuration lock. If another CLI or WebUI session already has a configuration lock, you must remove it before you can make any changes. If you do not remove the configuration lock, you can use to WebUI or CLI with Read Only permissions.a message appears. You can run show commands, but you cannot change any settings unless you override the configuration lock.

Only users with read/write privileges can log in with a configuration lock.

Use the following commands temporarily restrict the ability of other admin users to make configuration changes. This feature allows you to lock out other users for a specified period of time while you make configuration changes.

**Syntax**

```
set config-lock off
set config-lock on [timeout VALUE override]
show config-lock
show config-state
```

**Parameters**

| Parameter | Description |
|---|---|
| `<on \|off>` | Controls the behavior when logging in to clish.<br>Off - Disable exclusive access.<br>On - Enable exclusive access. Clish<br>When you enable config-lock, the default timeout value is 300 seconds. |
| `on timeout` | Enable config-lock for the specified interval in seconds (5-900). |
| `on override` | Override an existing configuration lock and disable it. |

# Environment Commands

**Description** Use these commands to set the CLI environment for a user for a particular session, or permanently.

DRAFT

**Syntax**

To show the client environment

```
show clienv all
show clienv config-lock
show clienv debug
show clienv echo-cmd
show clienv on-failure
show clienv output
show clienv prompt
show clienv rows
show clienv syntax-check
```

To set the client environment

```
set clienv config-lock VALUE
set clienv debug VALUE
set clienv echo-cmd VALUE
set clienv on-failure VALUE
set clienv output VALUE
set clienv prompt VALUE
set clienv rows VALUE
set clienv syntax-check VALUE
```

To save the client environment permanently

```
save clienv
```

DRAFT

**Parameters**

| Parameter | Description |
|---|---|
| `all` | Show all the client environment settings. |
| `config-lock <On \| Off >` | The default value of the config-lock parameter. If it is set to 'on'; clish will acquire config-lock when invoked otherwise continue without a config-lock.<br>The value can be 'on' or 'off'.<br>Clarify this |
| `debug <0-6>` | The debug level. Level 0 (lowest) to level 6 (highest). Predefined levels are:<br>0 Do not do debugging. Display error messages only.<br>5 Show confd requests, responses.<br>6 Show handler invocation parameters, results. |
| `ech-cmd <On \| Off >` | Echo all commands. When using the load commands command, all commands are echoed before being executed.<br>Default: off |
| `on-failure <stop \| continue>` | • Continue - continue running commands from a file or a script and only display error messages.<br>• Stop - stop running commands from a file or a script when the system encounters an error.<br>Default: stop |
| `output <pretty \|structured \| xml>` | The command line output format ("Client Environment Output Format" on page 19).<br>Default: pretty |
| `prompt VALUE` | The appearance of the command prompt. To set the prompt back to the default, use the keyword default. Any printable character is allowed, as well as combinations of the following variables:<br>%H : Replaced with the Command number.<br>%I : Replaced with the User ID.<br>%M : Replaced with the Hostname.<br>%P : Replaced with the Product ID.<br>%U : Replaced with the User Name. |
| `rows integer` | The number of rows to show on your console or xterm. If the window size is changed the value will also change, unless the value set is to 0 (zero). |
| `syntax-check <On \| Off >` | Put the shell into syntax-check mode. Commands you enter are checked syntactically and are not executed, but values are validated.<br>Default: off |
| `save clienv` | Permanently save the environment variables that were modified using the set clienv commands. |

# Client Environment Output Format

**Description** The CLI supports three output formats: pretty, structured, and xml.

**Syntax** To show the output format

```
show clienv output VALUE
```

To set the output format

```
set clienv output VALUE
```

**Parameters**

| Parameter | Description |
|---|---|
| `pretty` | Output is formatted to be clear. For example<br>`Gaia> set clienv output pretty`<br>`Gaia> show user admin`<br>`Uid     Gid     Home Dir.      Shell          Real`<br>`Name`<br>`0       0       /home/admin    /etc/cli.sh    n/a` |
| `Structured` | Output is delimited by semi-colons. For example<br>`Gaia> set clienv output structured`<br>`Gaia> show user admin`<br>`Uid;Gid;Home Dir.;Shell;Real Name;`<br>`0;0;/home/admin;/etc/cli.sh;;` |
| `xml` | Adds XML tags to the output. For example<br>`Gaia> set clienv output xml`<br>`Gaia> show user admin`<br>`<?xml version="1.0"?>`<br>`<CMDRESPONSE>`<br>`<CMDTEXT>show user admin</CMDTEXT>`<br>`<RESPONSE><System_User>`<br>`<Row>`<br>`<Uid>0</Uid>`<br>`<Gid>0</Gid>`<br>`<Home_Dir.>/home/admin</Home_Dir.>`<br>`<Shell>/etc/cli.sh</Shell>`<br>`<Real_Name></Real_Name>`<br>`</Row>`<br>`</System_User>`<br>`</RESPONSE>`<br>`</CMDRESPONSE>` |

# Expert Mode

The default shell of the CLI is called `clish`. Clish contains a limited set of commands . It does not allow access to low level system functions.

For low level configuration, use the more permissive `expert` shell.

To use the expert shell, run

```
expert
```

To exit the expert shell and return to clish, run

```
exit
```

# User Defined (Extended) Commands

**Description**

Manage user defined (extended) commands in clish. Extended commands include:

1. Built in extended commands. These are mostly for configuration and troubleshooting of Gaia and Check Point products.
2. User defined commands.

You can do role based administration (RBA) with extended commands by assigning extended commands to roles and then assigning the roles to users or user groups.

**Syntax**

To show all extended commands

```
show extended commands
```

To show the path and description of a specified extended command

```
show command VALUE
```

To add an extended command

```
add command VALUE path VALUE description VALUE
```

To delete an extended command

```
delete command VALUE
```

**Parameters**

| Parameter | Description |
|---|---|
| `command` | Name of the extended command |
| `path` | Path of the extended command |
| `description` | Description of the extended command |

**Example**

To add the `free` command to the systemDiagnosis role and assign a user with that role:

1. To add the free command, run
   ```
   add command free path /usr/bin/free description "Display
   amount of free and used memory in the system"
   ```
2. Save the configuration. Run
   ```
   save config
   ```
3. Log out of Gaia and log in again.
4. To add the free command to the systemDiagnosis role, run
   ```
   add rba role systemDiagnosis domain-type System readwrite-
   features ext_free
   ```
5. To assign user john with the systemDiagnosis role, run
   ```
   add rba user john roles systemDiagnosis
   ```

DRAFT

# Chapter 4

# System Overview

This chapter describes the **System Overview** page of the <tp_gui>, and the commands that you can use to get the same information at the CLI.

In This Chapter

# Showing System Overview Information- WebUI

The WebUI **Overview** page shows the following **System Overview** information:

- **Product** - The name of the installed product. Usually, Gaia.
- **Kernel** - The OS kernel build number.
- **Edition** - The OS edition. either 32-bit or 64-bit.
- **Build Number** - The OS build number
- **System Uptime** - Show how long the sytem has been running
- **Platform** - The hardware platform

# Showing System Overview Information - clish (uptime, version)

## Uptime

| **<name>** | |
|---|---|
| **Description** | Show how long the sytem has been running |
| **Syntax** | `show uptime` |
| **Parameters** | None |

## Version

| **<name>** | |
|---|---|
| **Description** | Show the name and versions of the OS components |

DRAFT

**<name>**

**Description** Show the name and versions of the OS components

**Syntax** To show the full system version information

```
show version all
```

To show version information for OS components

```
show version os build
show version os edition
show version os kernel
```

To show name of the installed product

```
show version product
```

**Parameters**

| Parameter | Description |
|---|---|
| all | All system information |
| os build | The OS build number |
| os edition | The OS edition. either 32-bit or 64-bit. |
| os kernel | The OS kernel build number. |
| product | The name of the installed product. Usually, Gaia. |

DRAFT

# Chapter 5

# Interface Management

Placeholder

In This Chapter

## Network Interfaces

Gaia supports these network interface types:

- Ethernet physical interfaces.
- Alias (Secondary IP address on an Ethernet interface).
- VLAN
- Bond
- Bridge
- Loopback

Move somewhere appropriate:

**Note** - If you make changes to IP addresses or delete interfaces, the firewall sometimes does not learn of the changes when you get the topology. If you get the topology and your changes to interfaces are not shown, stop and restart the firewall.

### Configuring Interface Link States- WebUI

The configuration and status of interface are shown in the **Interface Management > Interfaces** page.

Interfaces can be changed while they are offline. The interface status indicators are:

| Link Status | Description |
|---|---|
| Grey (Down) | The physical interface is disabled (Down). To enable the interface:<br>1. Select the interface<br>2. Click **Edit**<br>3. Click **Enable** |
| Red (no Link) | The physical interface is enabled, but the device does not detect a connection to the network. |
| Green (Up) | The physical interface is ready for use. It is enabled (Up) and connected to the network. |

DRAFT

# Ethernet Interfaces

You cannot do a hot swap of Network Interface Cards (NICs) when using Gaia. To add or remove a NIC so that it is recognized by Gaia:

1. Turn off the computer.
2. Add, remove or replace NICs.
3. Restart the computer.

## Configuration using the WebUI

## Configuration using the CLI

### Description

### Syntax

```
show interfaces all
gaia117> show commands feature interface
Add Commands:
add interface VALUE 6in4 VALUE remote VALUE ttl
VALUE
add interface VALUE 6to4 VALUE ttl VALUE
add interface VALUE alias VALUE
add interface VALUE loopback VALUE
add interface VALUE vlan VALUE
Delete commands:
delete interface VALUE 6in4 VALUE
delete interface VALUE 6to4 VALUE
delete interface VALUE alias VALUE
delete interface VALUE ipv4-address
delete interface VALUE ipv6-address
delete interface VALUE loopback VALUE
delete interface VALUE vlan VALUE
Set commands:
set interface VALUE ipv4-address VALUE mask-length
VALUE
set interface VALUE ipv4-address VALUE subnet-mask
VALUE
set interface VALUE ipv6-address VALUE mask-length
VALUE
set interface VALUE { comments VALUE mac-addr VALUE
mtu VALUE state VALUE speed VALUE duplex VALUE auto-
negotiation VALUE }
set interface VALUE { ipv6-autoconfig VALUE }
Show Commands:
show interface VALUE 6in4s
show interface VALUE 6to4s
show interface VALUE alias VALUE
show interface VALUE aliases
show interface VALUE all
show interface VALUE all
show interface VALUE ipv4-address
show interface VALUE ipv6-address
show interface VALUE loopback VALUE
show interface VALUE loopbacks
show interface VALUE vlans
show interface VALUE { comments mac-addr mtu state
speed duplex auto-negotiation type }
show interface VALUE { ipv6-autoconfig }
```

### Parameters

| Parameter | Description |
|---|---|
| | |

DRAFT

**Description**

**Return Value**

**Example**

**Output**

**Comments**

# VLAN Interfaces

DRAFT

### VLAN Highlights

Check Point security devices support virtual LAN (VLAN) interfaces on supported Ethernet interfaces. VLAN interfaces let you configure subnets with a secure private link to gateways and management servers using your existing topology. With VLAN interfaces, you can multiplex Ethernet traffic into many channels using one cable.

### How VLANs Work

The Check Point VLAN implementation lets you add a logical subnet using a VLAN ID to a physical interface. A VLAN interface adds four bytes to the packet header, for a total of 18 bytes. Incoming VLAN traffic is examined for the presence of VLAN header. If there is a VLAN header, it sends the traffic if a to the applicable VLAN subnet. If there is no VLAN header, Traffic goes to the channel 0 (untagged) interface. In the Check Point implementation, untagged, channel-0 traffic sent to a VLAN is dropped.

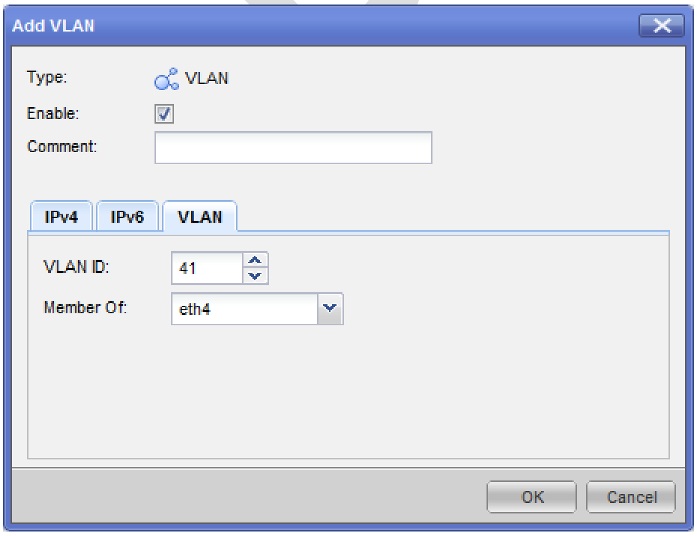
Outgoing traffic from a VLAN interface receives a VLAN header. Check Point devices can receive and generate fully compliant IEEE 802.1Q tags. The IEEE802.1Q standard defines the technology for virtual bridged networks. Check Point devices are interoperable as a router, but not as a switch.

This section shows you how to configure VLAN interfaces using the WebUI and the CLI.

## *Configuration Using the WebUI*

### To configure a VLAN interface using the WebUI:

1. In the WebUI navigation tree, select **Network Interfaces**.
2. Select the **Enable** option to activate the VLAN interface.
3. Click **Add** > **VLAN**. For an existing VLAN interface, select the interface and then click **Edit**.
4. In the **Add** (or **Edit**) **VLAN** window **IPv4** and **IPv6** tabs, enter the IP addresses and subnet information as necessary. You can optionally select the **Obtain IP Address automatically** option.
5. On the **VLAN** tab, enter or select a **VLAN ID** (VLAN tag) between 2 and 4094.



Add VLAN

Type: VLAN

Enable: ☑

Comment:

IPv4 | IPv6 | VLAN

VLAN ID: 41

Member Of: eth4

6. In the **Member Of** field, select the physical interface related to this VLAN.

**Note** - You cannot change the VLAN ID or physical interface for an existing VLAN interface. To change these parameters, delete the VLAN interface and then create a New VLAN interface.

## *Configuration Using the CLI*

### To configure a VLAN interface using the command line:

1. If you are adding a new VLAN interface:
   Run `add interface <IF Name> vlan <VLAN ID>`
   - **IF Name** - Physical interface associated with this VLAN
   - **VLAN ID** - VLAN ID (VLAN tag)

   Example:

   ```
   add interface eth1 vlan 10
   ```
2. Run this command to configure the additional parameters:

   ```
   set interface <IF Name>.<VLAN ID> ipv4-address <IPv4 Address> [ipv6-address
   <IPv6 Address>]
   ```
   - **IF Name** - Physical interface associated with this VLAN
   - **VLAN ID** - VLAN ID (VLAN tag)
   - **IPv4 Address** - Interface IPv4 address and the subnet in CIDR notation (xxx.xxx.xxx.xxx/xx)
   - I**Pv6-address** - Interface IPv6 address and the prefix (only if you are using IPv6)

   Example:

   ```
   set interface eth1.10 ipv4-address 172.30.1.1/24 ipv6-address
   2000:172:30::1/64
   ```

# Bridge Interfaces

### Bridge Mode Highlights

Check Point security devices support bridge interfaces that implement native, Layer-2 bridging. Configuring your device as a bridge lets network administrators deploy security devices in an existing topology without reconfiguring the existing IP routing scheme. This is an important advantage for large-scale, complex environments.

### How It Works

You configure Ethernet interfaces (including aggregated interfaces) on your Check Point security device to work like ports on a physical bridge. The interfaces then send traffic using Layer-2 addressing. You can configure some interfaces as bridge interfaces, while other interfaces on the same device work as layer-3 devices. Traffic between bridge interfaces is inspected at Layer-2. Traffic between two Layer-3 interfaces, or between a bridge interface and a Layer-3 interface is inspected at Layer-3.

This section shows you how to configure bridge interfaces using the WebUI and the CLI.

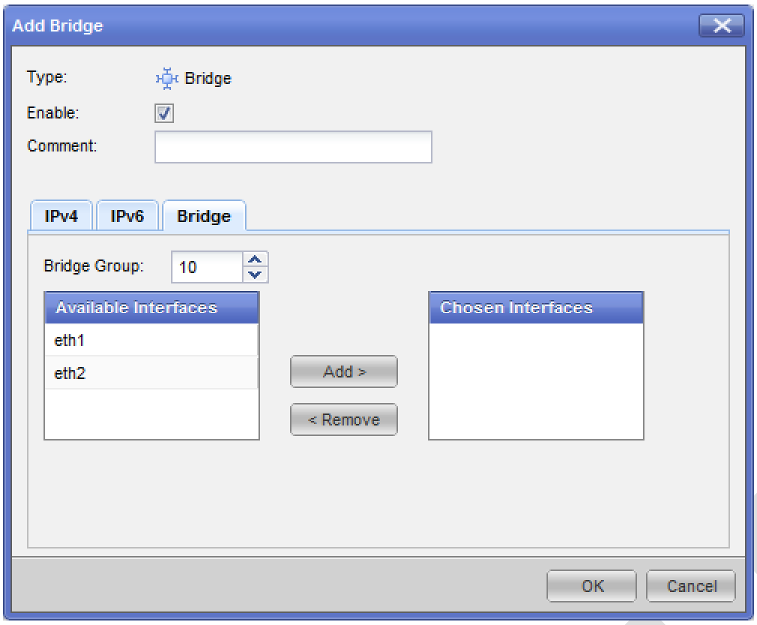
## *Configuration using the WebUI*

### To configure a bridge interface:

1. In the WebUI navigation tree, select **Network Interfaces**.
2. Select the **Enable** option to activate the bridge interface.
3. Click **Add** > **Bridge**. For an existing bridge interface, select the interface and then click **Edit**.
4. In the **Add** (or **Edit**) **Bridge** window **IPv4** and **IPv6** tabs, enter the IP addresses and subnet information as necessary. You can optionally select the **Obtain IP Address automatically** option.

DRAFT

5. On the **Bridge** tag, enter or select a **Bridge Group** ID between 1 and 1024.



Add Bridge

Type: Bridge

Enable: ☑

Comment:

Bridge Group: 10

Available Interfaces

eth1

eth2

Chosen Interfaces

6. On the **Bridge** tab, select the interfaces from the **Available Interfaces** list and then click **Add**.

## *Configuration using the CLI*

Bridge interfaces are known as **Bridging Groups** in Gaia CLI commands. You can optionally assign an IPv4 or IPv6 address to a bridge interface.

**To create a new bridge interface**:

Run:

```
add bridging group <Bridge IF> interface <IF>
```

- **Bridge IF** - Bridge interface name (unique integer between 0 and 1024)
- **IF** - Physical interface name

Run this command once for each physical interface included in the bridge interface.

### To delete a bridge interface:

1. Run:

   ```
   delete bridging group <Bridge IF> interface <IF>.
   ```

   This command deletes the physical interface. Run this command once for each physical interface included in the bridge interface.

2. Run:

   ```
   delete bridging group <Bridge IF>.
   ```

   This command deletes the bridge interface itself.

### To add or change a bridge interface IP address:

- For an IPv4 IP address, run

  ```
  set interface <Bridge IF> ipv4-address <IP> subnet-mask <Mask>.
  ```

- For an IPv6 IP address, run

  ```
  set interface <Bridge IF> ipv6-address <IP> mask-length <Prefix>.
  ```

  - **Bridge IF** - Bridge interface name
  - **IP** - IP address - IPv4 or IPv6 as required
  - **Mask** - IPv4 subnet mask in dotted decimal format.
  - **Prefix** - IPv6 prefix length

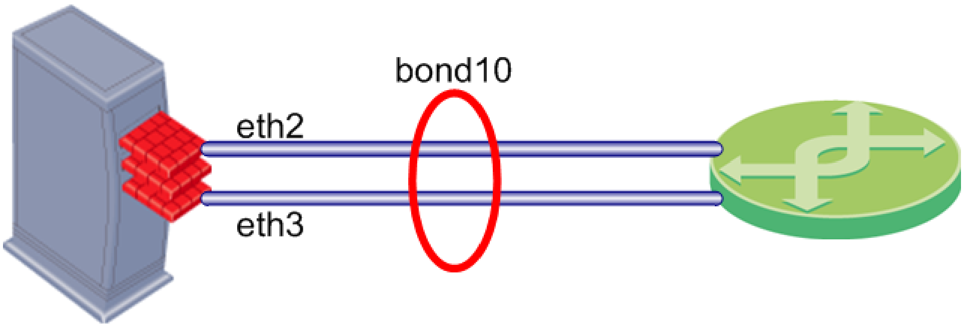
  Example:

  ```
  set interface 777 ipv6-address 3000:40::1 mask-length 64
  ```

DRAFT

# Link Aggregation

Check Point security devices support **Link Aggregation**, a technology that joins multiple physical interfaces into one virtual interface, known as a **bond interface**. The bond interface gives fault tolerance and increases throughput by sharing the load among many interfaces. Check Point devices support the IEEE 802.3ad Link Aggregation Control Protocol (LCAP) for dynamic link aggregation.



A **bond interface** (also known as a **bonding group** or **bond**) is identified by its **Bond ID** (for example: *bond1*) and is assigned an IP address. The physical interfaces included in the bond are called **slaves** and do not have IP addresses.

You can define bond interfaces using one of these functional  strategies:

- **High Availability (Active/Backup)**: Gives redundancy when there is an interface or link failure. This strategy also supports switch redundancy. You can configure High Availability to work one of in these modes:
  - **Round Robin** - Selects the active slave interface sequentially.
  - **Active/Backup** - If the active slave interface goes down, the connection automatically fails over to the primary slave interface. If the primary slave interface is not available, the connection fails over to a different slave.
- **Load Sharing (Active/Active)**: Slave interfaces are active simultaneously. Traffic is distributed among the slave interfaces to maximize throughput. Load Sharing does not support switch redundancy. You can configure load sharing using one of these modes:
  - **Round Robin** - Selects the active slave interface sequentially.
  - **802.3ad** - Dynamically uses active slaves to share the traffic load using the LACP protocol. This protocol enables full interface monitoring between the gateway and a switch.
  - **XOR** - Selects the algorithm for slave selection according to the TCP/IP layer.

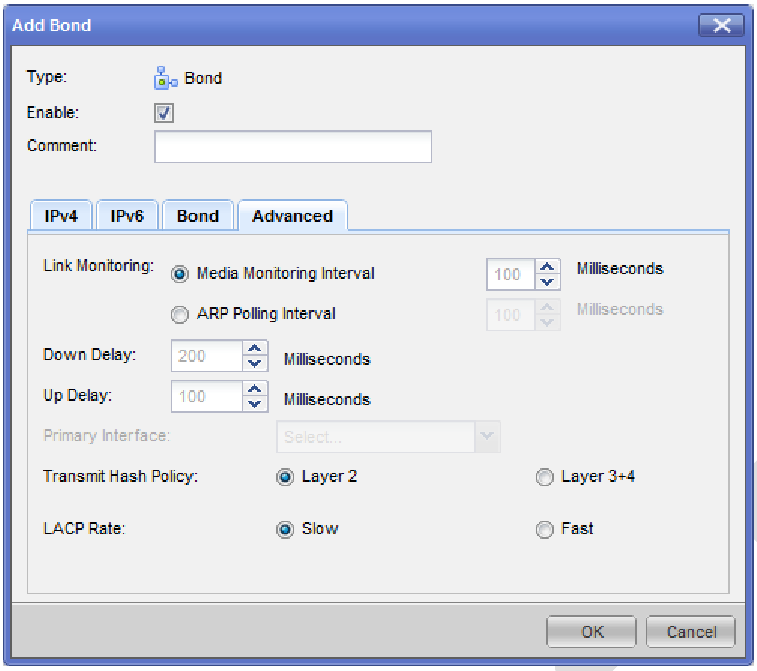
## *Configuring Bond Interfaces Using the WebUI*

### To configure a bond interface using the WebUI:

1. Make sure that the slave interfaces do not have IP addresses.
2. On the WebUI **Network Interfaces** page, click **Enable**.
3. For a new bond interface, select **Add** > **Bond**. For an existing Bond interface, double-click the bond interface**.**
4. Select the **Enable** option to activate the bond interface.
5. On the **Ipv4** and **IPv6** tabs (optional), enter the IP address information.
6. On the **Bond** tab, select or enter a **Bond Group** name. This parameter is an integer between 1 and 1024.
7. Select slave interfaces from the **Available Interfaces** list and then click **Add**.
8. Select an **Operation Mode** (**Round Robin** is the default).
9. On the **Advanced** tab, select a **Link Monitori**ng option and its frequency in milliseconds:
   - **Media Monitoring Interval** - This sets the frequency of requests sent to the Media Independent Interface (MMI) to confirm that a slave interface is up. The valid range is 1-5000 ms and the default is 100 ms.

DRAFT

- **ARP Monitoring** - This defines the frequency of ARP requests sent to confirm that a slave interface is up. ARP requests are sent to as many as five external MAC addresses.



Type: Bond

Enable: ☑

Comment:

Link Monitoring: ● Media Monitoring Interval 100 Milliseconds

○ ARP Polling Interval 100 Milliseconds

Down Delay: 200 Milliseconds

Up Delay: 100 Milliseconds

Primary Interface: Select...

Transmit Hash Policy: ● Layer 2 ○ Layer 3+4

LACP Rate: ● Slow ○ Fast

10. Select the **UP** and **Down** intervals in milliseconds. This parameter defines the waiting time, in milliseconds, to confirm the slave interface status before taking the specified action.
11. Select the **Primary Interface** (for Active/Backup bonds only).
12. Select the **Transmit Hash Policy** (XOR only). This parameter selects the algorithm for slave selection according to the specified TCP/IP layer.
13. Select the **LACP Rate**. This parameter sets the LACPDU packet transmission rate.

## *Configuring Bond intwerfaces Using the CLI*

When using the CLI, bond interfaces are known as **bonding groups**.

When using the CLI to create a bond interface, do these procedures in order:

1. Create the bond interface.
2. Define the slave interfaces and set them to the UP (on) State.
3. Define the bond operating mode.
4. Define other bond parameters as necessary.
5. Make sure that the bond interface is working correctly.

**Note** - Before running the CLI commands, make sure that the slave interfaces do not have an IP Address already assigned.

### Link Aggregation - CLI (bonding)

This section is a quick reference for link aggregation commands. The next sections include procedures for different tasks, including explanations of the configuration options.

**Description** Use these commands to configure link aggregation.

**Syntax**

```
add bonding group VALUE interface VALUE
delete bonding group VALUE interface VALUE
set bonding group VALUE interface
set bonding group VALUE primary VALUE
set bonding group VALUE mii-interval VALUE
set bonding group VALUE up-delay VALUE
set bonding group VALUE down-delay VALUE
set bonding group VALUE arp-polling-interval VALUE
set bonding group VALUE mode VALUE
set bonding group VALUE lacp-rate VALUE
set bonding group VALUE xmit-hash-policy VALUE
show bonding group VALUE show bonding groups
```

DRAFT

**Description** Use these commands to configure link aggregation.

**Parameters**

| Parameter | Description |
|---|---|
| `interface` | Name of slave interface |
| `primary` | Name of primary interface |
| `mii-interval` | Frequency that the system polls the Media Independent Interface (MMI) to get status |
| `up-delay`<br>`down-delay` | Waiting time to confirm the slave interface status before taking the specified action. |
| `arp-polling-interval` | Frequency of ARP requests sent to confirm a that slave interface is up |
| `mode` | Sets the bond interface operating mode |
| `lacp-rate` | Sets the LACPDU packet transmission rate |
| `xmit-hash-policy` | Selects the algorithm for slave selection according to the specified TCP/IP layer |

**Example**

```
set bonding group 666 interface eth1
```

**Comments** Most of these commands do not show output.

DRAFT

## Creating or Deleting a Bond Interface

### To add a new bond interface:

Run `add bonding group <Bond_id>`.

**Bond ID** - Bond name (integer between 1 and 1024)

Example:

```
add bonding group 777
```

### To delete a bond interface:

1. Make sure that you remove all slave interfaces from the bond.
2. Run `delete bonding group <bond_id>`.

## Defining Slave Interfaces

A bond interface typically contains between two and eight slave interfaces. This section shows how to add and remove a slave interface. The slave interface must not have IP addresses assigned to it.

### To add a slave interface to a bond, run:

```
add bonding group <Bond ID> interface <IF Name>
```

- **Bond ID** - Bond name
- **IF Name** - Slave interface name

Example:

```
add bonding group 777 interface eth4
```

### To set the slave interface to the UP (ON) state, run:

```
Set interface <IF> state on
```

- **IF** - Interface name

Example:

```
Set interface eth4 state on
```

### To delete a slave interface from a bond, run:

```
delete bonding group <Bond ID> interface <IF Name>
```

Example:

```
delete bonding group 777 interface eth4
```

**Note** - You must delete all non-primary slave interfaces before you remove the primary slave interface.

## Defining the Bond Operating Mode

You can define bond interfaces using one of these operating modes:

- **Round Robin** - Selects the active slave interface sequentially.
- **Active/Backup** - If the active slave interface goes down, the connection automatically fails over to the primary slave interface. If the primary slave interfaces is not available, the connection fails over to a different slave.
- **802.3ad** - Dynamically uses active slaves to share the traffic load using the LACP protocol. This protocol enables full interface monitoring between the gateway and a switch.
- **XOR** - Selects the algorithm for slave selection according to the TCP/IP layer.

### To define the bond operating mode:

Run set bonding group <Bond_id> mode <mode>.

- **Bond ID** - Bond name
- **Mode** - One of these key words:
  - round-robin
  - active-backup
  - xor
  - 8023AD

The default is active-backup

Example:

```
set bonding group 777 mode round-robin
```

## Defining the Primary Slave Interface

When using the **Active/Backup** operating mode, the system automatically fails over to the primary slave interface, if available. If the primary interface is not available, the system fails over to a different slave interface. By default, the first slave interface that you define is the primary interface. You must define the slave interfaces and set the operating mode as Active/Backup before doing this procedure.

**Note** - You must delete all non-primary slave interfaces before you remove the primary slave interface.

### To define the primary slave interface, run:

```
set bonding group <Bond ID> primary <IF>
```

- **Bond ID** - Bond name
- **IF** - Interface name

Example

```
set bonding group 777 primary eth4
```

## Defining the Media Monitoring Interval

This sets the frequency of requests sent to the Media Independent Interface (MMI) to confirm that a slave interface is up. The valid range is 1-5000 ms and the default is 100 ms.

### To configure the MMI, run:

```
set bonding group <Bond ID> mii-interval <Interval>
```

- **Bond ID** - Bond name

DRAFT

- **Interval** - Frequency range (1-5000 ms  default = 100 ms)

Example:

```
set bonding group 777 mii-interval 500
```

### To disable MMI monitoring, run:

```
set bonding group <Bond ID> mii-interval 0
```

## Defining the ARP monitoring interval

This defines the frequency of ARP requests sent to confirm that a slave interface is up. ARP requests are sent to as many as five external MAC addresses.

### To configure the ARP interval, run:

```
set bonding group <Bond ID> arp-polling-interval <Interval>
```

- **Bond ID** - Bond name
- **Interval** - Frequency (1-5000 ms  default = 100 ms)

Example:

```
Set bonding group 777 arp-polling-interval 500
```

### To disable the ARP interval, run:

```
set bonding group <Bond ID> arp-polling-interval 0
```

## Defining the UP and Down Delay Times

This parameter defines the waiting time, in milliseconds, to confirm the slave interface status before taking the specified action.

### To configure the UP and Down delay times, run:

```
set bonding group <Bond ID> down-delay <Delay time>
set bonding group <Bond ID> up-delay <Delay time>
```

- **Bond ID** - Bond name
- **Delay Time** - Delay (0-5000 ms  default = 200 ms)

Example:

```
set bonding group 777 down-delay 500
```

## Defining Load Sharing Parameters

When using load sharing modes (XOR or 802.3ad), you can configure these parameters:

- **LACP Rate** - This parameter sets the LACPDU packet transmission rate.
- **Transmit Hash Policy** (802.3ad only) - This parameter selects the algorithm for slave selection according to the specified TCP/IP layer.

### To set the LACP rate, run

```
set bonding group <Bond ID> lacp-rate [slow | fast]
```

- **Bond ID** - Bond name
- **Fast** - LACPDU packets sent every second
- **Slow** - LACPDU packets sent every 30 seconds

Example:

```
set bonding group 777 lacp-rate
```

### To set the Transmit Hash Policy, run:

```
set bonding group <Bond ID> xmit-hash-policy <layer>
```

- **Bond ID** - Bond name
- **Layer** - TCP/IP layer
    - **layer2** - Uses XOR of the physical interface MAC address
    - **layer3+4** - Uses upper layer protocol information

Example:

```
set bonding group 777 xmit-hash-policy layer2
```

DRAFT

### Making Sure that Link Aggregation is Working

To make sure that a link aggregation is working for a specified bond interface, run this command from the expert mode:

```
cat /proc/net/bonding/<Bond ID>
```

Example with output:

```
cat /proc/net/bonding/bond666
Ethernet Channel Bonding Driver: v3.2.4 (January 28, 2008)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: eth2
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 100
Down Delay (ms): 200

Slave Interface: eth2
MII Status: up
Link Failure Count: 2
Permanent HW addr: 00:50:56:94:11:de
```

# Loopback Interfaces

Placeholder

## *Configuring Loopback Interfaces - WebUI*

### To add a loopback interfcae:

1. In the navigation tree, click **Interface Management** > **Network Interfaces**.
2. In the **Interfaces** section, click **Add**, and select **Loopback** from the drop down list.

   The **Add Loopback** window opens.
3. Select **Enable**.
4. In **Comment**, you can leave information regarding the interface.

   You can configure The loopback interfcae as IPv4, IPv6, or IPv4 and IPv6. You cannot obtain the addresses automatically.
5. To configure an IPv4 address:

   a) In the **IPv4** tab, in **IPv4 address**, enter the address to be used. It cannot conflict with a destination network of a different interface.

   b) In **Subnet mask**, enter the Subnet mask number.
6. To configure an IPv6 address:

   a) In the **IPv6** tab, in **IPv6**, enter the address to use.

   b) In **Mask Length**, select the length with the arrows.
7. Click **OK**.

### To edit a loopback interface:

1. In the navigation tree, click **Interface Management** > **Network Interfaces**.
2. In the **Interfaces** section, select the loopback interface and click **Edit**. The **Edit (loopback interface name)** window opens.
3. In the **Edit** window, you can change any setting: clear **Enable**, change the comment, add, remove or change addresses.

### To delete a loopback interface:

1. In the navigation tree, click **Interface Management** > **Network Interfaces**. A message opens. It makes sure you choose to delete the interface.
2. Click **Yes**.

DRAFT

## *Configuring Loopback Interfaces - CLI (interface)*

Placeholder

# ARP

The Address Resolution Protocol (ARP) allows a host to find the physical address of a target host on the same physical network using only the target's IP address. ARP is a low-level protocol that hides the underlying network physical addressing and permits assignment of an arbitrary IP address to every machine. ARP is considered part of the physical network system and not as part of the Internet protocols.

## ARP- WebUI

### To show dynamic ARP entries

1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the *Static Arp* topic, click **Related Topics: Dynamic ARP**

### To show static ARP entries

1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the *Dynamic Arp* topic, click **Related Topics: Static ARP**

### To change Static and dynamic ARP parameters

1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the *Dynamic Arp* topic, click **Related Topics: Static ARP**
3. In the **ARP Table Settings** section:

   a) Enter the **Maximum Entries.** This is the maximum number of entries in the arp cache.

   Default: 1024, Range: 1024-16384

   b) Enter the **Validity Timeout.** This is the time, in seconds, to keep resolved dynamic ARP entries. If the entry is not referred to and is not used by traffic before the time elapses, it is deleted. Otherwise, a request will be sent to verify the MAC address.

   Default: 60 (seconds), Range: 60-86400 (24 hours)

### To add a static ARP entry

1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the *Dynamic Arp* topic, click **Related Topics: Static ARP**
3. Click **Add**.
4. Enter the **IP Address** of the static ARP entry and the **MAC Address** used when forwarding packets to the IP address.
5. **Click OK**.

### To delete a Static ARP entry

1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the *Dynamic Arp* topic, click **Related Topics: Static ARP**
3. Select a Static ARP entry
4. Click **Remove**.

### To flush all dynamic ARP entries

1. In the WebUI, go to the **Interface Management > ARP** page.
2. If you are in the *Static Arp* topic, click **Related Topics: Dynamic ARP**
3. Click **Flush All**.

DRAFT

# ARP - CLI (arp)

**Description** Commands to configure the Address Resolution Protocol (ARP)

**Syntax** To add a static arp entry

```
add arp static ipv4-address VALUE macaddress VALUE
```

To delete static and dynamic arp entries

```
delete arp dynamic all
delete arp static ipv4-address VALUE
```

To set arp parameters

```
set arp table validity-timeout VALUE
set arp table cache-size VALUE
```

To show arp parameters

```
show arp dynamic all
show arp static all
show arp table validity-timeout
show arp table cache-size
```

**Parameters**

| Parameter | Description |
|---|---|
| `static` | Configured static arp entries |
| `dynamic` | Configured dynamic arp entries |
| `ipv4-address` | IP Address of a static ARP entry. Range: Dotted-quad ([0-255].[0-255].[0-255].[0-255]).<br>Default: No Default |
| `macaddress` | The hardware address used when forwarding packets to the given IP address. Range: Six hexadecimal octets separated by colon.<br>Default: No Default |
| `table validity-timeout` | This is the time, in seconds, to keep resolved dynamic ARP entries. If the entry is not referred to and is not used by traffic before the time elapses, it is deleted. Otherwise, a request will be sent to verify the MAC address.<br>Default: 60 (seconds), Range: 60-86400 (24 hours) |
| `table cache-size` | This is the maximum number of entries in the arp cache.<br>Default: 1024, Range: 1024-16384 |

# DHCP Server

Dynamic Host Configuration Protocol (DHCP) for Check Point Gaia provides DHCP client and DHCP server capabilities for your Check Point appliance. DHCP lets you supply network configuration parameters, through a server, to clients which require the parameters to operate on a network. DHCP eliminates the need for you to configure each client manually and therefore reduces configuration errors.

The Check Point Gaia implementation of DHCP includes:

- Enabling the DHCP client

- Configuring the DHCP client interface
- Dynamic and fixed IP address allocation from the DHCP server.
- Automatic Domain Name System (DNS) server updates from the DHCP server.
- The option to specify different client parameters. That includes which servers are available for services such as DNS, NTP, TFTP, and SMTP. You can also configure NetBIOS over TCP/IP which includes identifying WINS and Datagram Distribution servers available to clients.
- Support for VLAN clients.

**Note** - If you enable the Gaia DHCP server, the appliance receives and accepts DHCP requests even if there is a firewall rule blocking DHCP requests. Although requests are shown as blocked in the firewall logs, the Gaia DHCP server still provides addresses to clients that request them. If you don’t need the DHCP server, leave it disabled (the default option). If you enable the DHCP server but do not want DHCP requests from the outside to be accepted, enable it only on internal interfaces.

# Configuring a DHCP Server- WebUI

From Gaia

### To Enable the DHCP Server Process:

1. In the tree view, click **Interface Management** > **DHCP Server**.
2. Below DHCP Server Configuration, select **Enable DHCP Server**.
3. Click **Apply**.

**Note** - You must configure an Ethernet interface and enter the subnet address and the subnet mask length on which the interface is listening before you enable the DHCP Server Process. See Configuring the DHCP Server. For more information on how to configure Ethernet interfaces, see Ethernet Interfaces (on page 24).

### To Disable the DHCP Server Process:

1. In the tree view, click **Interface Management** > **DHCP Server**.
2. Below DHCP Server Configuration, clear **Enable DHCP Server**.
3. Click **Apply**.

### To Configure the DHCP Server Process:

1. In the tree view, click **Interface Management** > **DHCP Server**.
2. select Enable DHCP Server.
3. Click **Apply**.

**Note** - You must configure an Ethernet interface and enter the subnet address and the subnet mask length on which the interface is listening before you enable the DHCP Server Process. See Configuring the DHCP Server. For more information on how to configure Ethernet interfaces, see Ethernet Interfaces (on page 24).

4. Below DHCP Server Interface, click **Add**.
5. Enter the subnet address of the Ethernet interface you configured.
6. Enter the mask length for the subnet in the Mask Length text box.
7. (Optional) Below **Lease Configuration**, in **Default Lease**, enter the lease length, in seconds, for client IP addresses. This is applied only if clients do not request a unique lease time. If you do not enter a value, the configuration default is 43,200 seconds.
8. (Optional) Below **Lease configuration**, in **Maximum Lease**, enter the maximum lease length, in seconds, for client IP addresses. This is the longest lease available. If you do not enter a value, the configuration default is 86,400 seconds.
9. Below **Address Pool**, in the **Start** and **End** fields, enter the range of IP addresses for the server to assign to clients.

**Note** - If you configure a large number of VLANs, there might be a delay in IP addresses assignement to VLAN interfaces.

### To Add a DHCP Address Pool:

1. In the tree view, click **Interface Management** > **DHCP Server**. The **Edit DHCP** window opens.

DRAFT

2. Select an IP address, click **Add**. A new line shows in the Address Pool table.
3. In that new line, enter the range of IP addresses for the server to assign to clients in **Start** and **End**.

**Note -**

- Make sure that Enabled DHCP is selected. This is the default selection.
- If you configure a large number of VLANs, there might be a delay in IP addresses assignement to VLAN interfaces.

4. Click **Apply**.

### To Enable a DHCP Adrress Pool:

1. In the tree view, click **Interface Management** > **DHCP Server**.
2. Below DHCP Server Interfaces, select an interface. The **Edit DHCP** window opens.
3. Select Enable DHCP.
4. Click **OK**..

# Configuring a DHCP Server - CLI (dhcp)

**Description** Use these commands to configure DHCP clients and DHCP servers.

**Syntax** To enable or disable the DHCP Server:

```
set dhcp server disable
set dhcp server enable
```

To create subnets:

```
add dhcp server interface VALUE exclude-ip-pool start VALUE end
VALUE
add dhcp server interface VALUE include-ip-pool start VALUE end
VALUE
add dhcp server interface VALUE subnet VALUE netmask VALUE
```

To change subnet configurations:

```
set dhcp server interface VALUE default-gateway VALUE
set dhcp server interface VALUE default-lease VALUE
set dhcp server interface VALUE disable
set dhcp server interface VALUE dns VALUE
set dhcp server interface VALUE domain VALUE
```

According to team leader ghanin, dns (+domain) will be automatic

```
set dhcp server interface VALUE enable
set dhcp server interface VALUE exclude-ip-pool VALUE disable
set dhcp server interface VALUE exclude-ip-pool VALUE enable
set dhcp server interface VALUE include-ip-pool VALUE disable
set dhcp server interface VALUE include-ip-pool VALUE enable
set dhcp server interface VALUE max-lease VALUE
set dhcp server interface VALUE subnet VALUE netmask VALUE
```

To view all DHCP configurations

```
show dhcp server all
```

To view subnet configurations:

```
show dhcp server interface VALUE ip-pools
show dhcp server interfaces
show dhcp server status
```

To delete subnets:

```
delete dhcp server interface VALUE exclude-ip-pool VALUE
delete dhcp server interface VALUE include-ip-pool VALUE
```

DRAFT

**Description** Use these commands to configure DHCP clients and DHCP servers.

**Parameters**

| Parameter | Description |
|---|---|
| `interface` | The name of the interface |
| `start` | The IP address that starts the allocated IP Pool range, the one with the lowest number. |
| `end` | The IP address that ends the allocated IP Pool range, the one with the highest number. |
| `subnet` | The subnet address |
| `netmask` | The subnet mask number |
| `default-gateway` | The default gateway IP address |
| `default-lease` | The number of seconds you choose for the client, unless the client asks for a certain one. Seperate from the system default lease, which is valid if you do not command otherwise. |
| `max-lease` | The maximum number of seconds you allow. |
| `exclude-ip-pool` | The range of IPs to exclude. For example: `192.168.3.120-192.168.3.212`. |
| `include-ip-pool` | The range of IPs to include. |

**Example**

```
set dhcp server interface VALUE exclude-ip-pool VALUE disable
```

**Output**

```
gw-940449>
```

**Comments** The output is a new command line. In the absence of an error message, this means the command works.

# Hosts and DNS

## Host Addresses

You should add host addresses for systems that will communicate frequently with the system. You can:

- View the entries in the hosts table.
- Add an entry to the list of hosts.
- Modify the IP address of a host.
- Delete a host entry.

### *Configuring Hosts- WebUI*

**To add a static host entry**

1. Go to the **Interface Management > Hosts and DNS** page.
2. In the **Hosts** section, click **Add**.
3. Enter the
   - **Host Name**. Must include only alphanumeric characters, dashes ('-'), and periods ('.'). Periods must be followed by a letter or a digit. The name may not end in a dash or a period. There is no default value.
   - **IPv4 address**

DRAFT

- **IPv6 address**

### To edit a static host entry

1. Go to the **Interface Management > Hosts and DNS** page.
2. In the **Hosts** section, select a host and click **Edit**.
3. Edit the
   - **Host Name.**
   - **IPv4 address**
   - **IPv6 address**

### To delete a static host entry

1. Go to the **Interface Management > Hosts and DNS** page.
2. In the **Hosts** section, select a host and click **Delete**.

## *Configuring Hosts - CLI (host)*

DRAFT

**Description**

Add, edit, delete and show the name and addresses for hosts that will communicate frequently with the system

**Syntax**

To add a host name and address:

```
add host name VALUE ipv4-address VALUE
add host name VALUE ipv6-address VALUE
```

To edit the name and IPv4 or IPv6 address of a host:

```
set host name VALUE ipv4-address VALUE
set host name VALUE ipv6-address VALUE
```

To delete a host name and address:

```
delete host name VALUE ipv4
delete host name VALUE ipv6
```

To show an IPv4 or IPv6 host address:

```
show host name VALUE ipv4
show host name VALUE ipv6
```

To show all IPv4 or IPv6 hosts:

```
show host names ipv4
show host names ipv6
```

**Parameters**

| Parameter | Description |
|---|---|
| `name VALUE` | The name of a static host. Must include only alphanumeric characters, dashes ('-'), and periods ('.'). Periods must be followed by a letter or a digit. The name may not end in a dash or a period. There is no default value. |
| `ipv4-address VALUE` | The IPv4 address of the host |
| `ipv6-address VALUE` | The IPv6 address of the host |

# Host Name

You set the host name (system name) during initial configuration. You can change the name.

## *Configuring Host Name - WebUI*

### To show the host name

The host name is in the header of the WebUI.

### To change the host name

1. Open the **Interface Management > Host and DNS** page.
2. In the **System Name** section, enter the **Host Name**.

## *Configuring Host Name - CLI (hostname)*

**Description** Use this group of commands to configure the host name of your platform.

**Syntax** **To set the host name**

```
set hostname VALUE
```

**To show the host name**

```
show hostname
```

# Domain Name Service (DNS)

DRAFT

Gaia uses the Domain Name Service (DNS) to translate host names into IP addresses. To enable DNS lookups, you must specify the primary DNS server for your system. You can also specify secondary and tertiary DNS servers. When resolving host names, the system consults the primary name server first, followed by the secondary and tertiary name servers if a failure or time-out occurs. You can also define a DNS Suffix, which is a search for host-name lookup.

## *Configuring DNS - WebUI*

### To configure the DNS Server for the Gaia computer:

1. In the WebUI, go to the **Interface Management > Hosts and DNS** page.
2. In the **System Name** section, enter the **Domain Name.**
3. In the **DNS** Section, enter the

   a) **DNS Suffix**. A search list for host-name lookup. The search is normally determined from the local domain name. By default, it contains only the local domain name. A valid domain name suffix is made up of subdomain strings separated by periods. Subdomain strings must begin with an alphabetic letter and may consist only of alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 (modified slightly in RFC 1123).

   For example, if you set the DNS Suffix to `example.com` and try to ping some host `foo` (by running `ping foo`), and foo cannot be resolved, then the resolving computer will try to resolve `foo.example.com`.

   b) IPv4 address of the **Primary DNS Server**. The server to use when resolving hostnames. This should be a host running a DNS server

   c) (Optional) IPv4 address of the **Secondary DNS Server**. The server to use when resolving hostnames if the primary server does not respond. This should be a host running a DNS server.

   d) (Optional) IPv4 address of the **Tertiary DNS Server**. The server to use when resolving hostnames if the primary and secondary servers do not respond. This should be a host running a DNS server.

## *Configuring DNS - CLI (dns)*

**Description** Configure, show and delete the DNS servers and the DNS suffix for the Gaia computer.

**Syntax**

To configure the DNS servers and the DNS suffix for the Gaia computer.

```
set dns primary VALUE
set dns secondary VALUE
set dns tertiary VALUE
set dns suffix VALUE
```

To show the DNS servers and the DNS suffix for the Gaia computer.

```
show dns primary
show dns secondary
show dns tertiary
show dns suffix
```

To delete the DNS servers and the DNS suffix for the Gaia computer.

```
delete dns primary
delete dns secondary
delete dns tertiary
delete dns suffix
```

**Parameters**

| Parameter | Description |
|---|---|
| `primary` | The server to use when resolving hostnames. This should be a host running a DNS server. |
| `secondary` | The server to use when resolving hostnames if the primary server does not respond. This should be a host running a DNS server. |
| `tertiary` | The server to use when resolving hostnames if the primary and secondary servers do not respond. This should be a host running a DNS server. |
| `suffix` | A search list for host-name lookup. The search is normally determined from the local domain name. By default, it contains only the local domain name. A valid domain name suffix is made up of subdomain strings separated by periods. Subdomain strings must begin with an alphabetic letter and may consist only of alphanumeric characters and hyphens. The domain name syntax is described in RFC 1035 (modified slightly in RFC 1123).<br>For example, if you set the DNS Suffix to `example.com` and try to ping some host `foo` (by running `ping foo`), and foo cannot be resolved, then the resolving computer will try to resolve `foo.example.com`. |
| `VALUE` | An IPv4 address |

# Static Routes

A static route defines the destination and one or more paths (next hops) to get to that destination. You define static routes manually using the WebUI or the `set static-route` command from the CLI.

Static routes let you add paths to destinations that are unknown by dynamic routing protocols. You can define multiple paths (next hops) to a destination and define priorities for selecting a path. Static routes are also useful for defining the default route.

Static route definitions include these parameters:

- Destination IP address.
- Route type:
  - **Normal** - Accepts and sends packets to the specified destination.

    - **Reject -** Drops packets and sends an error message to the traffic source.
    - **Black hole** - Drops packets, but does not send an error message.
- Next-hop gateway type:
    - **Address** - Identifies the next hop gateway by its IP address.
    - **Logical** - Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface.
- Gateway identifier - IP address or interface name.
- Priority (Optional) - Assigns a path priority when there are many different paths.
- Rank (Optional) - Selects a route when there are many routes to a destination that use different routing protocols. You must use the CLI to configure the rank.

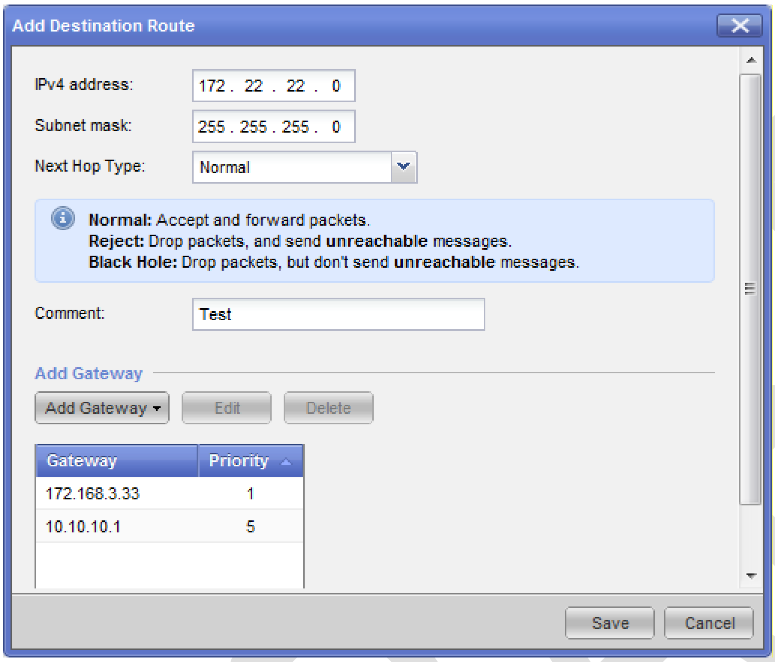
DRAFT

# Configuring IPv4 Static Routes - WebUI

You can configure static routes one at a time or use the Batch Mode to configure many routes simultaneously.

### To configure one static route at a time:

1. In the WebUI navigation tree, select **Static Routes**.
2. In the **Static Routes** pane, click **Add**
   or
   Select a route and click **Edit** to change an existing route.
3. In the **Add** (or **Edit**) **Destination Route** window, enter the IPv4 address and subnet mask.



Add Destination Route

IPv4 address: 172 . 22 . 22 . 0

Subnet mask: 255 . 255 . 255 . 0

Next Hop Type: Normal

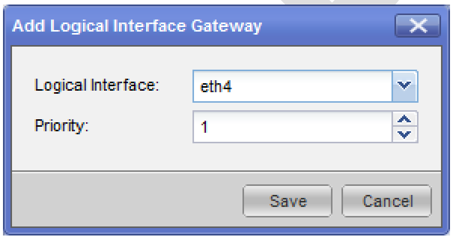
**Normal:** Accept and forward packets.
**Reject:** Drop packets, and send **unreachable** messages.
**Black Hole:** Drop packets, but don't send **unreachable** messages.

Comment: Test

Add Gateway

| Gateway | Priority |
|---|---|
| 172.168.3.33 | 1 |
| 10.10.10.1 | 5 |

4. Select the **Next Hop Type**.
   - **Normal** - Accepts and sends packets to the specified destination.
   - **Reject** - Drops packets and sends an error message to the traffic source.
   - **Black Hole** - Drops packets, but does not send an error message.
5. Click **Add Gateway** or double-click an existing gateway.
6. For new interfaces only, select an interface type.
   - **Normal** - Identifies the destination gateway by its IP address.
   - **Network Interface** - Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface. This option is known as a logical interface in the CLI.
7. In the **Add** (or **Edit**) **Interface Gateway** window, enter the IP address or interface name.



Add Logical Interface Gateway

Logical Interface: eth4

Priority: 1

8. Select a **Priority** between 1 and 8. The priority sets the order for selecting the next hop among many gateways. 1 (default) is the highest priority and 8 is the lowest. This parameter is required.

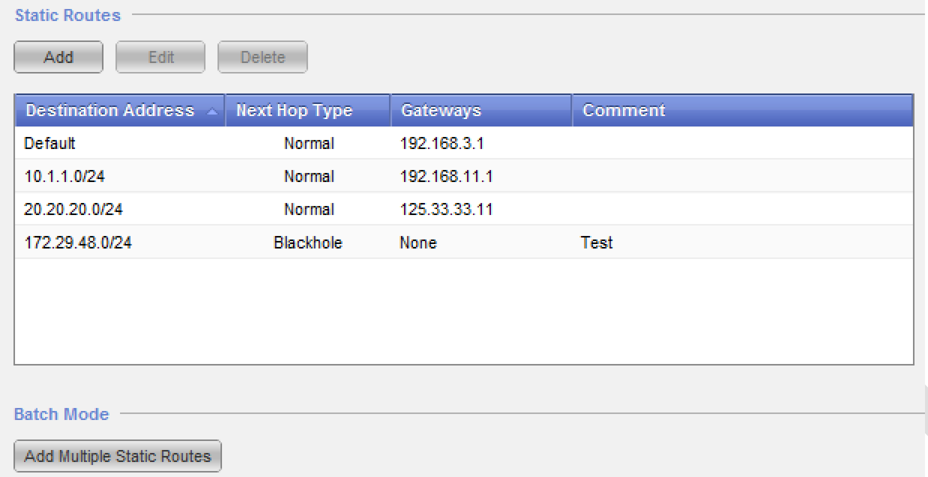
## *Configuring Many Static Routes at Once*

You can use the batch mode to configure multiple static routes in one step.

**Note -** You cannot configure a network (logical) interface using this option.

### To add many static routes at once:

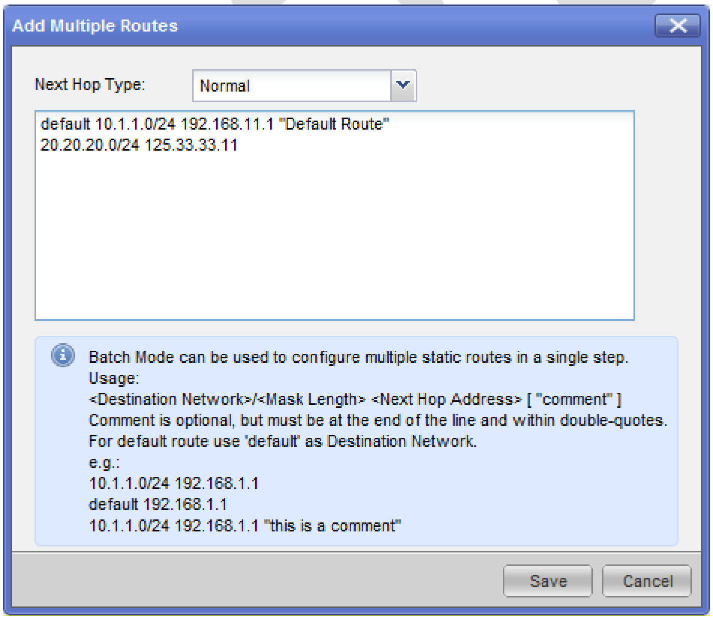
1. In the WebUI navigation tree, select **Static Routes**.
2. In the **Static Routes** pane, click **Add Multiple Static Routes**.



| Destination Address | Next Hop Type | Gateways | Comment |
|---|---|---|---|
| Default | Normal | 192.168.3.1 | |
| 10.1.1.0/24 | Normal | 192.168.11.1 | |
| 20.20.20.0/24 | Normal | 125.33.33.11 | |
| 172.29.48.0/24 | Blackhole | None | Test |

3. In the **Add Multiple Routes** window, select the **Next Hop Type**.
   - **Normal** - Accepts and sends packets to the specified destination
   - **Reject** - Drops packets and sends an error message to the traffic source
   - **Black Hole** - Drops packets, but does not send an error message
4. Add the routes in the text box, using this syntax:

```
<Destination IP>/<Mask length> <Next Hop IP> [<Comment>]
```



Next Hop Type: Normal

```
default 10.1.1.0/24 192.168.11.1 "Default Route"
20.20.20.0/24 125.33.33.11
```

Batch Mode can be used to configure multiple static routes in a single step.
Usage:
<Destination Network>/<Mask Length> <Next Hop Address> [ "comment" ]
Comment is optional, but must be at the end of the line and within double-quotes.
For default route use 'default' as Destination Network.
e.g.:
10.1.1.0/24 192.168.1.1
default 192.168.1.1
10.1.1.0/24 192.168.1.1 "this is a comment"

**default** - Use this as an alternative to the default route IP address

**Destination IP** - Destination IP address using dotted decimal notation

**Mask length** - Net mask using slash (/xx) notation

**Next Hop IP** - Next hop gateway IP address using dotted decimal notation

**Comment** - Optional free text comment

Examples:

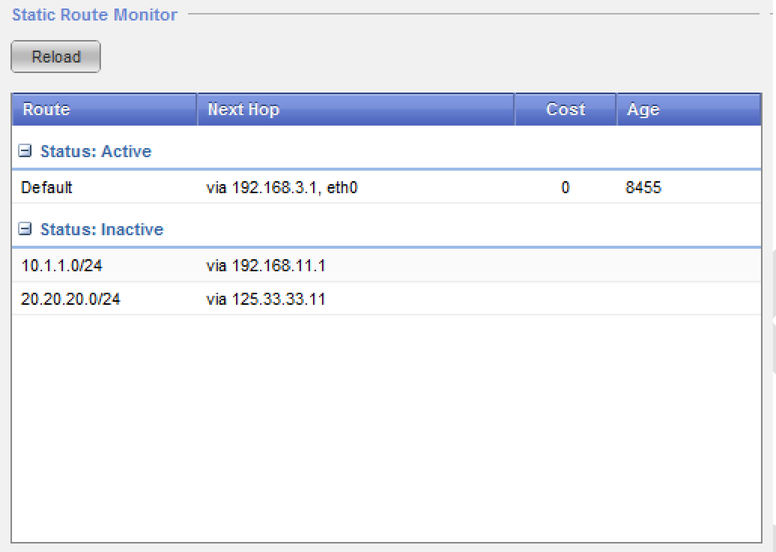
```
default 10.1.1.0/24 192.168.11.1 "Default Route"
20.20.20.0/24 125.33.33.11
```

5. Click **Apply**.

   The newly configured more static routes show in the list of Static Routes in the **Static Routes** page.

   **Note -** The text box shows entries that contain errors with messages at the top of the page.

6. Correct errors and reload the affected routes.
7. Click the **Monitoring** tab to make sure that the routes are configured correctly.



| Route | Next Hop | Cost | Age |
|---|---|---|---|
| ⊟ Status: Active | | | |
| Default | via 192.168.3.1, eth0 | 0 | 8455 |
| ⊟ Status: Inactive | | | |
| 10.1.1.0/24 | via 192.168.11.1 | | |
| 20.20.20.0/24 | via 125.33.33.11 | | |

DRAFT

# Configuring Static Routes - CLI (static-route)

You only use the `set` operation with the `static-route` command, even when adding or deleting a static route.

**Description** Add, change or delete an IPv4 static route.

**Syntax**

```
set static-route <Destination>
   nexthop gateway address <GW IP> [priority <P Value>] on|off
   nexthop gateway logical <GW IF> [priority <P Value>] on|off
   nexthop blackhole
   nexthop reject

set static-route <Destination> off
set static-route <Destination> rank <0-255>
```

To show static routes

```
show route static
```

**Parameter**

| Keyword | Description |
|---|---|
| `nexthop` | Defines the next hop path, which can be a `gateway`, `blackhole` or `reject`. |
| `gateway` | Accepts and sends packets to the specified destination. |
| `blackhole` | Drops packets, but does not send an error message. |
| `reject` | Drops packets and sends an error message to the traffic source. |
| `address` | Identifies the next hop gateway by its IP address. |
| `logical` | Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface. |
| `priority` | Assigns a path priority when there are many different paths. The available path with the lowest priority value is selected. |
| `on` | Adds the specified route or next hop. |
| `off` | Deletes the specified route or next hop. If you specify a next hop, only the specified path is deleted. If no next hop is specified, the route and all related paths are deleted. |
| `rank` | Selects a route when there are many routes to a destination that use different routing protocols. The route with the lowest rank value is selected.<br>Use the `rank` keyword in place of the `nexthop` keyword with no other parameters. |

**Values**

| Value Type | Description |
|---|---|
| `Destination` | Destination IP address using dotted decimal/mask length (slash) notation. You can use the `default` keyword instead of an IP address when referring to the default route. |
| `GW IP` | Gateway IP address in dotted decimal notation in dotted decimal format without a net mask. |
| `GW IF` | Name of the interface that connects to the next hop gateway. |
| `P Value` | Priority. An integer between 1 and 8 (default=1). |
| `Rank Value` | Rank. An integer between 0 and 255 (default=0). |

**Examples**

```
set static-route 4.4.4.0/24 nexthop gateway address 7.7.7.6 on
set static-route 4.4.4.0/24 nexthop gateway address 9.9.9.2 off
set static-route 4.4.4.0/24 off
set static-route 172.116.14.0/24 nexthop blackhole
set static-route 40.40.40.0/24 rank 2
```

**Comments**

There are no `add` commands for the `static-route` feature. To show static routes, run

```
show route static
```

DRAFT

## *CLI Procedures*

This section includes some basic procedures for managing static routes using the CLI.

### To show static routes, run

```
show route static
 Codes: C - Connected, S - Static, R - RIP, B - BGP,
        O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA)
        A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed

S      0.0.0.0/0           via 192.168.3.1, eth0, cost 0, age 164115
S      172.29.48.0/24      is a blackhole route
S      172.116.14.0/24     is a reject route
```

### To add a static route, run:

```
set static-route <Destination> nexthop gateway <GW IP> on
set static-route <Destination> nexthop gateway <GW IF> on
```

`Destination` - Destination IP address.
`GW IP` - Next hop gateway IP address.
`GW IF` - Interface that connects to the next hop.

Example:

```
set static-route 4.4.4.0/24 nexthop gateway address 7.7.7.6 on
set static-route 4.4.4.0/24 nexthop gateway logical 7.7.7.6 on
```

### To add a static route with paths and priorities, run:

```
set static-route <Destination> nexthop gateway <GW ID> priority <P Value>
```

`Destination` - Destination IP address
`GW IP` - Next hop gateway IP address
`P Value` - Integer between 1 and 8 (default =1)

Run this command for each path, assigning a priority value to each. You can define two or more paths using the same priority to specify a backup path with equal priority.

Examples:

```
set static-route 4.4.4.0/24 nexthop gateway address 9.9.9.2 on
priority 1
set static-route 4.4.4.0/24 nexthop gateway address 9.9.9.3 on
priority 1
set static-route 4.4.4.0/24 nexthop gateway logical eth4 on priority 2
set static-route 4.4.4.0/24 nexthop gateway logical eth5 on priority 3
```

### To add a static route where packets are dropped, run:

```
set static-route <Destination> nexthop reject
set static-route <Destination> nexthop blackhole
```

`Destination` - Destination IP address.
`Reject` - Drops packets and sends an error message to the traffic source.
`Blackhole` - Drops packets, but does not send an error message.

Examples:

```
set static-route 172.116.14.0/24 nexthop reject
or
set static-route 172.116.14.0/24 nexthop blackhole
```

### To delete a route and all related paths, run:

```
set static-route <Destination> off
```

`Destination` - Destination IP address.

Example:

```
set static-route 172.116.14.0/24 off
```

DRAFT

**To delete a path only, run:**

```
set static-route <Destination> nexthop gateway <GW ID> off
```

`Destination` - Destination IP address.
`GW ID` - Next hop gateway IP address or interface name.

Example:

```
set static-route 4.4.4.0/24 nexthop gateway address 7.7.7.6 off
```

# IPv6 Static Routes

## Configuring IPv6 Static Routes - WebUI

You can configure IPv6 static routes one at a time.

**To configure one static route at a time:**

1. In the WebUI navigation tree, select **IPv6 Static Routes**.
2. In the **IPv6 Static Routes** pane, click **Add**
   or
   Select a route and click **Edit** to change an existing route.
3. In the **Add** (or **Edit**) **Destination Route** window, enter the IPv6 address and prefix (default = 64).
4. Select the **Next Hop Type**.
   - **Normal** - Accepts and sends packets to the specified destination.
   - **Reject** - Drops packets and sends an error message to the traffic source.
   - **Black Hole** - Drops packets, but does not send an error message.
5. Click **Add Gateway** or double-click an existing gateway.
6. In the **Add** (or **Edit**) **Gateway** window, enter the IP address or interface name.
7. Select a **Priority** between 1 and 8. The priority sets the order for selecting the next hop among many gateways. 1 is the highest priority and 8 is the lowest. This parameter is required.

DRAFT

# Configuring Static Routes - CLI (static-route)

This section includes a complete command reference for the `ipv6 static-route` command. You can only use the `set` operation with this command, even when adding or deleting a static route.

**Description** Add, change or delete an IPv4 static route.

**Syntax**

```
set ipv6 static-route <Destination>
   nexthop gateway <GW IP>
      [priority <P Value>] on|off
      interface <GW IF> [priority <P Value>] on|off
   nexthop blackhole
   nexthop reject
   off
```

**Parameter**

| | |
|---|---|
| `nexthop` | Defines the next hop path. |
| `on` | Enables the specified route or next hop. |
| `off` | Deletes the specified route or next hop. If you specify a next hop, only the specified path is deleted.  If no next hop is specified, the route and all related paths are deleted. |
| `gateway` | Accepts and sends packets to the specified destination. |
| `blackhole` | Drops packets, but does not send an error message. |
| `reject` | Drops packets and sends an error message to the traffic source. |
| `interface` | Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface. |
| `priority` | Assigns a path priority when there are many different paths. The available path with the lowest priority value is selected. The gateway with the lowest priority value is selected. |

**Value**

| | |
|---|---|
| `Destination` | Destination IP address. |
| `Route Type` | `gateway` - Accepts and sends packets to the specified destination<br>`reject` - Drops packets and sends an error message to the traffic source<br>`blackhole` - Drops packets, but does not send an error message- |
| `GW IP` | Identifies the next hop gateway by its IP address. |
| `GW IF` | Identifies the next hop gateway by the interface that connects to it. Use this option only if the next hop gateway has an unnumbered interface. |
| `P Value` | Integer value between 1 and 8 (default=1). |

**Examples**

```
set ipv6 static-route 3100:192::0/64 nexthop 3900:172::1
priority 2 on

set ipv6 static-route 3100:192::0/64 nexthop 3900:172::1
interface eth3 priority 2 on

set ipv6 static-route 3100:192::0/64 nexthop off
set ipv6 static-route 3300:123::0/64 nexthop blackhole
```

**Comments** There are no `add` or `show` commands for the static route feature.

## *CLI Procedures*

This section includes some basic procedures for managing static routes using the CLI.

### To show static routes, run

```
show ipv6 route static
Codes: C - Connected, S - Static, B - BGP, Rg - RIPng, A - Aggregate,
       O - OSPFv3 IntraArea (IA - InterArea, E - External),
       K - Kernel Remnant, H - Hidden, P - Suppressed

S      3100:55::1/64        is directly connected
S      3200::/64            is a blackhole route
S      3300:123::/64        is a blackhole route
S      3600:20:20:11::/64   is directly connected, eth3
```

### To add a static route, run:

```
set ipv6 static-route <Destination> nexthop gateway <GW IP> on
set ipv6 static-route <Destination> nexthop gateway <GW IP> interface
<GW IF> on
```

**Destination** - Destination IPv6 address.
**GW IP** - Next hop gateway IPv6 address.
**GW IP** - Next hop gateway interface name.

Example:

```
set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 on
set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 interface
eth3 on
```

### To add a static route with paths and priorities, run:

```
set static-route <Destination> nexthop gateway <GW ID> priority <P Value>
```

**Destination** - Destination IP address.
**GW IP** - Next hop gateway IP address.
**P Value** - Integer between 1 and 8 (default =1)

Run this command for each path, assigning a priority value to each. You can define two or more paths using the same priority to specify a backup path with equal priority.

Example:

```
set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 priority 3
on
```

### To add a static route where packets are dropped, run:

```
set ipv6 static-route <Destination> nexthop reject
set ipv6 static-route <Destination> nexthop blackhole
```

**Destination** - Destination IP address.
**Reject** - Drops packets and sends an error message to the traffic source.
**Blackhole** - Drops packets, but does not send an error message.

Examples:

```
set ipv6 static-route 3100:192::0/64 nexthop reject
```

or

```
set ipv6 static-route 3100:192::0/64 nexthop blackhole
```

### To delete a route and all related paths, run:

```
set ipv6 static-route <Destination> off
```

**Destination** - Destination IP address.

Example:

```
set ipv6 static-route 3100:192::0/64 off
```

### To delete a path only, run:

```
set static-route <Destination> nexthop gateway <GW IP> off
```

**Destination** - Destination IP address.
**GW IP** - Next hop gateway IP address or interface name.

DRAFT

Example:

```
set ipv6 static-route 3100:192::0/64 nexthop gateway 3900:172::1 off
```

DRAFT

Chapter 6

# System Management

This chapter describes the system management options

In This Chapter

## Time

Synchronized clock times are very important for a variety of purposes, such as:

- Distributed applications that require time synchronization.
- Analyzing event logs from different devices.
- Ensuring cron jobs run at the correct time.
- Ensuring that applications that use system time to validate certificates find the correct time. For example:  in audit logs, network devices time stamps must be synchronized to about a second, to correlate events.

You can set the system time and date:

- Manually
- From a time server, using Network Time Protocol (NTP)

### NTP

Network Time Protocol (NTP) is an Internet standard protocol used to synchronize the clocks of computers in a network to the millisecond. Synchronized clock times are very important for distributed applications that require time synchronization, such as cluster member synchronization, and for:

- Analyzing event logs from different devices.
- Ensuring cron jobs run at the correct time.
- Ensuring that applications that use system time to validate certificates find the correct time.

NTP runs as a continuous background client program on a computer. It sends periodic time requests to the servers you configure, obtains server time stamps, and uses them to adjust the client's clock. It is recommended to configure more than one server for redundancy.

## Configuring Network Time Protocol - WebUI

### To configure NTP

1. In the tree view, click **System Management** > **Time**.

   The **Time and Date Settings** window opens.

2. Click **Set Time and Date**.

DRAFT

The **Time and Date Settings** window opens.

3. Select **Set Time and Date automatically using Network Time Protocol (NTP)**.
4. Optionally, enter the **Primary NTP server** and the **Secondary NTP server**.
5. Click **OK**.

### To show and manually set the system time and date:

1. In the tree view, click **System Management** > **Time**.
2. Click **Set Time and Date**.

   The **Time and Date Settings** window opens.
3. Select **Set Time and Date manually.**
4. Enter the Time and Date in their related fields.
5. Click **OK**.

### To show and manually set the time zone:

1. In the tree view, click **System Management** > **Time**.
2. Below Time Zone, click **Set Time Zone**. The **Time zone Settings** window opens.
3. Select the time zone from the drop down list.
4. Click **OK**.

# Configuring NTP

## NTP

**Description**

Use this command to configure Network Time Protocol (NTP)

**Syntax**

To monitor and troubleshoot your NTP implementation:

```
show ntp active
show ntp current
show ntp servers
```

To add a new NTP server:

```
set ntp active VALUE
set ntp server primary VALUE version VALUE
set ntp server secondary VALUE version VALUE
```

To delete an NTP server:

```
delete ntp server VALUE
```

**Parameters**

| Parameter | Description |
|---|---|
| `active` | On to activate the NTP server. Off to deactivate. |
| `current` | The IP address of the NTP server you are using. |
| `primary` | The IP address of the primary NTP server. |
| `secondary` | The IP address of the secondary NTP server. |
| `version` | The version number of the NTP server. |
| `server` | The IP address of the NTP server. |

**Return Value**

**Example**

```
show ntp servers
```

**Output**

```
IP Address                Type                  Version
pool.ntp.org              Primary               4
```

DRAFT

**Comments**

Server-Specifies the IP address of the time server from which your system synchronizes its clock. The specified time server does **not** synchronize to the local clock of your system.

Version-The version number Specifies which version of NTP to run. Check Point recommends that you run version 3.

## Time

**Description**

Show and set the system time in HH:MM:SS format

**Syntax**

To set the time:

```
set time VALUE
```

To show the time

```
show time
```

**Parameters**

| Parameter | Description |
|---|---|
| `VALUE` | The current system time in HH:MM:SS format |

**Example**

```
show time
```

**Output**

```
12:03:54
```

## Clock

**Description**

Show current system date and time

**Syntax**

To show the clock

```
show clock
```

**Parameters**

| Parameter | Description |
|---|---|
| `clock` | The current system day, date, and time. The current system time is in HH:MM:SS format. |

**Example**

```
show clock
```

**Output**

```
Thu Oct  6 15:20:00 2011 IST
```

## Time Zone

**Description**

Show and Set the system time zone in the format AREA / REGION

**Syntax**

To set the time zone

```
set timezone VALUE / VALUE
```

To show the time zone

```
show timezone
```

**Parameters**

| Parameter | Description |
|---|---|
| `VALUE / VALUE` | The time zone in the format AREA / REGION<br>AREA is a geographic area, such as Asia<br>REGION is a region inside a specific area, such as Jerusalem.<br>Use TAB to list available values. |

DRAFT

**Description** Show and Set the system time zone in the format AREA / REGION

**Example**

```
Set Time Zone America /Detroit
```

## Date

**Description** Show and Set the system date

**Syntax** To set the date

```
set date VALUE
```

To show the date

```
show date
```

**Parameters**

| Parameter | Description |
|---|---|
| VALUE | The date in the YYYY-MM-DD format. |

**Example**

```
set date 2012-08-10
```

DRAFT

# SNMP

Through the SNMP protocol, network management applications can query a management agent using a supported MIB. The Check Point SNMP implementation lets an SNMP manager monitor the system and modify selected objects only. You can define and change one read-only community string and one read-write community string. You can set, add, and delete trap receivers and enable or disable various traps. You can also enter the location and contact strings for the system.

For more detailed information about the MIBs that the Check Point implementation supports, download a PDF version of the online documentation from the Check Point support site at http://support.checkpoint.com (http://support.checkpoint.com\n - http://support.checkpoint.com\n). To view detailed information about each supported MIB, go to the `/etc/snmp/mibs` directory.

The Check Point implementation also supports the User-based Security model (USM) portion of SNMPv3.

Simple Network Management Protocol (SNMP) is an Internet standard protocol. SNMP is used to send and receive management information to other network devices. SNMP sends messages, called protocol data units (PDUs), to different network parts. SNMP-compliant devices, called agents, keep data about themselves in Management Information Bases (MIBs) and resend this data to the SNMP requesters.

<tp_gaia> implemention of SNMP is built on UCD-SNMP 4.0.1. Changes have been made to the first version to address security and other fixes. For more information, see Net-SNMP (http://www.net-snmp.org - http://www.net-snmp.org).

**Warning** - If you use SNMP, it is recommended that you change the community strings for security purposes. If you do not use SNMP, disable the community strings.

SNMP, as implemented on Check Point platforms, supports:

- GetRequest, GetNextRequest, GetBulkRequest, and a select number of traps. The Check Point implementation also supports SetRequest for three attributes only: sysContact,sysLocation, and sysName. You must configure a read-write community string for set operations to work.
- SNMP v1, v2, and v3. For more information about SNMP v3, see Managing SNMP Users.

  **Note** - The Check Point implementation of SNMPv3 does not yet support SNMPv3 traps.

- Other public and proprietary MIBs.

| MIB | Source | Function |
|---|---|---|
| Rate-Shape MIB | proprietary | Monitoring rate-shaping statistics and configuration. Monitoring system-specific parameters. |
| Gaia System MIB | proprietary | Defines the system MIB for Gaia. The Gaia chassis temperature, fan group, and power-supply group function only on certain firewalls. |
| Gaia Registration MIB | proprietary | Defines the object ID (OID) prefixes. |
| OID Registration MIB | proprietary | Defines the object ID (OID) prefixes. |
| Unit Types MIB | proprietary | Contains OID values for the different types of circuit cards used in Check Point equipment. |
| TCP MIB | RFC 2012 | Provides management information of TCP implementations. |
| EtherLike MIB | RFC 1650 | Generic objects for Ethernet-like network interfaces. |
| Host Resources MIB | RFC 1514 | Provides information about the system, such as hardware, software, processes, CPU utilization, disk utilization, and so on. |

DRAFT

| MIB | Source | Function |
|---|---|---|
| IANAifType MIB | IANA | Defines the IANAifType textual convention, including the values of the ifType object defined in the MIB-II ifTable. |
| IF MIB | RFC 2233 | Describes generic objects for network interface sublayers |
| IP MIB | RFC 2011 | Provides management information for IP and ICMP implementations. |
| IP Forwarding MIB | RFC 2096 | Displays CIDR multipath IP routes. |
| ISDN MIB | RFC 2127 | Describes the management of ISDN interfaces.<br>**Note**: The isdnMibCallInformation trap is not supported by Gaia. |
| VRRP MIB | RFC 2787 | Provides dynamic failover statistics. |
| RIP MIB | RFC 1724 | Describes RIP version 2 protocol. |
| SNMP Framework MIB | RFC 2571 | Outlines SNMP management architecture. |
| SNMP MPD MIB | RFC 2572 | Provides message processing and dispatching. |
| SNMP User-based SM MIB | RFC 2574 | Provides management information definitions for SNMP User-based Security Model |
| SNMPv2 MIB | RFC 1907 | Defines SNMPv2 entities.<br>**Note:** The warmStart trap is not supported. |
| SNMPv2 SMI | RFC 2578 | |
| SNMPv2 TC | RFC 854 | Defines textual conventions for various values reported in OIDs and Traps. |
| Dial-Control MIB | RFC 2128 | Describes peer information for demand access and other kinds of interfaces.<br>**Note:** Gaia does not support the dialCtlPeerCallInformation and dialCtlPeerCallSetup traps. |
| Entity MIB | RFC 2737 | Represents the multiple logical entities that a single SNMP agent supports.<br>Gaia does not support the entConfigChange trap. |
| Tunnel-MIB | RFC 2667 | Provides statistics about IP tunnels. |
| UDP-MIB | RFC 2013 | Provides statistics about UDP implementations. |
| Frame Relay DTE MIB | RFC 2115 | Keeps statistics and errors in one or more circuits of a device implementing Frame Relay. |
| Token Ring MIB | RFC 1748 | |
| Check Point MIB | proprietary | Statistics and version information on any firewalls currently installed. |
| 1213 MIB | RFC 1213 | Contains the original definition of MIB-II. Check Point provides this MIB with the system to ensure backwards compatibility with SNMP v1. |

DRAFT

| MIB | Source | Function |
|---|---|---|
| Gaia-LBCluster-MIB | proprietary | Provides information about Gaia load- balancing systems. |
| HWM MIB | proprietary | Contains hardware management information.<br>**Note:** Gaia does not send the traps that this MIB supports when the Check Point platform is used as an IP security device. |
| Nokia Common MIB OID Registration MIB | proprietary | |
| Nokia Common NE Role MIB | proprietary | |
| Nokia Enhanced SNMP Solution Suite Alarm IRP MIB | proprietary | **Note**: Gaia does not send traps that this MIB supports when the Check Point platform is used as an IP security device. |
| Nokia Enhanced SNMP Solution Suite Common Definition MIB | proprietary | **Note**: Gaia does not send traps that this MIB supports when the Check Point platform is used as an IP security device. |
| Nokia Enhanced SNMP Solution Suite PM Common Definition MIB | proprietary | |
| Nokia Enhanced SNMP Solution Suite PM IRP MIB | proprietary | **Note:** Gaia does not send traps that this MIB supports when the Check Point platform is used as an IP security device. |
| Nokia NE3S Registration MIB | proprietary | |
| Nokia Link Aggregation MIB | proprietary | Contains the traps required for managing link aggregation. |
| Nokia NTP MIB | proprietary | |
| SNMPv2-CONF | | Gaia does not support this MIB but it is included for those customers who need it to enable their management tools. This MIB resides in the /etc/snmp/mibs/unsupported directory. |

DRAFT

The proprietary MIBs and the public MIBs are supplied with the system. To see more detailed information about the MIBs, see the `/etc/snmp/mibs` directory.

**Note** - The SNMPv2-CONF MIB resides in the `/etc/snmp/mibs/unsupported` directory.

The SNMP agent implemented in <tp_gaia> enables an SNMP manager to monitor the device and to change the sysName, sysContact, and sysLocation objects only.

**Note** - If you select the Disable checkbox, all community strings are disabled and SNMPv1 and v2 do not function. This has the same effect as selecting only SNMPv3 in the earlier step.

Use Gaia to run these tasks:

- Define and change one read-only community string.
- Define and change one read-write community string.

- Enable and disable the SNMP daemon.
- Create SNMP users.
- Change SNMP user accounts.
- Add or delete trap receivers.
- Enable or disable the various traps.
- Enter the location and contact strings for the device.

# SNMP Proxy Support for Check Point MIB

Gaia supports the use of a proxy for SNMP GetRequest and SNMP GetNextRequest for Check Point objects. These are guidelines and limitations you must be aware of.

## *Using the Check Point MIB*

You must use the Check Point version of the Check Point MIB (CP-MIB) text file in `$FWDIR/lib/snmp` of your network management tool.

Whenever Gaia SNMPd starts or restarts, it searches for the CheckPoint-MIB.txt. This is an example of a message you may see as a result of the search:

```
IP650 [admin]# Jan 31 12:17:19 IP650 [LOG_ERR] snmpd: Cannot find module
(CheckPoint-MIB) : At line 1 in (none)
```

You can ignore this message.

**Note** - Any SNMP requests to the CP-MIB when the Check Point SNMPd (CP-SNMPd) is not running, time out (the Gaia SNMPd does not respond).

The SNMP Proxy support is hard-coded to work only with the CP-SNMPd. It is not a generic proxy that you can use to access other MIBs. If you change these default configurations, the SNMP Proxy for the CP-MIB does not work:

- CP-SNMPd must continue to run on port 260.
- CP-SNMPd must continue to accept SNMPv1 and have a read community set to **public**.
- CP-SNMPd must continue to be accessible through *localhost* on the Check Point Gaia device.

The SNMP Proxy is not a trap proxy and only proxies SNMP Get and SNMP GetNext requests.

When simultaneous SNMP queries arrive, the SNMP Proxy returns valid values to only one request.

Because Gaia uses a proxy to support the Check Point MIB, refer to the Check Point documentation for any limitations on the CP-SNMPd.

Where does this reference point to?

# Configuring SNMP - WebUI

### Enable SNMP

The SNMP daemon is enabled by default. If you choose to use SNMP, configure it according to your security requirements. At minimum, you must change the default community string to something other than public. It is also advised to select SNMPv3, rather than the default v1/v2/v3, if your management station supports it.

**Note** - If you do not plan to use SNMP to manage the network, disable it. Enabling SNMP opens potential attack vectors for surveillance activity. It lets an attacker learn about the configuration of the device and the network.

You can choose to use all versions of SNMP (v1, v2, and v3) on your system, or to grant SNMPv3 access only. If your management station supports v3, select to use only v3 on your Gaia system. SNMPv3 limits community access. Only requests from users with enabled SNMPv3 access are allowed, and all other requests are rejected.

DRAFT

### To Enable SNMP:

1. In the tree view, click **System Management** > **SNMP**.
2. Select Enable SNMP Agent.

   **Warning** - You must start the Check Point SNMP daemon after you start the Check Point Security Gateway services. If you start the Check Point SNMP daemon before you start Security Gateway services, the Gaia daemon does not start.

3. In **Version** drop down list, select the version of SNMP to run:
   - **1/v2/v3 (any)**

     Select this option if your management station does not support SNMPv3.

   - **v3-Only**

     Select this option if your management station supports v3. SNMPv3 provides a higher level of security than v1 or v2.

4. In **SNMP Location String**, enter a string that contains the location for the system. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `Bldg 1, Floor 3, WAN Lab, Fast Networks, Speedy, CA`
5. In **SNMP Contact String**, enter a string that contains the contact information for the device. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `John Doe, Network Administrator, (111) 222-3333`
6. Click **Apply**.

## SNMP Agent Address

An agent address is a specified IP address at which the SNMP agent listens and reacts to requests. The default behavior is for the SNMP agent to listen to and react to requests on all interfaces. If you specify one or more agent addresses, the system SNMP agent listens and responds only on those interfaces.

You can use the agent address as a different method to limit SNMP access. For example: you can limit SNMP access to one secure internal network that uses a specified interface. Configure that interface as the only agent address.

### To Set an SNMP Agent Address:

1. In the tree view, click **System Management** > **SNMP**.
2. The SNMP Addresses table shows the applicable interfaces and their IP addresses. Select the header row checkbox to select all or select individual interfaces.

   **Note** - If no agent addresses are specified, the SNMP protocol responds to requests from all interfaces.

## Version Settings

### To Configure the Chosen Version:

#### V1/V2 Settings

1. In **Read Only Community String**, set a string other than **public**. This is a basic security precaution that you must always use.
2. (Optional). Set a **Read-Write Community String**.

   **Warning** - Set a read-write community string only if you have reason to enable set operations, and if your network is secure.

#### V3 - User-Based Security Model (USM)

Gaia supports the user-based security model (USM) component of SNMPv3 to supply message-level security. With USM (described in RFC 3414), access to the SNMP service is controlled on the basis of user identities. Each user has a name, an authentication pass phrase (used for identifying the user), and an optional privacy pass phrase (used for protection against disclosure of SNMP message payloads).

The system uses the MD5 hashing algorithm to supply authentication and integrity protection and DES to supply encryption (privacy). It is recommended to use authentication and encryption. You can use them independently by specifying one or the other with your SNMP manager requests. The Gaia system responds accordingly.

DRAFT

**Note** - Check Point systems do not protect traps with authentication or encryption.

SNMP users are maintained separately from system users. You can create SNMP user accounts with the same names as existing user accounts or different. You can create SNMP user accounts that have no corresponding system account. When you delete a system user account, you must separately delete the SNMP user account.

### To Add a USM User:

1. In the tree view, click **System Management** > **SNMP**.
2. Below V3 - User-Based Security Model (USM), click **Add**. The **Add New USM User** window opens.
3. In **User Name**, The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access.
4. In **Security Level,** Select from the drop down lost:
   - **authPriv**—The user has authentication and privacy pass phrases and can connect with or without privacy encryption.
   - **authNoPriv**—The user has only an authentication pass phrase and can connect only without privacy encryption.
5. In **Authentication Pass Phrase**, enter a password for the user that is between 8 and 128 characters in length.
6. In **Privacy Pass Phrase**, enter a pass phrase that is between 8 and 128 characters in length. Used for protection against disclosure of SNMP message payloads.
7. Click **Save**. The new user shows in the table.

### To delete a USM user

1. In the tree view, click **System Management** > **SNMP**.
2. Below V3 - User-Based Security Model (USM), select the user and click **Remove**. The **Deleting USM User Entry** window opens.
3. The window shows this message: **Are you sure you want to delete "username" entry?** Click **Yes**.

### To Edit a USM User:

1. In the tree view, click **System Management** > **SNMP**.
2. Below V3 - User-Based Security Model (USM), select the user and click **Edit**. The **Edit USM User** window opens.
3. In the window you can change the security level, the authentication passphrase, or the privacy pass phrase.
4. Click **Save**.

## SNMP Traps

Managed devices use trap messages to report events to the network management station (NMS). When some types of events occur, the platform sends a trap to the management station.

Traps are defined in text files located in the `/etc/snmp/mibs` directory:

- System traps are defined in the Nokia-IPSO-System-MIB.
- The ifLinkUpDown trap is defined in the IF-MIB.
- Clustering traps are defined in the Nokia-IPSO-LBCluster-MIB.
- Disk mirror traps are defined in the Nokia-IPSO-System-MIB.

Below is a list of the objects related to individual traps:

- The systemTrapConfigurationChange, systemTrapConfigurationFileChange, and systemTrapConfigurationSaveChange traps are related to the GaiaConfigGroup objects. These objects include GaiaConfigIndex, GaiaConfigFilePath, GaiaConfigFileDateAndTime, GaiaConfigLogSize, GaiaConfigLogIndex, and GaiaConfigLogDescr.
- The systemTrapDiskMirrorSetCreate, systemTrapDiskMirrorSetDelete, systemTrapDiskMirrorSyncFailure, and systemTrapDiskMirrorSyncSuccess traps are related to the GaiaDiskMirrorGroup objects. These objects include GaiaTotalDiskMirrorSets, GaiaMirrorSetIndex, GaiaMirrorSetSourceDrive, GaiaMirrorSetDestinationDrive, and GaiaMirrorSetSyncPercent.
- The linkUp and linkDown traps are related to the ifIndex, ifAdminStatus, and ifOperStatus objects.

DRAFT

Types of SNMPv1 and SNMPv2 traps which Gaia supports.

**Note** - The Check Point implementation of SNMPv3 does not yet support SNMPv3 traps.

| Type of Trap | Description |
|---|---|
| coldStart | Notifies when the SNMPv2 agent is re-initialized. |
| linkUp/ linkDown | Notifies when one of the links, which is administratively up, comes up or is lost. |
| lamemberActive | Notifies when a port is added to a link aggregation group. |
| lamemberInactive | Notifies when a port is removed from a link aggregation group. |
| Authorization | Notifies when an SNMP operation is not properly authenticated.<br>Although all implementation of SNMPv2 must be able to generate this trap, the snmpEnableAuthenTraps object indicates if this trap is generated. |
| vrrpTrapNewMaster | Notifies when a new VRRP master is elected. |
| vrrpTrapAuthFailure | Notifies when a VRRP hello message is not properly authenticated. |
| systemTrapConfigurationChange | Notifies when a change to the system configuration is applied. |
| systemTrapConfigurationFileChange | Notifies when a different configuration file is selected. |
| systemTrapConfigurationSaveChange | Notifies when a permanent change to the system configuration occurs. |
| systemTrapLowDiskSpace | Notifies when space on the system disk is low.<br>This trap is sent if the disk space utilization has reached 80 percent or more of its capacity. If this situation persists, a subsequent trap is sent after 15 minutes. |
| systemTrapNoDiskSpace | Notifies when the system disk is full.<br>This trap is sent if 2 percent or less of the disk space remains available, or if the remaining disk space is equal to or less than 1 MB. If this situation persists, a subsequent trap is sent after 15 minutes. |
| systemTrapDiskFailure | Notifies when a particular disk drive fails.<br>**Note** - The systemTrapDiskFailure applies only to Check Point platforms that support disk mirroring. |
| systemTrapDiskMirrorSetCreate | Notifies when a system disk mirror set is created. |
| systemTrapMirrorSetDelete | Notifies when a system disk mirror set is deleted. |

DRAFT

| | |
|---|---|
| systemTrapDiskMirrorSyncSuccess | Notifies when a system disk mirror set is successfully synced. |
| systemTrapDiskMirrorSyncFailure | Notifies when a system disk mirror set fails during syncing.<br>**Note -** The disk mirror traps are supported only on systems where disk mirroring is supported. |
| clusterMemberReject | Notifies when a member request to join a cluster is rejected. |
| clusterMemberJoin | Notifies when a member node joins the cluster. |
| clusterMemberLeft | Notifies when a member node leaves the cluster. |
| clusterNewMaster | Notifies when a cluster is formed and a new master is elected. |
| clusterProtocolInterfaceChange | Notifies when a failover occurs from the primary cluster network to the secondary cluster network. |
| systemPowerSupplyFailure | Notifies when a power supply for the system fails.<br>This trap includes the power supply index and is supported only on platforms with two power supplies installed and run. |
| systemFanFailure | Notifies when a CPU or chassis fan fails. This trap includes the fan index. |
| SystemOverTemperature | Notifies when a power supply failure occurs because of high temperature.<br>This trap is followed by a power supply failure trap that specifies the power supply index that failed. The power supply failure trap is supported only on platforms with two power supplies installed and run. |
| systemSnmpProcessShutdown | Notifies when the status of the SNMP daemon is changed, turned off or turned on. |

DRAFT

### To Enable or Disable trap Types:

1. In the tree view, click **System Managemen**t > **SNMP**.
2. Below Enabled Traps, click **Set**. The **Add New Trap Receiver** window opens.
3. Select from the **Disabled Traps** list, and click **Add>** to set as Enabled Trap.
4. To disable, select from the **Enabled Traps** list, and click **Remove>** to Disable Trap.
5. Click **Save**.
6. In Trap User, select an SNMP user from the drop down list.
7. In **Polling Frequency**, enter or use the arrows to select the number of seconds between polls.
8. Click **Apply**.

### To Configure Trap Receivers (management stations):

1. In the tree view, click **System Managemen**t > **SNMP**.
2. Below Trap Receivers Settings, click **Add**. The **Add New Trap Receiver** window opens.
3. In **IPv4 Address**, enter the IP address (or the hostname if DNS is set) of a receiver.
4. In **Version**, Select the Trap SNMP Version for the trap receiver from the drop down menu.
5. In **Community String**, enter the community string for the specified receiver.

6. Click **Save**.

### To Edit Trap Receivers:

1. In the tree view, click **System Managemen**t > **SNMP**.
2. Below Trap Receivers Settings, select the trap and click **Edit**. The **Edit Trap Receiver** window opens.
3. You can change the Version or the community string.
4. Click **Save**.

### To Delete Trap Receivers:

1. In the tree view, click **System Managemen**t > **SNMP**.
2. Below Trap Receivers Settings, select the trap and click **Remove**. The **Deleting Trap Receiver Entry** window opens.
3. The window shows this message: **Are you sure you want to delete "IPv4 address" entry?** Click **Yes**.

# Configuring SNMP - CLI (snmp)

This section is taken as-is from the IPSO CLI Guide

**Description** Use These commands to configure SNMP

DRAFT

**Description** Use These commands to configure SNMP

**Syntax**

**Enable SNMP**

Set Commands:

```
set snmp agent VALUE
set snmp agent-version VALUE
set snmp location VALUE
set snmp contact VALUE
```

Show Commands:

```
show snmp agent
show snmp agent-version
show snmp location
show snmp contact
```

Delete Commands:

```
delete snmp location
delete snmp contact
```

**SNMP Agent Address**

Add commands:

```
add snmp address VALUE
```

Set Commands:

```
set snmp community VALUE read-only
set snmp community VALUE read-write
```

Show Commands:

```
show snmp address
show snmp community
```

Delete Commands:

```
delete snmp address VALUE
delete snmp community VALUE
```

**Version Settings**

Add Commands:

```
add snmp usm user VALUE security-level authNoPriv
auth-pass-phrase VALUE
add snmp usm user VALUE security-level authNoPriv
auth-pass-phrase-hashed VALUE
add snmp usm user VALUE security-level authPriv
auth-pass-phrase VALUE privacy-pass-phrase VALUE
add snmp usm user VALUE security-level authPriv
auth-pass-phrase VALUE privacy-pass-phrase-hashed
VALUE
add snmp usm user VALUE security-level authPriv
auth-pass-phrase-hashed VALUE privacy-pass-phrase-
hashed VALUE
add snmp usm user VALUE security-level authPriv
auth-pass-phrase-hashed VALUE privacy-pass-phrase
VALUE
```

Set Commands:

```
set snmp usm user VALUE security-level authNoPriv
auth-pass-phrase VALUE
set snmp usm user VALUE security-level authPriv
auth-pass-phrase VALUE privacy-pass-phrase VALUE
set snmp usm user VALUE security-level authPriv
privacy-pass-phrase VALUE auth-pass-phrase VALUE
```

Show Commands:

```
show snmp usm user VALUE
show snmp usm users
```

Delete Commands:

DRAFT

**Description** Use These commands to configure SNMP

**Parameters**

| Parameter | Description |
|---|---|
| `snmp agent` | `on` or `off` to enable or disable. |
| `snmp agent-version` | `any` or `v3-Only` |
| `location` | In SNMP Location String, enter a string that contains the location for the system. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `Bldg 1, Floor 3, WAN Lab, Fast Networks, Speedy, CA` |
| `contact` | In SNMP Contact String, enter a string that contains the contact information for the device. The maximum length for the string is 128 characters. That includes letters, numbers, spaces, special characters. For example: `John Doe, Network Administrator, (111) 222-3333` |
| `snmp address` | An interface IP address. If you do not select one at which the SNMP Agent listens and responds to requests, it responds to requests from all interfaces. |
| `community VALUE read-only` | Set a string. This is a basic security precaution. The default is **public**. |
| `community VALUE read-write` | Set a string (optional). |
| `usm user` | The range is 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters. This can be the same as a user name for system access. |
| `authNoPriv` | The user has only an authentication pass phrase and can connect only without privacy encryption. |
| `authPriv` | The user has authentication and privacy pass phrases and can connect with or without privacy encryption. |
| `auth-pass-phrase` | A password for the user that is between 8 and 128 characters in length. |
| `auth-pass-phrase-hashed` | A hashed password for the user that is between 8 and 128 characters in length. |
| `privacy-pass-phrase` | A pass phrase that is between 8 and 128 characters in length. Used for protection against disclosure of SNMP message payloads. |
| `usm users` | All USM users |
| `traps receiver` | IP address selected to receive traps sent by the agent. |
| `community` | Set a string |
| `traps trap` | The trap name |

**Description** Use These commands to configure SNMP

**Return Value**

**Example**

```
show snmp traps enabled-traps
```

**Output**

```
authorizationError
```

**Comments**

- CLI only displays the enabled traps. For all trap types, see table in Configuring SNMP - WebUI (on page 60).
- In pass phrase, notice the different options for regular and hashed pass phrase: `auth-pass-phrase` and `auth-pass-phrase-hashed`

# Interpreting Error Messages

This section lists and explains certain common error status values that can appear in SNMP messages. Within the PDU, the third field can include an error-status integer that refers to a specific problem. The integer zero (0) means that no errors were detected. When the error field is anything other than 0, the next field includes an error-index value that identifies the variable, or object, in the variable-bindings list that caused the error.

The following table lists the error status codes and their meanings.

| Error status code | Meaning | Error status code | Meaning |
|---|---|---|---|
| 0 | noError | 10 | wrongValue |
| 1 | tooBig | 11 | noCreation |
| 2 | NoSuchName | 12 | inconsistentValue |
| 3 | BadValue | 13 | resourceUnavailable |
| 4 | ReadOnly | 14 | commitFailed |
| 5 | genError | 15 | undoFailed |
| 6 | noAccess | 16 | authorizationError |
| 7 | wrongType | 17 | notWritable |
| 8 | wrongLength | 18 | inconsistentName |
| 9 | wrongEncoding | | |

**Note** - You might not see the codes. The SNMP manager or utility interprets the codes and displays and logs the appropriate message.

The subsequent, or fourth field, contains the error index when the error-status field is nonzero, that is, when the error-status field returns a value other than zero, which indicates that an error occurred. The error-index value identifies the variable, or object, in the variable-bindings list that caused the error. The first variable in the list has index 1, the second has index 2, and so on.

The next, or fifth field, is the variable-bindings field. It consists of a sequence of pairs; the first is the identifier. The second element is one of the following five: value, unSpecified, noSuchOjbect, noSuchInstance, and EndofMibView. The following table describes each element.

DRAFT

| Variable-bindings element | Description |
|---|---|
| value | Value associated with each object instance; specified in a PDU request. |
| unSpecified | A NULL value is used in retrieval requests. |
| noSuchObject | Indicates that the agent does not implement the object referred to by this object identifier |
| noSuchInstance | Indicates that this object does not exist for this operation. |
| endOfMIBView | Indicates an attempt to reference an object identifier that is beyond the end of the MIB at the agent. |

## GetRequest

The following table lists possible value field sets in the response PDU or error-status messages when performing a *GetRequest.*

| Value Field Set | Description |
|---|---|
| noSuchObject | If a variable does not have an *OBJECT IDENTIFIER* prefix that exactly matches the prefix of any variable accessible by this request, its value field is set to *noSuchObject*. |
| noSuchInstance | If the variable's name does not exactly match the name of a variable, its value field is set to *noSuchInstance*. |
| genErr | If the processing of a variable fails for any other reason, the responding entity returns *genErr* and a value in the error-index field that is the index of the problem object in the variable-bindings field. |
| tooBig | If the size of the message that encapsulates the generated response PDU exceeds a local limitation or the maximum message size of the request’s source party, then the response PDU is discarded and a new response PDU is constructed. The new response PDU has an error-status of *tooBig*, an *error-index* of zero, and an empty *variable-bindings* field. |

DRAFT

## GetNextRequest

The only values that can be returned as the second element in the variable-bindings field to a GetNextRequest when an error-status code occurs are unSpecified or endOfMibView.

## GetBulkRequest

The GetBulkRequest minimizes the number of protocol exchanges by letting an SNMPv2 manager request that the response be as large as possible given the constraints on the message size.

The GetBulkRequest PDU has two fields that do not appear in the other PDUs: non-repeaters and max-repetitions. The non-repeaters field specifies the number of variables in the variable-bindings list for which a single-lexicographic successor is to be returned. The max-repetitions field specifies the number of lexicographic successors to be returned for the remaining variables in the variable-bindings list.

If at any point in the process, a lexicographic successor does not exist, the endofMibView value is returned with the name of the last lexicographic successor, or, if there were no successors, the name of the variable in the request.

If the processing of a variable name fails for any reason other than endofMibView, no values are returned. Instead, the responding entity returns a response PDU with an error-status of genErr and a value in the error-index field that is the index of the problem object in the variable-bindings field.

# Job Scheduler

You can use WebUI to access cron and schedule regular jobs. The cron daemon runs jobs at dates and times you specify through this procedure.

## Configuring Job Scheduler - WebUI

### To schedule jobs:

1. In the tree view, click **System Management** > **Job Scheduler**.
2. Below Scheduled Jobs, click **Add**. The **Add A New Scheduled Job** window opens.
3. In **Job Name**, enter the name of the job. Use alphanumeric characters only, and no spaces.
4. In **command to Run**, enter the name of the command. The command must be a UNIX command.
5. Below **Schedule**, select the frequency (Daily, Weekly, or Monthly) for this job. Enter the time of day for this job, in the twenty four hour clock format.
6. Click **OK**. The job shows in the Scheduled Jobs table.
7. Below E-mail Notification, in Send jobs output to the following E-mail, enter the E-mail to receive the notifications.
8. Click **Apply**.

### To delete scheduled jobs

1. In the Overview tree, click **System Management** > **Job Scheduler**.
2. In the scheduled Jobs table, click the job to delete.
3. Click **Delete**. The **Are you sure you want to delete the selected job?** window opens.
4. Click **OK** to confirm, or **Cancel** to abort.

### To edit the scheduled jobs:

1. In the Overview tree, click **System Management** > **Job Scheduler**.
2. In the scheduled Jobs table, click the job that you want to edit.
3. Click **Edit**. The **Edit Scheduled Job** opens.
4. Enter the changes.
5. Click **Ok**.

## Configuring Job Scheduler - CLI (cron)

**Description** Use these commands to configure your system to schedule regular jobs. The cron daemon does jobs on the dates and times you specify.

DRAFT

**Description**

Use these commands to configure your system to schedule regular jobs. The cron daemon does jobs on the dates and times you specify.

**Syntax**

To add scheduled jobs:

```
add cron job VALUE command VALUE recurrence daily time VALUE
add cron job VALUE command VALUE recurrence monthly month
VALUE days VALUE time VALUE
add cron job VALUE command VALUE recurrence weekly days VALUE
time VALUE
```

To delete scheduled jobs:

```
delete cron all
delete cron job VALUE
delete cron mailto
```

To change existing scheduled jobs:

```
set cron job VALUE command VALUE
set cron job VALUE recurrence daily time VALUE
set cron job VALUE recurrence monthly month VALUE days VALUE
time VALUE
set cron job VALUE recurrence weekly days VALUE time VALUE
set cron mailto VALUE
```

To monitor and troubleshoot the job scheduler configuration:

```
show cron job VALUE command
show cron job VALUE recurrence
show cron jobs
show cron mailto
```

**Parameters**

| Parameter | Description |
|---|---|
| `job` | The name of the job. |
| `command` | The name of the command. |
| `recurrence daily time` | To specify a job for once a day, enter `recurrence daily`, and the time of day, in the twenty four hour clock format. For example: `14:00`. |
| `recurrence monthly month` | To specify a job for once a month, enter `recurrence monthly month`, and the specific months. Each month by number, and separate by commas. For example: for January through March, enter `1,2,3` |
| `days` | To specify the days, enter the day by number, when 0 is Sunday and 6 is Saturday. Separate several days with commas. For example: for Monday and Thursday enter `1,4` |
| `time` | To specify the time, enter the time in the twenty four hour clock format. For example: `14:00`. |
| `recurrence weekly days` | To specify a job for once a week, enter `recurrence weekly`, and the day by number, when 0 is Sunday and 6 is Saturday. |
| `mailto` | To specify a mail recipient, enter the email address. One email address per command. |

**Example**

```
show cron job myjob recurrence
```

**Description** Use these commands to configure your system to schedule regular jobs. The cron daemon does jobs on the dates and times you specify.

**Output**

```
Every week on Sunday, Wednesday at 15:00
```

**Comments** Only Show commands provide an output.

# Mail Notification

Mail notifications (also known as Mail Relay) allow you to send email from the Security Gateway. You can send email interactively or from a script. The email is relayed to a mail hub that sends the email to the final recipient.

Mail notifications are used as an alerting mechanism when a Firewall rule is triggered. It is also used to email the results of cron jobs to the system administrator.

Gaia supports these mail notification features:

- Presence of a mail client or Mail User Agent (MUA) that can be used interactively or from a script.
- Presence of a Sendmail-like replacement that relays mail to a mail hub by using SMTP.
- Ability to specify the default recipient on the mail hub.

Gaia does not support these mail notification features:

- Support for incoming email.
- Support for mail transfer protocols other than outbound SMTP.
- Ability to telnet to port 25.
- Support for email accounts other than admin or monitor.

## Configuring Mail Notification - WebUI

**To configure mail notifications recipient:**

1. In the tree view, click **System Management** > **Mail Notification**.
2. In The **Mail Server** field, enter the server. For example:  mail.company.com
3. In the **User Name** field, enter the user name. For example:  user@mail.company.com
4. Click **Apply**.

## Configuring Mail Notification - CLI (mail-notification)

**Description** Use this group of commands to configure mail notifications.

**Syntax** To configure the mail server and user that receive the mail notifications:

```
set mail-notification server VALUE
set mail-notification username VALUE
```

To view the mail server and user configurations:

```
show mail-notification server
show mail-notification username
```

**Parameters**

| Parameter | Description |
|---|---|
| `server` | The IP address or hostname of the mail server to receive mail notifications. For example: mail.company.com |
| `username` | The username on the mail server that receives the admin or monitor mail notifications. For example:  user@mail.company.com |

DRAFT

**Description** Use this group of commands to configure mail notifications.

**Example**

```
show mail-notification server
```

**Output**

```
Mail notification server: mail.company.com
```

**Comments**

# Messages

When you connect to a Gaia system or log out, the message: **This system is for authorized use only** shows on the login page. You can change or disable this message on the Banner and message of the day Configuration page. You can also configure a Message of the Day that users see when they log in using the command line.

## Configuring Messages - WebUI

**To configure messages:**

1. In the tree view, click **System Management** > **Messages**.
2. To enter a Banner message, select Banner message.
3. To enter a Message of the day, select Message of the day.
4. Enter the messages.
5. Select or clear the message options.
6. Click **Apply**.

## Configuring Messages - CLI (message)

**Description**

**Syntax**

```
set message banner VALUE [ msgvalue VALUE ]
set message motd VALUE [ msgvalue VALUE ]
show message all [ status ]
show message banner [ status ]
show message motd [ status ]
```

**Parameters**

| Parameter | Description |
|---|---|
| `message banner` | To enable the Message banner option, enter `on`. To disable this option, enter `off`. |
| `message motd` | To enable the Message of the day option, enter `on`. To disable it, enter `off`. |
| `message all status` | Shows the status of any type of message. |

**Example**

```
show message banner status
```

**Output**

```
Banner message on
```

**Comments**

- Do not enter the brackets in the commands. They mean that the content is optional, depending on the previous value.
- Message banner is the message users see when they connect to the system.
- Message of the day is the message users see when they log in to the system using the command line.

DRAFT

# Display Format

Placeholder

## Configuring Display Format - WebUI

Placeholder

## Configuring Display Format - CLI (format)

Placeholder

DRAFT

# Chapter 7

# Advanced Routing

Dynamic Routing is fully integrated into the WebUI and the command-line shell. The BGP, OSPF and RIP protocols are supported.

Dynamic Multicast Routing is supported, using the PIM (Sparse mode and Dense mode) and IGMP protocols.

To learn about dynamic routing, see the *Gaia Advanced Routing WebUI and CLI Guid*e.

DRAFT

# Chapter 8

# User Management

Intro.

Placeholder

In This Chapter

DRAFT

## Change My Password

You can change your own password. A user with privileges to the Users feature can change the passwords of user, admin, and monitor users.

⚠ **Warning** - Because a user with read and write permission to the Users feature can change the password of a user, or an admin user, you should be cautiously assign this permission.

### Configuring Change My Password - WebUI

**To change your current user password:**

1. In the tree view, click **User Management** > **Change My Password**.
2. In **Old Password**, enter your old password.
3. In **New Password** and in **Confirm New Password**, enter the new Password.
4. Click **Apply**.

### Configuring Change My Password - CLI (selfpasswd)

**Description**

Use these commands to change the password for admin and monitor. Admin and Monitor are default users. Typically, you set the initial passwords for admin and monitor at system startup.

**Syntax**

```
set selfpasswd
set selfpasswd oldpass VALUE passwd VALUE
```

**Parameters**

| Parameter | Description |
|---|---|
| `selfpasswd oldpass` | Your current password. |
| `passwd` | The new password you want. |

# Users

Use the WebUI and CLI to manage user accounts. You can:

- Add users to your Gaia system.
- Edit the home directory of the user.
- Edit the default shell for a user.
- Give a password to a user.
- Give privileges to users.

These users are created by default and cannot be deleted:

- **admin** — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user has a User ID of 0, and therefore has all of the privileges of a root user.
- **monitor** — Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.

When you add a new user, the user is given read-only privileges to the WebUI and CLI by default. However, the user must be assigned one or more roles before they can log in.

**Note** - You can assign permissions to all Gaia features or a subset of the features without assigning a user ID of 0. If you assign a user ID of 0 to a user account (you can do this only in the CLI), the user is equivalent to the Admin user and the roles assigned to that account cannot be modified.

When you create a user you can add pre-defined roles (privileges) to the user. For more information, see "Role-Based Administration" ("Roles" on page 80).

DRAFT

## Managing User Accounts - WebUI

### To see a list of all users

Choose **User Management > Users** in the navigation tree.

You can also see the user name that you used to log in with in the toolbar of the WebUI.

### To add a user

1. Open the **User Management > Users** page.
2. Click **Add**
3. In the **Add User** page, enter the following:
   - **Login Name -** (1–31 characters),
   - **Home Directory -** for the new user. Must be subdirectory of `/home`
   - **Password**.
   - **Confirm Password**
4. Click **OK**

### To delete a user

1. Open the **User Management > Users** page.
2. Select the User
3. Click **Delete**.

### *User Account Fields- WebUI*

| Item | Description |
|---|---|
| Login Name | Name used to identify the user. The valid characters are alphanumeric characters, dash (-), and underscore (_).<br>**Range:** 1-32 characters |

| Item | Description |
|---|---|
| Real Name | User's real name or other informative label. |
| Home directory | This is the full Linux path name of a directory where the user will log in. The home directory for all users must be in /home. |
| Shell | • `/etc/cli.sh` - User is allowed to use the full Gaia CLI (clish). This is the default option. By default, some basic networking commands (such as `ping`) are also available. The *Extended Commands mechanism* makes it possible to add Linux commands that can be used.<br>User can run `shell` to enter the `bash` shell.<br>• `/bin/bash, /bin/csh, /bin/sh, /bin/tcsh` - Standard Linux shells.<br>User can run `clish` to enter the clish shell.<br>• `/usr/bin/scponly` - User is allowed to log in only using SCP, and to trasfer files to and from the system. No other commands are allowed.<br>• `/sbin/nologin` - User is not allowed to log in. |
| Reset Password | Change the user password.<br>**Important** - After resetting the password, tell the user to immediately change their password in **User Management > Change My Password**. |
| Password | Use this field to enter a new password if you are changing it.<br>**Range:** 6-128 characters. All printable characters are allowed.<br>**Note -** If you use an asterisk (*) in a password, users with that password are unable to log in. |
| Confirm Password | Re-enter the new password if you are changing it. |
| Access Mechanisms | Choose whether the user is able to access Gaia from the command line, from the WebUI, both, or neither. |
| Roles | Assign a role to the user. Define the roles in **User Management > Roles**. |

DRAFT

# Managing User Accounts - CLI (user)

**Description** Use these commands to add new users and to set and change user passwords, user ID, group ID, home directory, and default shell.

**Syntax**

To view configuration and conditions:

```
show users
show user VALUE gid
show user VALUE homedir
show user VALUE realname
show user VALUE shell
show user VALUE uid
```

To delete an existing user:

```
delete user VALUE
```

To add user accounts:

```
add user VALUE uid VALUE homedir VALUE
```

To modify user accounts:

```
set user VALUE newpass VALUE
set user VALUE password
set user VALUE password-hash VALUE
set user VALUE {realname VALUE uid VALUE gid VALUE homedir
VALUE shell VALUE}
```

**Comments**

You can use the `add user` command to add new users, but you must use the `set user name passwd` command to set the password and allow the user to log on to the system.

For information on removing access mechanism permissions from a user, see the `delete rba user` command.

DRAFT

**Parameters**

| Parameter | Description |
|---|---|
| `user` *VALUE* | Specifies the new user name or an existing user name. The valid characters are alphanumeric characters, dash (-), and underscore (_). Range: 1-32 characters |
| *password* | Starts a password change dialog. You will be asked to enter a new password for the user and then asked to verify it by re-entering it. The password you enter will not be visible on terminal. |
| `newpass VALUE` | Specifies a new password for the user. If you use this keyword to change the password, you will not be asked to verify the new password and the password you enter is visible on the terminal. |
| `uid VALUE` | Specifies the specified user's user ID (`0-65535`), which is used to identify the user's permissions. |
| `gid VALUE` | Specifies the ID (`0-65535`) for the primary group to which a user belongs. Use the group management commands to specify membership in other groups. |
| `homedir VALUE` | Specifies the user's home directory, where the user is placed on login. Enter the full Linux path name. If the directory doesn't already exist, it is created. The home directory for all users must be in a directory under `/home`/. |
| `shell VALUE` | Specifies the user's shell, which is invoked when the user logs in. The default shell is /bin/csh. To change the shell, enter the new shell path name.<br>/etc/cli.sh  - User is allowed to use the full Gaia CLI (clish). This is the default option. By default, some basic networking commands (such as ping) are also available. The Extended Commands mechanism makes it possible to add Linux commands that can be used.<br>User can run shell to enter the bash shell.<br>/bin/bash, /bin/csh, /bin/sh, /bin/tcsh - Standard Linux shells.<br>User can run clish to enter the clish shell.<br>/usr/bin/scponly - User is allowed to log in only using SCP, and to  trasfer files to and from the system. No other commands are allowed.<br>/sbin/nologin  - User is not allowed to log in. |

# Roles

Role-based administration (RBA) lets Gaia administrators create and have separate roles. With RBA, an administrator can allow users to access features by including the features in a role and assigning the role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features. This feature also provides improved auditing capabilities.

When you add a new user, the user is given access rights to the WebUI **Overview** page and the CLI. The user cannot access other WebUI pages or run commands from the CLI. You must assign roles to the user to give more access privileges.

To assign a set of access permissions to a user, create a role that specifies administrative or monitoring access to the required features. You then assign this role to the relevant user.

You can also specify which access mechanisms (WebUI or the CLI) are available to the user when you edit the user.

**Note -** When users log in to the WebUI, the navigation tree displayed depends on the role or roles assigned to their user account. If the roles do not provide access to a feature, they will not see a link to the feature in the tree. If they have read-only access to a feature, they will see a link and be able to access the page, but all the controls will be disabled.

These roles are predefined on the system:

- **adminRole**—Gives the user read/write access to all features.
- **monitorRole**—Gives the user read-only access to all features.

**Note -** When you assign a role containing access to a feature to a user, the user gets access to the WebUI **Configuration** pages for that feature but not to the **Monitoring** pages for that feature. To provide access to the Monitoring pages, you must include the monitor privilege for that feature in the role definition.

# Configuring Roles - WebUI

Roles are defined in the **User Management > Roles** page of the WebUI.

### To see a list of existing roles

Choose **User Management > Roles** in the navigation tree.

### To add or edit a role

1. Choose **User Management > Roles** in the navigation tree.
2. Select one of the following:
3. To *add a role*, click **Add** and enter a **Role Name**. The role name can be a combination of letters and numbers, but it must start with a letter.

   To *edit a role*, select a Role and click **Edit**. You cannot edit the name of an existing role.

   **Important** - Because a user with read/write permission to the User Management feature can change the password of a user, including the admin user, be cautious in assigning roles that contain this permission.

4. Add features by selecting **Read/Write** or **Read-Only**.

   Remove features by selecting **None**.

### To delete a role

1. Choose **User Management > Roles** in the navigation tree.
2. Select the role to delete.
3. Click **Delete**.

   **Note -** You cannot delete the adminRole, or monitorRole default roles.

### To assign users to a role

1. Choose **User Management > Roles** in the navigation tree.
2. Click **Assign Members**.
3. Assign the users to the role.

### To assign roles and access mechanisms to a user

1. Choose **User Management > Users** in the navigation tree.
2. Select a user
3. Click **Edit**.
4. To assign roles: In the **Roles** section

DRAFT

- Add roles by moving them to the **Assigned** column.
- Remove Roles by moving them to the **Available** column.
- To select a range of roles press Shift-Click.
- To select multiple roles one at a time, select Ctrl-click.

5. To assign **Access Mechanisms**: Select **Command Line**, or **Web**, or the two of them.

If you select none of the two, the user cannotwill not be able to use the command line or the WebUI.

**Note** - When you assign a role containing access to a feature to a user, the user gets access to the WebUI **Configuration** pages for that feature but not to the **Monitoring** pages for that feature. To provide access to the Monitoring pages, you must include the monitor privilege for that feature in the role definition.

# Configuring Roles - CLI (rba)

DRAFT

**Description** Use these commands to

**Syntax**

What is the difference between the following?

```
show rba all
show rba roles
```

Unclear

```
show rba role VALUE
```

Unclear

```
show rba users
```

To show the roles assigned to a user

```
show rba user VALUE
```

To remove a feature from a role:

```
delete rba role VALUE {readonly-features VALUE readwrite-
features VALUE}
```

To remove privileges for access mechanisms from a user:

```
delete rba user VALUE access-mechanisms VALUE
```

To remove a role assignment from a user:

```
delete rba user VALUE roles VALUE
```

To add a role:

```
add rba role VALUE domain-type VALUE {readonly-features VALUE
readwrite-features VALUE}
add rba user VALUE access-mechanisms VALUE
add rba user VALUE roles VALUE
```

**Parameters**

| Parameter | Description |
|---|---|
| `all` | All roles |
| `role VALUE` | The name of the role. You can enter a comma separated list of roles. |
| `roles` | ? |
| `user VALUE` | The username of the user |
| `users` | ? |
| `{readonly-features VALUE readwrite-features VALUE}` | List of read-only features and the list of read-write features to add or delete. Separate each with a comma and do not use spaces. For a list of available features, use the tab completion in the CLI. |
| `access-mechanisms VALUE` | Assign users privilege to use WebUI or the CLI.<br>check this |
| `roles VALUE` | ? |
| `domain-type VALUE` | ? |

DRAFT

# Password Policy

One of the important elements of securing your Check Point network security platform is to set user passwords and create a good password policy. To create strong, unique passwords that use a variety of character types and to require password changes, are key factors to your overall network security.

These sections give information on how to configure your platform using the WebUI to:

- Enforce creation of strong passwords
- Push users to change passwords at regular intervals
- Monitor and prevent use of already used passwords

The features included in password and User Management make global and comprehensive passwords management possible. We recommend that you use the functions in password and account management to set and manage your user passwords and password policies.

The password policies you set with password and account management are sharable across a cluster.

None of the password and account management features apply to nonlocal users that authentication servers such as RADIUS manage their login information and passwords. Also, they do not apply to non-password authentication, such as the public key authentication supported by SSH.

To manage user passwords, see Change My Password (on page 76) and Managing User Accounts ("Users" on page 77).

## Password History Checks

The password history feature checks for the reuse of passwords and forces users to use a new password each time they change their password. The number of already used passwords that this feature checks against is defined by the history length.

The password history feature works in concert with the forced password change feature that requires users to use new passwords at defined intervals. Password history check is enabled by default.

The password history check applies to user passwords set by the administrator the same as passwords set by the user. The history check does not apply to SNMPv3 USM user pass phrases.

**Note** - The password history check does not apply to cluster administrator (cadmin) users. These users sometimes need to recreate cluster configurations and might want to reuse the original cluster administrator password when they do so.

These are considerations you might think of when you use this feature:

- The password history file for a user is updated only when the user successfully changes password. If you change the history length, for example:  from ten to five, the stored passwords number does not change. Next time the user changes password, the new password is examined against all stored passwords, maybe more than five. After the password change succeeds, the password file is updated to keep only the five most recent passwords.
- Passwords get into a user password history file only if the password history feature is enabled during password creation.
- This feature always checks the new password against the password from before, even if not in the password history file.

# Mandatory Password Change

Forcing users to change passwords regularly or to change their administrator-assigned password to their own is also important for a strong security policy. Using the WebUI, you can set user passwords to expire after a specified number of days. When a password expires, the user is forced to change the password the next time the user logs in. This feature works in conjunction with the password history check to get users to use new passwords at regular intervals.

You can also get an individual user to change password the next time the user logs in, independently of policies. To do so, use **Reset Password** in **User Management** > **Users**. Know that users with access to the User Management page can override a forced password change.

This feature does not apply to SNMPv3 USM user pass phrases.

**Note** - For mandatory password change to work, you must enable Check for password Reuse. To configure, see To configure password history check ("Configuring Password Policy- WebUI" on page 84).

In Voyager, you must also enable session management. Do you need to do this in Gaia? If so, how?

# Configuring Password Policy- WebUI

## To Configure Password strength:

1. In the tree view, click **User Management** > **Password policy**.
2. Below Password strength, in the **Minimum Password Length** field, enter the minimum number of characters to use in the password. The default is 6.

   **Note** - Does not apply to passwords that are already set.
3. You can select Disallow Palindromes (a sequence of letters, numbers, or characters that are read the same in each direction). In default, it is selected.
4. In Password Complexity, select the required number of character types. The default is two character types.
5. Click **Apply**.

## To configure password history check:

1. In the tree view, click **User Management** > **Password policy**.
2. Below Password History, select Check for Password Reuse to enable the password history check. In default, it is selected.
3. In the **History Length** field, enter a number from 1-1000. The default is 10. This value determines the number of former passwords to keep and examine against for each user.
4. Click **Apply**.

DRAFT

### To configure mandatory user password change

1. In the tree view, click **User Management** > **Password policy**.
2. Below Mandatory Password Change, in Password Expiration, select Passwords never expire or Password expire after (enter number) days. The default is Passwords never expire.

   **Note** - The range of days allowed to enter is 1-1827.

3. Click **Apply**.

# Configuring Password Policy- CLI (password-controls)

**Description**

Use these commands to set policies for managing user passwords and accounts. The features included in password and account management are a global and comprehensive way to manage password policy.

**Syntax**

To change password and account management configuration:

```
set password-controls complexity VALUE
set password-controls history-checking VALUE
set password-controls history-length VALUE
set password-controls min-password-length VALUE
set password-controls palindrome-check VALUE
set password-controls password-expiration VALUE
```

To view password and account management configuration:

```
show password-controls all
show password-controls complexity
show password-controls history-checking
show password-controls history-length
show password-controls min-password-length
show password-controls palindrome-check
show password-controls password-expiration
```

**Parameters**

| Parameter | Description |
|---|---|
| `complexity` | The required number of character types. The range is 1-4. The default is 2. |
| `history-checking` | On or Off. On enables the history check. |
| `history-length` | The number of past passwords to keep and check against for each user. The range is 1-1000. The default is 10. |
| `min-password-length` | The minimum number of characters of a password. Does not apply to passwords that have already been set. |
| `palindrome-check` | On or Off. On prevents passwords that are palindromes. The default is On. |
| `password-expiration` | The number of days in which a new password expires. The range is 1-1827. The default is never. When set to never, passwords do not expire. Does not apply to SNMP users. |

**Example**

```
show password-controls all
```

**Description** Use these commands to set policies for managing user passwords and accounts. The features included in password and account management are a global and comprehensive way to manage password policy.

**Output**

```
Password Strength
    Minimum Password Length 6
    Password Complexity 2
    Password Palindrome Check on

Password History
    Password History Checking on
    Password History Length 10

Mandatory Password Change
    Password Expiration Lifetime never
```

**Comments**

From Gaia

DRAFT

# Authentication Servers

The AAA component of the system manages user access to the appliance. Generally, AAA includes Authentication (identifying a user), Authorization (determining what a user is permitted to do), and Accounting (tracking some aspects of a user's activity).

Check Point Gaia implements Pluggable Authentication Modules (PAM), an industry-standard framework for authenticating and authorizing users. Using PAM, authentication, account management, and session management algorithms are contained in shared modules that you configure on your appliance.

**Note** - Generally, AAA uses the terms authentication, authorization, and accounting while PAM uses related, but not quite identical, terms authentication, account management, and session management. In particular, note that "accounting" is not the same as "account management."

⚠ **Warning** - If you configure a system so that users can be authenticated only by a PAM-based method (you disable local authentication), you cannot log in using a console connection.

## RADIUS

RADIUS (Remote Authentication Dial-In User Service) is a client/server authentication software system that supports remote-access applications. This service lets an organization to keep user profiles in a centralized database that resides on an authentication server. A host contacts a RADIUS server, which determines who has access to that service.

Gaia accepts RADIUS server users without corresponding local accounts on the Check Point system (if the RADIUS server and Gaia are configured correctly). See Configuring Nonlocal RADIUS Users.

You can configure RADIUS as an AAA module for your appliance to work as a RADIUS client. Check Point systems do not include RADIUS server functionality.

You can configure your appliance to contact more than one RADIUS server. If the first server in the list is unreachable, the next RADIUS server in the priority ranking is contacted to supply the functionality. You can remove a server at all times.

# Configuring RADIUS Authentication Servers - WebUI

### To configure a RADIUS client on your appliance:

1. In the tree view, click **User Management** > **Authentication Servers**.
2. Below RADIUS Servers, click **Add**. The **Add New RADIUS Server** window opens.
3. In the **Priority** field, enter a number. This number determines which server to try first, second, and so on.
4. In the **Host** field, enter the IP address or name of your RADIUS server.

   > **Note** - RADIUS supports only IPv4 addresses.

5. In **UDP Port**, enter the number of the UDP port to contact on the server host. The default is 1812, which is specified by the RADIUS standard. The range is 1 to 65535.

   > **Warning** - Firewall software often blocks traffic on port 1812. To ensure that RADIUS packets are not dropped, make sure that each firewall between the RADIUS server and Gaia devices are configured to let traffic move on UDP port 1812.

6. In **Shared secret**, enter the shared secret used to authenticate the authorization profile between the RADIUS server and the local client. Enter a text string without a backslash. You must also configure this same value on your RADIUS server. The RFC recommends that the shared secret be at least 16 characters long. Some RADIUS servers limit the shared secret to 15 or 16 characters. Consult the documentation for your RADIUS server.
7. In **Timeout in Seconds** (optional), enter the number of seconds the system waits for a response after contacting the server. The default value is 3. Depending on your client configuration. If there is no response, it retries the same server or attempts to contact a different server.
8. Click **OK**.

### To edit a RADIUS client on your appliance:

1. In the tree view, click **User Management** > **Authentication Servers**.
2. Select a RADIUS client from the table.
3. Click **Edit**. The **Edit RADIUS Server** window opens.
4. You can edit the Host name, UDP port number, Shared secret, or the Timeout. You cannot change the Priority value.
5. Click **OK**.

### To delete a RADIUS client on your appliance:

1. In the tree view, click **User Management** > **Authentication Servers**.
2. Select a RADIUS client from the table.
3. Click **Delete**. The **Remove RADIUS Server** window opens.
4. Click **OK** to confirm.

# Configuring RADIUS Authentication Servers - CLI (aaa)

**Description** Use these commands to configure Radius authentication servers

DRAFT

**Description**

Use these commands to configure Radius authentication servers

**Syntax**

To configure RADIUS for use in a single authentication profile:

```
add aaa radius-servers priority VALUE host VALUE [ port VALUE
] prompt-secret timeout VALUE
add aaa radius-servers priority VALUE host VALUE [ port VALUE
] secret VALUE timeout VALUE
add aaa tacacs-servers authentication hostname VALUE key VALUE
```

To delete a RADIUS configuration:

```
delete aaa radius-servers priority VALUE
```

To change the configuration of a RADIUS entry:

```
set aaa radius-servers priority VALUE host VALUE
set aaa radius-servers priority VALUE new-priority VALUE
set aaa radius-servers priority VALUE port VALUE
set aaa radius-servers priority VALUE prompt-secret
set aaa radius-servers priority VALUE secret VALUE
set aaa radius-servers priority VALUE timeout VALUE
set aaa tacacs-servers authentication hostname VALUE key VALUE
set aaa tacacs-servers authentication state VALUE
```

To view a list of all servers associated with an authentication profile:

```
show aaa radius-servers list
```

To view the RADIUS server configuration:

```
show aaa radius-servers priority VALUE host
show aaa radius-servers priority VALUE port
show aaa radius-servers priority VALUE timeout
```

**Parameters**

| Parameter | Description |
|---|---|
| | |

**Example**

```
show aaa radius-servers priority 1 host
```

**Output**

```
RADIUS server host fred
```

DRAFT

**Description** Use these commands to configure Radius authentication servers

**Comments**

- These commands already exist, but not yet supported:

  ```
  set aaa tacacs-servers authentication hostname VALUE key
  VALUE
  ```

  ```
  set aaa tacacs-servers authentication state VALUE commands
  ```

  add aaa tacacs-servers authentication hostname VALUE key VALUE
- `priority` is a number that indicates the priority of the server. The priority determines which server is tried first. A smaller number indicates a higher priority.
- `new-priority` changes the priority number of the server.
- `host` is the name or IP address of the RADIUS server in dot-delimited format.
- `port` is The UDP port to contact on the server host. You determine the correct value by the configuration of your RADIUS server. Common values are 1812 (default) and 1645 (nonstandard but used traditionally).
- `prompt secret` prompts you to enter the shared secret during the run of the command.
- `timeout` is the number of seconds to wait for the server to respond. The default value 3 seconds.
- `secret` is the shared secret used to authenticate the RADIUS server and the local client to each other. The same value must be configured on your RADIUS server.

# Copy of Configuring Nonlocal RADIUS Users

To grant access by nonlocal users (not defined on the Check Point system), you must configure the RADIUS server and Check Point system appropriately.

**Note** - If you configure a RADIUS user with a blank password (on your RADIUS+ server), Gaia does not grant access to that user.

### To configure a RADIUS server for nonlocal Gaia users

1. Copy the file nokiaGaia.dct (for Steel-Belted RADIUS servers) or dictionary.nokia (for freeRADIUS servers) to your RADIUS server.

   These files are in /etc on the Check Point system.
2. Define the user roles. Add these Check Point Vendor-Specific Attributes (VSA) to users in your RADIUS user configuration file:

   ```
   Nokia-IPSO-User-Role = "role1[:domain1;domain2;…..],role2[:domain1:…
   ```

   For example:

   ```
   Nokia-IPSO-User-Role = "foorole, barrole"
   ```

   ```
   Nokia-IPSO-User-Role = "foorole:foodomain, barrole"
   ```

   ```
   Nokia-IPSO-User-Role = "foorole:foodomain;bardomain,
   barrole:foodomain;bardomain"
   ```

   **Note** - Make sure the role names match existing roles in the Gaia system.

   If a nonlocal user is a cluster administrator, you must also specify the cluster ID, as in `Nokia-IPSO-User-Role = "clusterAdminRole:100",` in which 100 is the cluster ID.
3. Specify if the Check Point users must have superuser access to the Gaia shell. Add these VSA:

   ```
   Nokia-IPSO-SuperUser-Access = <0|1>
   ```

   in which

   - 0 provides nonsuperuser access
   - 1 provides superuser access

DRAFT

### To configure a Check Point system for nonlocal users

Step 4 of this procedure has two cross references to sections that explain how to add and remove Service Profiles. Service profiles are components of AAA Service Modules. Are they supported in Gaia? They are not supported in Not supported in Gaia EA4 build 75

1. On your Check Point system, create the roles that are to be assigned to the nonlocal users.
2. Create an authentication profile of type RADIUS and set the control level to sufficient.
3. Add the new authentication profile to each service profile.
4. Make the RADIUS authentication profile the first authentication mechanism for each service. Delete the other authentication profiles for each service and then re-add them.

   The other profiles are then added after the RADIUS authentication profile. See step 4 for information about adding an authentication profile to a service. See To remove a profile from a service profile for more information about deleting an authentication profile from a service.
5. For very important users, configure the Check Point system to grant access even if the RADIUS server is unavailable:

   a) Create local accounts for these users.

   b) If necessary, add a local authentication profile after the RADIUS profile for all the service profiles.

### To log in as a superuser

If the Check Point Superuser VSA is set to 1 for a nonlocal user, they can log into the Gaia shell with superuser privileges:

1. Log into the system using command line.

   The default shell is the Gaia CLI.
2. Enter `shell` to access the Gaia shell.
3. Enter `sudo /usr/bin/su -.` The user has superuser privileges

# System Groups

You can define and configure groups with Gaia as you can with equivalent Linux-based systems. This function is retained in Gaia for advanced applications and for retaining compatibility with Linux.

Use groups for these purposes:

- Specify Linux file permissions.
- Control who can log in through SSH.

For other functions that are related to groups, use the role-based administration feature, described in "Role-Based Administration" ("Roles" on page 80).

All users are assigned by default to the `users` group. You can edit a user’s primary group ID (using clish) to be something other than the default. However, you can still add the user to the `users` group. The list of members of the `users` group includes only users who are explicitly added to the group. The list of does not include users added by default.

# Configuring System Groups- WebUI

### To see a list of all Groups

Choose **User Management > System Groups** in the navigation tree.

### To add a  group

1. In the the **User Management > System Groups** page, click **Add.**
2. Enter the **Group Name.** 1-8 alphanumeric characters.
3. Enter a **Group ID** number.

   Group ID ranges 0-99 and 65531-65535 are reserved for system use. (GID 0 is reserved for users with root permissions and GID 10 is reserverd for the  predefined `Users` groups). If you specify a value in the reserved ranges, an error message is displayed.
4. Click **OK.**

DRAFT

### To add a member to a group

1. In the the **User Management > System Groups** page, select a group.
2. Click **Edit.**
3. Click **Add New Member.**
4. Select a user.
5. Click **OK.**

### To delete a member from a group

1. In the the **User Management > System Groups** page, select the group.
2. Click **Edit**.
3. Select the member
4. Click **Remove Member**
5. Click **OK**

### To Delete a Group

1. In the the **User Management > System Groups** page, select the group.
2. Click **Delete.**
3. Click **OK**.

## Configuring System Groups - CLI (group)

**Description** The commands in this section allow you to manage groups.

**Syntax** To view existing group members:

```
show group VALUE
```

To see existing groups:

```
show groups
```

To set the Group ID:

```
set group VALUE gid VALUE
```

To add a group or a group member:

```
add group VALUE gid VALUE
add group VALUE member VALUE
```

To delete a group or a group member

```
delete group VALUE member VALUE
```

**Parameters**

| Parameter | Description |
|---|---|
| group VALUE | Name of group. 1-8 alphanumeric characters, Must be unique on your system. |
| gid VALUE | Numeric Group ID. Must be unique on your system.<br>**Note -** Group ID ranges 0-99 and 65531-65535 are reserved for system use. (GID 0 is reserved for users with root permissions and GID 10 is reserverd for the predefined `Users` groups). If you specify a value in the reserved ranges, an error message is displayed. |
| member VALUE | Name of a existing user, including users admin and monitor. |

DRAFT

Chapter 9

# High Availability

In This Chapter

DRAFT

## VRRP

Virtual Router Redundancy Protocol (VRRP) supplies dynamic failover of IP addresses from one router to a different one in the event of failure. VRRP is defined in RFC 3768. The Check Point implementation of VRRP includes all of the features described in RFC 3768, plus the additional feature of monitored circuit, described below.

VRRP lets you supply alternate router paths for end hosts that are configured with static default routes. Static default routes minimize configuration and processing overhead on end hosts. When end hosts are configured with static routes, normally the failure of the master router results in the isolation of all hosts that are unable to detect available alternate paths to their gateway. VRRP lets you supply a higher availability default path to the gateway, and not configure Dynamic Routing or Router Discovery protocols on every end host.

The Check Point VRRP implementation of includes additional functionality called monitored circuit. *Monitored-circuit VRRP* eliminates the black holes caused by asymmetric routes that can be created if only one interface on the master fails (as opposed to the entire platform failing). Gaia releases priority over all of the interfaces in the virtual router to let the backup take over entirely.

### Before configuring VRRP

1. Synchronize all platforms that are part of the VRRP group to have the same system times.

   The simplest way to coordinate system times is to enable NTP on all nodes of the VRRP group. You can also manually change the time and time zone on each node to match other nodes (to within a few seconds).
2. Add hostnames and IP address pairs to the host table of each node in your VRRP group. This is not required but lets you use hostnames instead of IP addresses or DNS servers.

This section explains the simple method to Monitored-Circuit VRRP

## VRRP Overview

Virtual Router Redundancy Protocol (VRRP) supplies dynamic failover of IP addresses from one router to a different one in the event of failure. VRRP is defined in RFC 3768. The Check Point implementation of VRRP includes all of the features described in RFC 3768, plus the additional feature of monitored circuit, described below.

VRRP lets you supply alternate router paths for end hosts that are configured with static default routes. Static default routes minimize configuration and processing overhead on end hosts. When end hosts are configured with static routes, normally the failure of the master router results in the isolation of all hosts that are unable to detect available alternate paths to their gateway. VRRP lets you supply a higher availability default path to the gateway, and not configure Dynamic Routing or Router Discovery protocols on every end host.

The Check Point implementation of VRRP includes additional functionality called monitored circuit. *Monitored-circuit VRRP* eliminates the black holes caused by asymmetric routes that can be created if only one interface on the master fails (as opposed to the entire platform failing). Gaia releases priority over all of the interfaces in the virtual router to let the backup take over entirely.

### Before configuring VRRP

1. Synchronize all platforms that are part of the VRRP group to have the same system times.

   The simplest way to coordinate system times is to enable NTP on all nodes of the VRRP group. You can also manually change the time and time zone on each node to match other nodes (to within a few seconds).
2. Add hostnames and IP address pairs to the host table of each node in your VRRP group. This is not required but lets you use hostnames instead of IP addresses or DNS servers.

This section explains the simple method to Monitored-Circuit VRRP.

## How VRRP Works

VRRP uses a virtual router to let end hosts use an IP address as the default first-hop router. A virtual router is defined as a unique virtual router ID (VRID), and the router IP addresses of the default route on a LAN. It is comprised of a master router and at least one backup router. If the master platform fails, VRRP specifies an election protocol that assigns a backup platform. The backup forwards IP traffic sent to the IP address of the virtual router.

The master sends periodic VRRP advertisements (also known as hello messages).

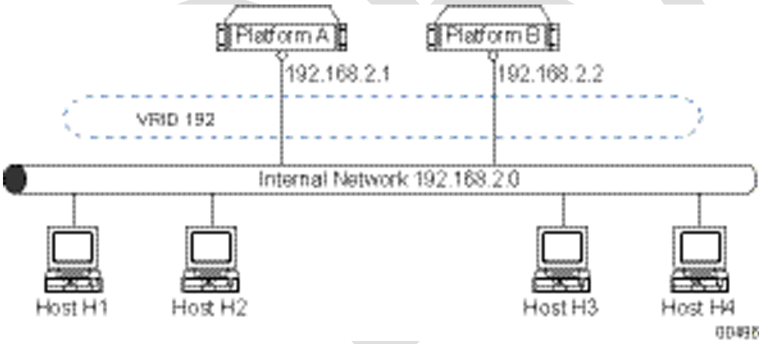
Check Point supplies support for OSPF, BGP, RIP, and PIM (sparse and dense modes) to advertise the IP address of the VRRP virtual router. You must use monitored-circuit VRRP to configure virtual IP support for a Dynamic Routing protocol.

**Note** - Gaia also supports OSPF on VPN tunnels that terminates at a VRRP group. Only active-passive VRRP configurations are supported, active-active configurations are not.

The master is defined as the router with the highest Priority parameter. You define a priority for each platform when you create the VRID or add a platform to it. If two platforms have equivalent priorities, the platform that comes online and broadcasts VRRP advertisements first becomes the master.

Simple VRRP Configuration (platform A is the master, and platform B is the backup):

original/frame/drawings/eps/00496.eps 154

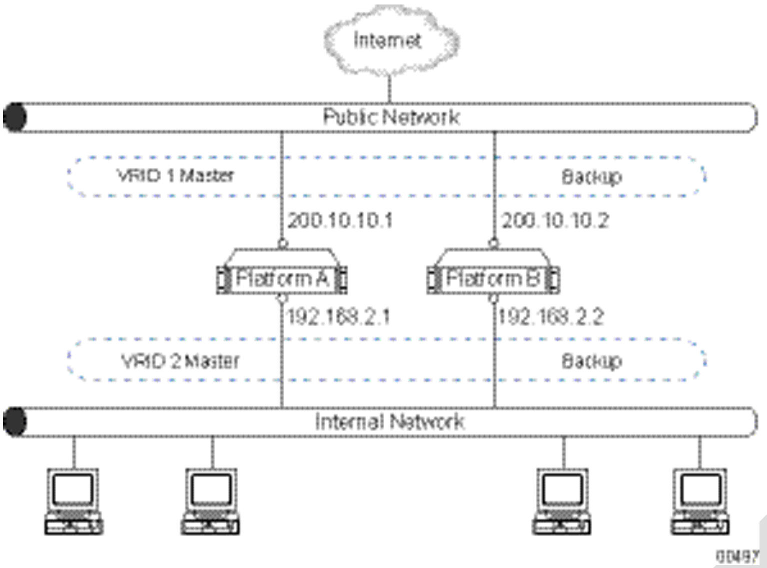


A VRRP router (a router that is running VRRP) might participate in more than one VRID. The VRID mappings and priorities are different for each VRID. You can create two VRIDs on the master and backup platforms. One VRID for connections with the external network, and one for connection with the internal network.

VRRP Configuration with Internal and External VRIDs:

DRAFT

original/frame/drawings/eps/00497.eps 155

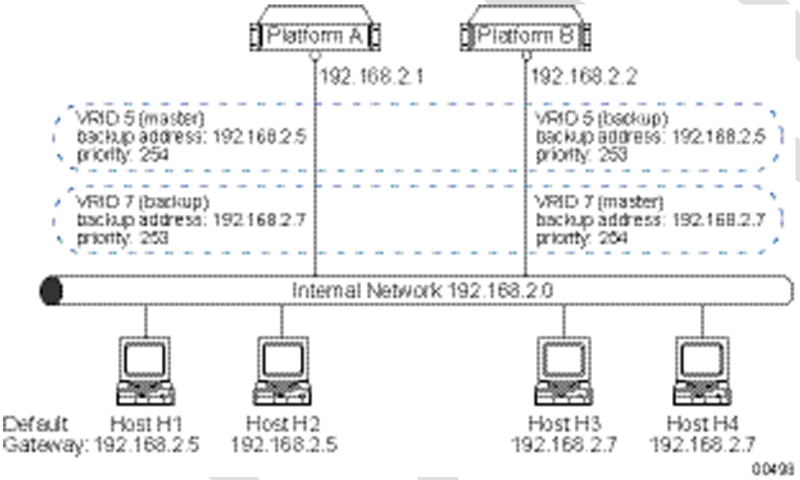


In this example, Platform A acts as the master for VRID 1 and VRID 2, while Platform B acts as the backup for VRID 1 and VRID 2.

You can configure some platforms to be part of multiple VRIDs while they simultaneously back up each other. This is known as an active-active configuration.

VRRP Configuration with some Backups at the same time:

original/frame/drawings/eps/00498.eps 156



In this active-active configuration, two VRIDs are implemented on the internal network for load sharing. Platform A is the master for VRID 5, and is the default gateway for Host H1 and Host H2. Platform B is the master for VRID 7, and is the default gateway for Host H3 and Host H4. Platforms A and B are configured to back each other up. If one platform fails, the other takes its VRID and IP addresses. It supplies load balancing, full redundancy, and uninterrupted service to the default IP addresses.

# Configuring VRRP - WebUI

This is the simple method to configure VRRP. It is the recommended method. This simple method automatically includes all the Monitored-Circuit interfaces that are on the same subnet, on the platform in the virtual router you create.

### To configure VRRP Global Settings:

1. In the **VRRP Global Settings** section, in **Cold Start Delay**, select the number of seconds that the system waits after starting and before joining a VRRP group. The value range is 1-3600. It is advised to configure a delay to let routing adjacencies form, or applications to synchronize before a system becomes the VRRP master.
2. In **Disable All Virtual Routers**, you can select to disable the routers, but it is advised to leave the clear default to keep the virtual routers enabled.

DRAFT

3. In **Monitor Firewall State**, you can select to clear (by default it is selected), but if you do, VRRP negotiation for master state might start before the firewall is fully started. This can result in two VRRP nodes assuming the master state while the firewall processes start.

   > **Note** - When selected, the system begins to monitor the firewall after the cold start delay period elapses. That can cause these problems:
   >
   > - If all the VRRP interfaces in a VRRP group fail, all the nodes become backup systems. None of the nodes is able to become the master, so no traffic is forwarded.
   > - If you change the time on any of the nodes, a VRRP transition (failover) occurs.
   > - Under certain circumstances, installing a firewall policy causes a VRRP transition to occur. This can happen if it takes a long time to install the policy.

4. Click **Apply Global Settings**.

### To add a virtual router:

1. In the **Virtual Routers** section, click **Add**. The **Add Virtual Router** window opens.
2. In **Virtual Router ID**, select the ID number of the virtual router.
3. In **Priority**, select the priority value. The priority value determines which router takes over in the event of a failure. The router with the higher priority becomes the new master. The range of values for priority is 1 to 254. The default setting is 100.
4. In **Hello Interval**, select the number of seconds at which the master sends VRRP advertisements. The range is 1-255 seconds (1 is default).

   All nodes of a given VRID must have the same hello Interval. If not, VRRP discards the packet and the two platforms go to master state.

   The hello interval also determines the failover interval; that is, how long it takes a backup router to take over from a failed master. If the master misses three hello advertisements, it is considered to be down because the minimum hello interval is 1 second, therefore the minimum failover time is 3 seconds (3 * Hello_interval).
5. In **Authentication**, select **None** or **Simple** password. You must select the same authentication method for all nodes in the VRID.
6. In **Priority Delta**, enter or select with the arrows the number to subtract from Priority to create an effective priority when an interface related to the backup fails. The range is 1-254.
7. To add Backup Addresses:

   a) In the **Backup Addresses** section, click **Add**. The **Add Backup Address** window opens.

   b) In **IPv4 address**, enter the IPv4 address.

   c) In **VMAC Mode**, from the drop-down list, select the mode: **VRRP**, **Interfac**e, **Static**, or **Extended**.

   d) Click **Save**. The new Vmac mode shows in the in the **Backup Address** table.
8. To remove a backup address, select an address and click **Delete**. The address is removed from the **Backup Address** table.
9. Click **Save**.

# Configuring VRRP - CLI (mcvr)

**Description**

DRAFT

**Description**

**Syntax**

To add a monitored-circuit virtual router:

```
add mcvr vrid VALUE backup-address VALUE vmac-mode
VALUE [ static-mac VALUE ]
add mcvr vrid VALUE priority VALUE priority-delta
VALUE [ hello-interval VALUE authtype VALUE
password VALUE ]

delete mcvr old-mc-config
```

To set a monitored-circuit virtual router:

```
set mcvr vrid VALUE authtype VALUE password VALUE
set mcvr vrid VALUE backup-address VALUE vmac-mode
VALUE [ static-mac VALUE ]
set mcvr vrid VALUE hello-interval VALUE
set mcvr vrid VALUE priority VALUE
```

To show a monitored-circuit virtual router setting:

```
show mcvr vrid VALUE all
show mcvr vrid VALUE authtype
show mcvr vrid VALUE backup-addresses
show mcvr vrid VALUE hello-interval
show mcvr vrid VALUE password
show mcvr vrid VALUE priority
show mcvr vrid VALUE priority-delta
show mcvr vrids
```

DRAFT

**Description**

**Parameters**

| Parameter | Description |
|---|---|
| `mcvr vrid` | The ID number of the monitored- circuit virtual router. |
| `backup-address` | The IPv4 address of the backup router. |
| `vmac-mode` | The VMAC Mode: VRRP, Interface, Static, or Extended. |
| `static-mac VALUE` | If in static mode, you must set the VMAC address manually. Enter the 48-bit VMAC address. |
| `priority` | The router with the higher priority becomes the new master when a failure occurs. The range is 1-254. The default setting is 100. |
| `priority-delta` | If an interface associated with a backup address fails, the value of the priority delta is subtracted from the priority to yield an effective priority for the physical router.<br>When the effective priority on the master is less than the priority of another router in the VRRP group, a new master is selected.<br>The range is 1-254 |
| `hello-interval` | The number of seconds at which the master sends VRRP advertisements. The range is 1-255 seconds (1 is default). |
| `authtype` | `none` for no password, or `simple` to use a password. |
| `password` | Your password |

**Example**

**Output**

**Comments**

# Advanced VRRP

## Advanced VRRP Overview

Virtual Router Redundancy Protocol (VRRP) supplies dynamic failover of IP addresses from one router to a different one in the event of failure. VRRP is defined in RFC 3768. The Check Point implementation of VRRP includes all of the features described in RFC 3768, plus the additional feature of monitored circuit, described below.

VRRP lets you supply alternate router paths for end hosts that are configured with static default routes. Static default routes minimize configuration and processing overhead on end hosts. When end hosts are configured with static routes, normally the failure of the master router results in the isolation of all hosts that are unable to detect available alternate paths to their gateway. VRRP lets you supply a higher availability default path to the gateway, and not configure Dynamic Routing or Router Discovery protocols on every end host.

The Check Point implementation of VRRP includes additional functionality called monitored circuit. *Monitored-circuit VRRP* eliminates the black holes caused by asymmetric routes that can be created if only one interface on the master fails (as opposed to the entire platform failing). Gaia does this by releasing priority over all of the interfaces in the virtual router to allow the backup to take over entirely.

### Before configuring VRRP

1. Synchronize all platforms that are part of the VRRP group to have the same system times.

   The simplest way to coordinate system times is to enable NTP on all nodes of the VRRP group. You can also manually change the time and time zone on each node to match other nodes (to within a few seconds).
2. Add hostnames and IP address pairs to the host table of each node in your VRRP group. This is not required but lets you use hostnames instead of IP addresses or DNS servers.

This section explains the advanced method. Use this method when you work on a system on which VRRP is already configured, or if you require control over the configuration of each interface.

## Configuring Advanced VRRP - WebUI

The advanced VRRP requires users to manually configure a virtual router for each monitored interface.

If you use this advanced method, and you wish to use to regular, simple method, you must delete the VRIDS, and recreate them in the regular VRRP section.

**Note** - You cannot move a backup address between interfaces while a platform is in the master state. To modify a virtual IP address, first cause a failover to the backup. Reduce the priority or disconnect an interface, delete the VRID on the interface, and recreate it with the new IP address. Then configure it as before.

### To configure VRRP Global Settings:

1. In the **VRRP Global Settings** section, in **Cold Start Delay**, select the number of seconds that the system waits after starting and before joining a VRRP group. The value range is 1-3600. It is advised to configure a delay to let routing adjacencies form, or applications to synchronize before a system becomes the VRRP master.
2. In **Disable All Virtual Routers**, you can select to disable the routers, but it is advised to leave the clear default to keep the virtual routers enabled.
3. In **Monitor Firewall State**, you can select to clear (by default it is selected), but if you do, VRRP negotiation for master state might start before the firewall is fully started. This can result in two VRRP nodes assuming the master state while the firewall processes start.

DRAFT

**Note** - When selected, the system begins to monitor the firewall after the cold start delay period elapses. That can cause these problems:

- If all the VRRP interfaces in a VRRP group fail, all the nodes become backup systems. None of the nodes is able to become the master, so no traffic is forwarded.
- If you change the time on any of the nodes, a VRRP transition (failover) occurs.
- Under certain circumstances, installing a firewall policy causes a VRRP transition to occur. This can happen if it takes a long time to install the policy.

4. Click **Apply Global Settings**.

### To add a virtual router:

1. In the **Virtual Routers** section, click **Add**. The **Add New Virtual Router** window opens.
2. In **Virtual Router ID**, select the ID number of the virtual router.
3. In **Interface**, select the interface for the virtual router.
4. In **Priority**, select the priority value. The priority value determines which router takes over in the event of a failure. The router with the higher priority becomes the new master. The range of values for priority is 1 to 254. The default setting is 100.
5. In **Hello Interval**, select the number of seconds at which the master sends VRRP advertisements. The range is 1-255 seconds (1 is default).

   All nodes of a given VRID must have the same hello Interval. If not, VRRP discards the packet and both platforms go to master state.

   The hello interval also determines the failover interval; that is, how long it takes a backup router to take over from a failed master. If the master misses three hello advertisements, it is considered to be down because the minimum hello interval is 1 second, therefore the minimum failover time is 3 seconds (3 * Hello_interval).
6. In **Preempt Mode**, if you keep it selected (the default), when the original master fails, a backup system becomes the acting master. When the original master returns to service, it becomes master again.

   If you clear it, when the original master fails, a backup system becomes the acting master, and the original does not become master again when it returns to service.
7. In **Auto-deactivation**, if you keep it clear (the default), a virtual router with the lowest priority available (1) can become master if no other VRRP routers exist on the network.

   If you select it, the effective priority can become 0. With this priority, the virtual router does not become the master even if there are no other VRRP routers on the network. If you enable Auto-deactivation, you should also configure the Priority and Priority Delta values to be equal so that the effective priority becomes 0 if there is a VRRP failure.
8. For each VRID, a virtual MAC (VMAC) address is assigned to the backup address. The VMAC address is included in all VRRP packet transmissions as the source MAC address. The physical MAC address is not used.

   In **VMAC Mode**, select the mode:

   - **VRRP**—the default mode. Gaia sets the VMAC to the format outlined in the VRRP protocol specification RFC 3768. It is automatically set to the same value on all nodes of a VRID.
   - **Interface**—Gaia sets the VMAC to the MAC address of the local interface. If you select **Interface** mode for both master and backup, the VMAC is different for each. The VRRP IP addresses are associated with different VMACs because they depend on the MAC address of the physical interfaces of the platform that is master at the time.

     **Note** - If you configure different VMACs on the master and backup, you must choose the correct proxy ARP setting for Network Address Translation.
   - **Static**—select this mode if you want to set the VMAC address manually. Then enter the 48-bit VMAC address in the Static VMAC text field.
   - **Extended**—similar to VRRP mode, except the system dynamically calculates three additional bytes of the interface hardware MAC address to generate a more random address. If you select this mode, Gaia constructs the same MAC address for master and backup platforms within the VRID.

DRAFT

**Note -** If you set the VMAC mode to interface or static, syslog error messages are displayed when you reboot or at failover, indicating duplicate IP addresses for the master and backup. This is expected behavior since both the master and backup routers temporarily use the same virtual IP address until they resolve into master and backup.

9. In **Authentication**, select **None** or **Simple** password. You must select the same authentication method for all nodes in the VRID.
10. To add Backup Addresses:

    a) In the **Backup Addresses** section, click **Add** to add a backup address. The **Add Backup Address** window opens.

    b) In **IPv4 address**, enter the IPv4 address.

    c) Click **Save**. The address shows in the **Backup Address** table.

    d) To remove a backup address, select an address and click **Delete**. The address is removed from the **Backup Address** table.

11. To configure Monitored interfaces:

    a) In the **Monitored Interfaces** section, click **Add**, to add a backup address. A warning that this action locks the interface for this virtual route opens.

    b) Click **OK**. The **Add Monitored Interface** window opens.

      (i) In **Interface**, from the drop-down list, select the interface.

      (ii) In Priority delta, enter or select with the arrows the number to subtract from Priority to create an effective priority when an interface related to the backup fails. The range is 1-254.

      (iii) Click **Save**. The interface and its priority delta show in the **Monitored Interfaces** table.

    c) To edit a monitored interface, select an interface and click **Edit**. The **Edit Monitored Interface** window opens.

      (i) Enter or select the new priority delta.

      (ii) Click **Save**.

    d) To remove a Monitored Interface, select an interface, and click **Delete**. The interface is removed from the **Monitored Interfaces** table.

12. Click **Save**.

## *Configuring Network Switches*

Use the information in this section as a guide when you connect your Check Point platforms to network switches.

### Use PortFast with Spanning Tree Protocol

If you use the Spanning Tree protocol on Cisco switches, in a network connected to Check Point systems that run VRRP, enable PortFast. PortFast sets interfaces to the Spanning-Tree forwarding state and not wait for the standard forward-time interval. If you use switches from a different vendor, use the equivalent feature supplied by that vendor.

If you use the Spanning Tree protocol without PortFast, or an equivalent feature, it can disrupt VRRP failovers.

### Do Not Cascade Switches

Do not connect interfaces that are in the same VRRP virtual router to different cascaded switches. For example: do not use this configuration:

- Master node: Interface of virtual router 1 connected to switch A.
- Backup node: Interface of virtual router 1 connected to switch B.
- Switch A and switch B connected by an uplink connection.

This configuration can disrupt VRRP failovers.

DRAFT

# Configuring the Check Point Security Gateway for VRRP

This section lists considerations for when you configure the Check Point Security Gateway for VRRP. For more details, refer to the Check Point documentation.

- Each VRRP node must run the same feature pack.
- The Operating System and Gaia must run on the same firewall.
- Complete the VRRP configuration before you put the systems into service. Make sure each system is configured, and the firewall begins synchronization before it puts the VRRP group in service. This procedure ensures that all connections are synchronized correctly.

When you use the Check Point cpconfig program, follow these guidelines:

- Install the Check Point Security Gateway on each node. Do not install the Check Point Security Gateway and Security Management server together on the same node.

  When you create and configure a gateway cluster object with the external VRRP IP address:
- Use the Check Point SmartDashboard application to create a gateway cluster object.
- Set the gateway cluster object address to the external VRRP IP address. That is, the VRRP IP (backup) address of the interface that faces the external network.
- Add a gateway object for each Check Point appliance to the gateway cluster object.
- In the gateway cluster object **General Propertys** window, clear ClusterXL.
- Configure interfaces for each member of the VRRP cluster. In **Topology**, select each VRRP cluster member, and click **Get** > **All Member's Interfaces with Topology**.
- Configure interfaces for the VRRP cluster. In **Topology**, select the gateway cluster object, and click **Get** > **All Member's Interfaces with Topology**.

When you complete configuring the gateway cluster object, you must also specify settings in **3rd Party Configuration** as described in this procedure.

### To configure settings for 3rd party configuration:

1. In the **Cluster Mode** section, select **High Availability**.
2. From the **Third-Party Solution** drop down list, select **Check Point VRRP**.
3. Select **Use State Synchronization**, and configure interfaces for it in **Topology**.

   **Note** - The Firewall Synchronization network requires a bandwidth of 100 mbps or greater.

   The interfaces that you configure for State Synchronization cannot be part of VLAN. They also cannot have more than one IP address assigned to them.
4. Select all the available check boxes.
5. Click OK to save your configuration changes.

   **Note** - you can use different encryption accelerator cards in two appliances of one VRRP group or IP cluster (such as the Check Point Encrypt Card in one appliance, and the older Check Point Encryption Accelerator Card in a different appliance). When you do, select encryption/authentication algorithms supported on the two cards. If the encryption/authentication algorithm is supported on the master only, and you use NAT, tunnels fail over incorrectly. If the encryption/authentication algorithm is supported on the master only, without NAT, tunnels are not accelerated after failover.

## Configuring VRRP Rules for Check Point Security Gateway

This section supplies information for firewall rules to work with VRRP.

Find this rule above the Stealth Rule:

| Source | Destination | Service | Action |
|---|---|---|---|
| `Firewalls`<br>`fwcluster-object` | `mcast-224.0.0.18` | `vrrp`<br>`igmp` | `Accept` |

Where:

- `Firewalls` is a Simple Group object containing the firewall objects.

DRAFT

- `fwcluster-object` is the gateway cluster object.
- `mcast-224.0.0.18` is a Node Host object with the IP address 224.0.0.18.

If your appliances run routing protocols such as OSPF and DVMRP, create new rules for each multicast destination IP address.

Alternatively, you can create a Network object to show all multicast network IP destinations with these values:

Name: `MCAST.NET`
IP: `224.0.0.0`
Netmask: `240.0.0.0`

You can use one rule for all multicast protocols you agree to accept, as shown below:

| Source | Destination | Service | Action |
|---|---|---|---|
| `cluster-all-ips` | `fwcluster-object`<br>`MCAST.NET` | `vrrp`<br>`igmp`<br>`ospf`<br>`dvmrp` | `Accept` |

## Troubleshooting VRRP

This section lists known problems with VRRP configurations. Please consult this section before contacting Customer Support. For information about contacting Check Point Customer Support, go to Check Point Support (http://www.nokia.com/nokia/0,,73109,00.html\n).

You can log information about errors and events for troubleshooting VRRP. Enable traces for VRRP.

### To enable traces for VRRP:

1. In the WebUI tree, select **Routing** > **Routing Options**.
2. In the **Trace Options** section, in the **Filter Visible Tables Below** drop down list, select **VRRP**.
3. In the **VRRP** table, select an option, and click **Activate**.

   The system restarts the routing subsystem and signals it to reread its configuration. The option you selected, its name and On/Off radio buttons show on the page.

### General Configuration Considerations

If VRRP failover does not occur as expected, make sure that the configuration of these items.

- All routers of a VRRP group must have the same system times. The simplest method to synchronize times is to enable NTP on all nodes of the VRRP group. You can also manually change the time and time zone on each node to match the other nodes. It must be no more than seconds apart.
- All routers of a VRRP group must have the same Hello Interval.
- The Priority Delta must be sufficiently large for the Effective Priority to be lower than the master router. Otherwise, when you pull an interface for a Monitored-Circuit VRRP test, other interfaces do not release IP addresses.
- You can use different encryption accelerator cards in two appliances of one VRRP group or IP cluster (such as the Check Point Encrypt Card in one appliance, and the older Check Point Encryption Accelerator Card in a different appliance). When you do, select encryption/authentication algorithms supported on the two cards. If the encryption/authentication algorithm is supported on the master only, and you use NAT, tunnels failover incorrectly. If the encryption/authentication algorithm is supported on the master only, without NAT, tunnels are not accelerated after failover.
- VRIDs must be the same on all routers in a VRRP group. If you use Monitored-Circuit VRRP, make sure all platforms of one virtual IP address use the same VRID.
- The VRRP monitor in the WebUI might show one of the interfaces in initialize state. This might suggest that the IP address used as the backup address on that interface is invalid or reserved.
- SNMP Get on Interfaces might list the incorrect IP addresses. This results in incorrect Policy. An SNMP Get (for the Firewall object Interfaces in the GUI Security Policy editor) fetches the lowest IP address for each interface. If interfaces are created when the node is the VRRP master, the incorrect IP address might be included. Repair this problem, edit the interfaces by hand if necessary.

DRAFT

### Firewall Policies

If your platforms run firewall software, you must configure the firewall policies to accept VRRP packets. The multicast destination assigned by the IANA for VRRP is 224.0.0.18. If the policy does not accept packets to 224.0.0.18, firewall platforms in one VRRP group take on Master state.

### Switched Environments

### Monitored-Circuit VRRP in Switched Environments

- With Monitored-Circuit VRRP, some Ethernet switches might not recognize the VRRP MAC address after a master to backup change. This is because many switches cache the MAC address related to the Ethernet device attached to a port. When the change to a backup router occurs, the MAC address for virtual router shifts to a different port. Switches that cache the MAC address might not change to the correct port during a VRRP change.

  To repair this problem, you can take one of the these actions:

  - Replace the switch with a hub.
  - Disable MAC address caching on the switch, or switch ports that the security platforms are connected to.

    It might be not possible to disable the MAC address caching. If so, set the address aging value sufficiently low that the addresses age out each second or two. This causes more overhead on the switch. Therefore, find out if this is a viable option for the model of switch you run.

- The Spanning Tree protocol prevents Layer 2 loops across multiple bridges. Spanning-Tree can be enabled on the ports connected to the two sides of a VRRP pair. It can also see multicast Hello Packets come for the same MAC address from two different ports. When the two occur, it can suggest a loop, and the switch blocks traffic from one port. If a port is blocked, no security platforms in the VRRP pair can get Hello Packets from other. In which instance, the two of them enter the master router state.

  If possible, turn off Spanning-Tree on the switch to resolve this issue. But, this can have deleterious effects if the switch is involved in a bridging loop. If you cannot disable Spanning-Tree, enable PortFast on the ports connected to the VRRP pair. PortFast causes a port to enter the Spanning-Tree forwarding state immediately, by passing the listening and learning states. The command to enable PortFast is `set spantree portfast 3/1-2 enable`, where `3/1-2` refers to slot 3, ports 1 and 2.

# Configuring Advanced VRRP - CLI (vrrp)

#### Description

DRAFT

**Description**

**Syntax**

### Set Commands

```
set vrrp
      coldstart-delay VALUE
      disable-all-virtual-routers off
      disable-all-virtual-routers on
      monitor-firewall off
      monitor-firewall on

set vrrp interface VALUE
      authtype none
      authtype simple VALUE
      monitored-circuit vrid VALUE auto-deactivation VALUE
      monitored-circuit vrid VALUE backup-address VALUE off
      monitored-circuit vrid VALUE backup-address VALUE on
      monitored-circuit vrid VALUE hello-interval VALUE
      monitored-circuit vrid VALUE monitored-off
      monitored-circuit vrid VALUE monitored-on
      monitored-circuit vrid VALUE monitored-priority-delta VALUE
      monitored-circuit vrid VALUE off
      monitored-circuit vrid VALUE on
      monitored-circuit vrid VALUE preempt-mode VALUE
      monitored-circuit vrid VALUE priority VALUE
      monitored-circuit vrid VALUE vmac-mode default-vmac
      monitored-circuit vrid VALUE vmac-mode extended-vmac
      monitored-circuit vrid VALUE vmac-mode interface-vmac
      monitored-circuit vrid VALUE vmac-mode static-vmac VALUE
      off
      virtual-router backup-vrid VALUE backup-address VALUE off
      virtual-router backup-vrid VALUE backup-address VALUE on
      virtual-router backup-vrid VALUE hello-interval VALUE
      virtual-router backup-vrid VALUE off
      virtual-router backup-vrid VALUE preempt-mode VALUE
      virtual-router backup-vrid VALUE priority VALUE
      virtual-router backup-vrid VALUE vmac-mode default-vmac
      virtual-router backup-vrid VALUE vmac-mode extended-vmac
      virtual-router backup-vrid VALUE vmac-mode interface-vmac
      virtual-router backup-vrid VALUE vmac-mode static-vmac VALUE
      virtual-router vrid VALUE hello-interval VALUE
      virtual-router vrid VALUE off
      virtual-router vrid VALUE on
      virtual-router vrid VALUE vmac-mode default-vmac
      virtual-router vrid VALUE vmac-mode extended-vmac
      virtual-router vrid VALUE vmac-mode interface-vmac
      virtual-router vrid VALUE vmac-mode static-vmac VALUE
```

### Show Commands

```
show vrrp
show vrrp interface VALUE
show vrrp interfaces
show vrrp stats
show vrrp summary
```

DRAFT

**Description**

**Parameters**

| Parameter | Description |
|---|---|
| `coldstart-delay` | The number of seconds that the system waits after starting and before joining a VRRP group. |
| `vrrp interface` | The name of the interface |
| `authtype simple` | The chosen password. |
| `monitored-circuit vrid` | `on` or `off` for the interface to be monitored. |
| `auto-deactivation` | `on` or `off`. On would create an effective priority 0. The virtual router with 0 priority cannot become master. |
| `backup-address` | The IPv4 address of the backup router. |
| `hello-interval` | The number of seconds at which the master sends VRRP advertisements. The range is 1-255 seconds (1 is default). |
| `monitored-priority-delta` | If an interface associated with a backup address fails, the value of the priority delta is subtracted from the priority to yield an effective priority for the physical router.<br>When the effective priority on the master is less than the priority of another router in the VRRP group, a new master is selected.<br>The range is 1-254 |
| `preempt-mode` | `on` or `off`. If on, after a failout, the original master becomes master again when returns to service. If off, the backup system that becomes master, remains master. |
| `priority` | The router with the higher priority becomes the new master when a failure occurs. The range is 1-254. The default setting is 100. |
| `virtual-router backup-vrid` | The backup virtual router ID number |
| `virtual-router vrid` | The virtual router ID number |

**Example**

```
show vrrp summary
```

**Output**

```
RTGRTG0019  VRRP: VRRP not enabled
```

**Comments**

# Chapter 10

# Maintenance

In This Chapter

DRAFT

## Upgrade

Placeholder

### Managing Upgrades - WebUI

Placeholder

### Managing Upgrades - CLI

Placeholder

## Restore Points

You can run manual backups of files or you can configure your system to run regularly scheduled backups, as described in "Creating Backup Files" on page 120 below.

You can also use the WebUI to manage your backup files, including the following tasks:

- Restore from locally stored files. See "To restore files" on page 124.
- Transfer backup files to, and restore them from, a remote server. See "Transferring Backup Files" on page 122.
- Delete backup files that are stored on the local system. See "To delete local backup files" on page 121.

You can also view a list of backup files that are stored locally by clicking Gaia Configuration > Configuration Summary.

# Backing Up and Restoring Files

You can perform manual backups of files..

You can also use the WebUI to manage your backup files, including the following tasks:

- Restore from locally stored files. See "To restore files" on page 124.
- Transfer backup files to, and restore them from, a remote server. See "Transferring Backup Files" on page 122.
- Delete backup files that are stored on the local system. See "To delete local backup files" on page 121.

You can also view a list of backup files that are stored locally by clicking Gaia Configuration > Configuration Summary.

## *Creating Backup Files*

You can create a backup file.

By default, the backup file is saved in /var/backup and contains everything in the following directories:

- configuration (/config)
- cron (/var/cron)
- etc (/var/etc)

**Note** - Export versions of Check Point Gaia do not include IPSec files.

You can also choose to include the following in your backup file:

- User home directories (stored in /var/emhome)
- Log files (stored in /var/logs)

### To create a backup file:

1. Click Backup and Restore under Configuration > System Configuration in the tree view.
2. Enter a file name for your backup file in the Backup File Name text box.

   If you do not enter a name, the backup file is not created.
3. Select any additional directories to include in the backup file:

   a) To include the home directories of all active users in the backup file, check the Backup Home Directories check box.

   b) To include log files in the backup file, check the Backup Log Files check box.

   c) To include application package files in the backup file, check the check box for each package to include in the backup file.

   Only installed packages that support backup are listed.
4. Click Apply.
5. Click Save to make your changes permanent.

### To delete local backup files:

1. Click Backup and Restore under Configuration > System Configuration in the tree view.
2. In the Delete Backup Files section, check the Delete check box next to the name of each backup file to delete.
3. Click Submit.

   The entry for the backup file disappears.

## *Restoring Files from Locally Stored Backup Files*

To restore files to the system, you must first create backup files as described in "Creating Backup Files" on page 120.

You can restore either from files stored locally or from files stored on a remote machine.

DRAFT

⚠ **Warning** - Restoring from a backup file overwrites your existing files.

### To restore files

1. Verify that the following prerequisites are met:
   - Enough disk space is available on your platform.

     ⚠ **Warning** - If you try to restore files and you do not have enough disk space, you risk damaging the operating system.

   - Your system is running the same version of the operating system and the same packages as those of the backup files from which you restore files.

     ⚠ **Warning** - Using incompatible versions can result in problems with configuration and data files, which might, or might not, be immediately detectable.
2. Click Backup and Restore under Configuration > System Configuration in the tree view.
3. If the file you are restoring from is stored on the local appliance, go to the Restore from Local section and perform the following steps. Otherwise, proceed to step 4.

   a) Select the name of the backup file from either the Manual Backup File or the Scheduled Backup File drop-down lists, depending on the type of file to restore.

   Manually backed-up files are in the /var/backup directory and scheduled backup files are in the /var/backup/sched directory. The drop-down lists contain lists of all the files in these directories, but some of the files might not be backup files.

   b) Proceed to step 5.
4. If the file you want to restore is stored on a remote device, go to the Restore From Remote section of the page. You can use FTP or HTTP to transfer the backup file to the Gaia platform.

   **To use FTP:**

   a) Click the FTP button.

   b) Enter the following information:

   - IP address of the FTP server.
   - Directory in which to save the backup file.
   - Enter the name of the user account for connecting to the FTP server.
   - Enter the name of the password to use when connecting to the FTP server.

   c) Proceed to step 5

   d) A list of available files in the directory you specify appears. Select the backup files you want to restore.

   **To use HTTP:**

   e) Click the HTTP button.

   f) Click the Browse button.

   g) Navigate to the location of the backup file.

   h) Select the backup file.

   i) Proceed to step 5
5. Click Apply.
6. Do not click Save. Ignore any messages indicating that unsaved changes will be lost.
7. Click Reboot and wait for the system to reboot.

   **Note** - You must reboot your system after restoring from backup files.

## Restore Files from Locally Stored Backup Files

```
set restore
   manual filename
   scheduled filename
```

DRAFT

Arguments

| | |
|---|---|
| `manual filename` | Specifies to restore your files to the system from a manual backup that is locally stored. Manual backups are stored in the var/backup/ directory. |
| `scheduled filename` | Specifies to restore your files to the system from a scheduled backup that is locally stored. Scheduled backups are stored in the<br>/var/backup/sched/ directory. |

**Warning** - Restoring from a backup file overwrites your existing files.

**Warning** - Make sure that you have enough disk space available on your Check Point platform before restoring files. If you try to restore files and you do not have enough disk space, you risk damaging the operating system.

**Note** - The system must be running the same version of the operating system and the same packages as those of the backup file(s) from which you restore file(s).

## Show Restore Commands

Use the following command to display information on your current restore configuration.

```
show restore
   manual filenames
   remote dir
   remote filenames
   remote site
   remote user
   scheduled filenames
```

Arguments

| | |
|---|---|
| `manual filenames` | Displays the names of the manual backup files that are available locally. |
| `remote dir` | Displays the path name of the directory on the remote server that contains the backup file to be restored |
| `remote filenames` | Displays the archive files that are available on the remote server. |
| `remote site` | Displays the IP address of the remote server from which the backup files will be restored. |
| `remote user` | Displays the name of the user account used to connect to the remote server where backed up files are stored. |
| `scheduled filenames` | Displays the names of the scheduled backup files that are available locally. |

DRAFT

# Restore Points

## *Configuring Restore Points- WebUI*

You can create an image of the system and restore it.

### To create an image:

1. In the tree view, click **Maintenance** > **Restore Points**.
2. Below available images, click **New Image**. The **Create New Image window** opens.
3. In the **Name** field, enter a name for the image.
4. In the **Description** field, enter a description for the image.
5. Click **OK**.

**Note** - To create the snapshot requires free space on the Backup partition. The required free disk space is the actual size of the root partition, multiplied by 1.15.

### To revert to an image:

1. In the tree view, click **Maintenance** > **Restore Points**.
2. Select an image.
3. Click **Revert**. The **Revert** window opens. It shows a warning regarding the settings overwrite, knowing the credentials, and the reboot. It also shows the selected image details.
4. Click **OK**.

### To delete an image:

1. In the tree view, click **Maintenance** > **Restore Points**.
2. Select an image.
3. Click **Delete**. The **Delete Image** window opens.
4. Click **Ok**.

### To import an image from the archive:

When you import an image, you can revert to it later.

1. In the tree view, click **Maintenance** > **Restore Points**.
2. Select an image.
3. Click **Import**. The **Import Image** window opens.
4. Click **Browse** to select the import file for upload.
5. Click **Upload**.
6. Click **OK**.

### To export an image to a client computer and External Media:

1. In the tree view, click **Maintenance** > **Restore Points**.
2. Select an image.
3. Click **Export**. The **Export Image (name)** window.
4. Click **Start Export**.
5. Select the export destination.

**Note** -

- The sanpshot exports to `/var/log`. The free space required in `/var/log` is the size of the snapshot multiplied by two.
- The minimum size of a snapshot is 2.5G, so the minimum free space you need in `/var/log` is 5G.

## *Configuring Restore Points - CLI (snapshot)*

**Description**

DRAFT

**Description**

**Syntax**

```
add snapshot VALUE desc VALUE

delete snapshot VALUE

set snapshot export VALUE path VALUE name VALUE
set snapshot import VALUE path VALUE name VALUE
set snapshot revert VALUE

show snapshot VALUE all
show snapshot VALUE date
show snapshot VALUE desc
show snapshot VALUE size

show snapshots
```

**Parameters**

| Parameter | Description |
|---|---|
| snapshot | Name of the image |
| desc | Description of the image |
| snapshot export | The name of the image to export |
| snapshot import | The name of the image to import |
| path | The storage location for the exported image. For example: /var/log |
| name | The name of the exported image (not the original image). |
| all | All image details |

**Example**

```
show snapshot micky all
```

**Output**

```
date  Mon Oct 10 18:43:41 2011
size  3.00G
description  test image
```

**Comments**

- To create the snapshot requires free space on the Backup partition. The required free disk space is the actual size of the root partition, multiplied by 1.15.
- The snapshot exports to `/var/log`. The free space required in `/var/log` is the size of the snapshot multiplied by two.

  The minimum size of a snapshot is 2.5G, so the minimum free space you need in `/var/log` is 5G.

# Hardware Health Monitoring

You can monitor these hardware elements:

- Fan sensors—Shows the fan number, location, status, and value.
- System Temperature sensor
- Voltage sensors
- Power Supply (on machines that support it)

## Showing Hardware Health Monitoring Information - WebUI

In the navigation tree, click **Maintenance** > **Hardware Health**.

In the Hardware Health table, you can view the status of the machine fans, system temperature, the voltages, and the power supply (on machines that support it).

For each component sensor, the table shows the value of its operation, and the status: **OK**, **Low**, or **High**.

To see the health history of a component, select the component sensor. A graph that shows the values along time opens.

To change the time intervals that the graph shows, click the **Minute** arrows.

To view different times, click the **Forward/Backward** arrows.

To refresh, click **Refresh**.

## Showing Hardware Monitoring Information - CLI (sysenv)

DRAFT

**Description**

These commands display the status for various system components, according to data readings from the supported sensors. Components for which the status can be displayed include temperature, voltage, power supplies, and fans. The command returns status only for installed components.

**Syntax**

To display all system status information:

```
show sysenv all
```

To display all system component information:

```
show sysenv fans
show sysenv ps
show sysenv temp
show sysenv volt
```

**Parameters**

| Parameter | Description |
|---|---|
| ps | Power Supply(not all machines support it) |

**Example**

```
show sysenv all
```

**Output**

```
gw-3002f0> show sysenv all

Hardware Information

Name     Value    unit        type      status  Maximum
Minimum
+12V     29.44    Volt        Voltage     0       12.6
11.4
+5V      6.02     Volt        Voltage     0       5.3
     4.75
VBat     3.23     Volt        Voltage     0       3.47
2.
```

**Comments**

The `show sysenv ps` command exists if the machine supports it or not.

# Security Management Server and Firewall Commands

## cpca_client

**Description** This command and all its derivatives are used to execute operations on the ICA.

**Usage** `cpca_client`

# cpca_client create_cert

**Description** Prompt the ICA to issue a SIC certificate for the Security Management server.

**Usage** `cpca_client [-d] create_cert [-p <ca_port>] -n "CN=<common name>" -f <PKCS12 filename>`

**Syntax**

| Argument | Description |
|---|---|
| `-d` | Debug flag |
| `-p <ca_port>` | Specifies the port used to connect to the CA (if the CA was not run from the default port 18209) |
| `-n "CN=<common name>"` | Sets the CN |
| `-f <PKCS12 filename>` | Specifies the file name where the certificate and keys are saved. |

DRAFT

# cpca_client revoke_cert

**Description** Revoke a certificate issued by the ICA.

**Usage** `cpca_client [-d] revoke_cert [-p <ca_port>] -n "CN=<common name>"`

**Syntax**

| Argument | Description |
|---|---|
| `-d` | Debug flag |
| `-p <ca_port>` | Specifies the port which is used to connect to the CA (if the CA was not run from the default port 18209) |
| `-n "CN=<common name>"` | Sets the CN |

# cpca_client lscert

**Description** Show all certificates issued by the ICA.

**Usage** `cpca_client [-d] lscert [-dn substr] [-stat Pending|Valid|Revoked|Expired|Renewed] [-kind SIC|IKE|User|LDAP] [-ser ser] [-dp dp]`

**Syntax**

| Argument | Description |
|---|---|
| `-d` | Debug flag |
| `-dn substring` | Filters results to those with a DN that matches this substring |
| `-stat` | Filters results to this status |
| `-kind` | Filters results for specified kind: SIC, IKE, User, or LDAP |

| Argument | Description |
|---|---|
| `-ser number` | Filters results for this serial number |
| `-dp number` | Filters results from this CDP |

# cpca_client set_mgmt_tools

**Description** Invoke or terminate the ICA Management Tool.

**Usage**
```
cpca_client [-d] set_mgmt_tools on|off  [-p <ca_port>]
[-no_ssl] [-a|-u "administrator|user DN" -a|-u "administrator|user DN" ... ]
```

**Syntax**

| Argument | Description |
|---|---|
| `-d` | Debug flag |
| `set_mgmt_tools on\|off` | • `on` - Start ICA Management tool<br>• `off` - Stop ICA Management tool |
| `-p <ca_port>` | Specifies the port which is used to connect to the CA (if the appropriate service was not run from the default port 18265) |
| `-no_ssl` | Configures the server to use clear http rather than https |
| `-a\|-u"administrator\|user DN"` | Sets the DNs of the administrators or user permitted to use the ICA Management tool |

**Comments**

1. If the command is run without `-a` or `-u` the list of the permitted users and administrators isn't changed. The server can be stopped or started with the previously defined permitted users and administrators.
2. If two consecutive start operations are initiated, the ICA Management Tool will not respond, unless you change the SSL mode. After the SSL mode has been modified, the server can be stopped and restarted.

DRAFT

# cp_conf

**Description** Configure/reconfigure a Security Gateway installation. The configuration available options for any machine depend on the installed configuration and products.

**Usage** `cp_conf`

# cp_conf sic

**Description** Enables the user to manage SIC.

**Usage**
```
cp_conf sic state # Get the current Trust state
cp_conf sic init <Activation Key> [norestart] # Initialize SIC
cp_conf sic cert_pull <Security Management server name/IP> <module object name>
# Pull certificate (DAIP only)
```

# cp_conf admin

**Description** Manage Check Point Administrators.

**Usage**

```
cp_conf admin get # Get the list of administrators.
cp_conf admin add <user> <passw> <permissions> # Add administrator
where permissions:
w - read/write
r - read only
cp_conf admin del <admin1> <admin2>... # Delete administrators.
```

# cp_conf ca

**Description** Initialize the Certificate Authority

**Usage**

```
cp_conf ca init # Initializes Internal CA.
cp_conf ca fqdn <name> # Sets the name of the Internal CA.
```

# cp_conf finger

**Description** Displays the fingerprint which will be used on first-time launch to verify the identity of the Security Management server being accessed by the SmartConsole. This fingerprint is a text string derived from the Security Management server's certificate

**Usage**

```
cp_conf finger get # Get Certificate's Fingerprint.
```

# cp_conf lic

**Description** Enables the administrator to add a license manually and to view the license installed.

**Usage**

```
cp_conf lic get # Get licenses installed.
cp_conf lic add -f <file name> # Add license from file.
cp_conf lic add -m <Host> <Date> <Signature Key> <SKU/Features> # Add license
manually.
cp_conf lic del <Signature Key> # Delete license.
```

# cp_conf client

**Description** Manage the GUI Clients allowed to connect to the management.

**Usage**

```
cp_conf client get # Get the GUI Clients list
cp_conf client add < GUI Client > # Add one GUI Client
cp_conf client del < GUI Client 1> < GUI Client 2>... # Delete GUI Clients
cp_conf client createlist < GUI Client 1> < GUI Client 2>... # Create new list.
```

# cp_conf ha

**Description** Enable or disable High Availability.

**Usage**

```
cp_conf ha enable/disable [norestart] # Enable/Disable HA\n",
```

# cp_conf snmp

**Description** Activate or deactivate SNMP.

**Usage**

```
cp_conf snmp get # Get SNMP Extension status.
cp_conf snmp activate/deactivate [norestart] # Deactivate SNMP Extension.
```

# cp_conf auto

**Description** Determine whether or not the Security Gateway/Security Management server starts automatically after the machine restarts.

DRAFT

**Usage** `cp_conf auto get [fw1] [fg1] [rm] [all] # Get the auto state of products.`
`cp_conf auto <enable|disable> <product1> <product2>... # Enable/Disable auto start.`

## cp_conf sxl

**Description** Enable or disable SecureXL acceleration.

**Usage** `cp_conf sxl <enable|disable> # Enable/Disable SecureXL.`

# cpconfig

**Description** Run a command line version of the Check Point Configuration Tool. This tool is used to configure an installed Check Point product. The options shown depend on the installed configuration and products. Amongst others, these options include:

- **Licenses and contracts** - Modify the necessary Check Point licenses and contracts.
- **Administrator** - Modify the administrator authorized to connect to the Security Management server.
- **GUI Clients** - Modify the list of SmartConsole Client machines from which the administrators are authorized to connect to a Security Management server.
- **SNMP Extension -** Configure the SNMP daemon. The SNMP daemon enables SecurePlatform to export its status to external network management tools.
- **PKCS #11 Token** - Register a cryptographic token, for use by SecurePlatform; see details of the token, and test its functionality.
- **Random Pool** - Configure the RSA keys, to be used by SecurePlatform.
- **Certificate Authority** - Install the Certificate Authority on the Security Management server in a first-time installation.
- **Secure Internal Communication** - Set up trust between the gateway on which this command is being run and the Security Management server.
- **Certificate's Fingerprint** - Display the fingerprint which will be used on first-time launch to verify the identity of the Security Management server being accessed by the SmartConsole. This fingerprint is a text string derived from the Security Management server's certificate.
- **Automatic Start of Check Point Products** - Specify whether Check Point Security Gateways will start automatically at boot time.

**Usage** `cpconfig`

**Further Info.** See the *R75.20 Installation and Upgrade Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=12269).

# cpinfo

**Description -** CPinfo is a utility that collects data on a machine at the time of execution. The CPinfo output file enables Check Point's support engineers to analyze setups from a remote location. Engineers can open the CPinfo file in demo mode, while viewing real Security Policies and objects. This allows for in-depth analysis of all of configuration options and environment settings.

**Usage -** `cpinfo [-v] [-l] [-n] [-o ] [-r | -t [tablename]] [-c Domain Management Server ... | -x vs]`

**Syntax**

| Argument | Description |
|---|---|
| `-z` | Output gzipped (effective with -o option) |
| `-r` | Includes the registry (Windows - very large output) |

DRAFT

| Argument | Description |
|---|---|
| `-v` | Prints version information |
| `-l` | Embeds log records (very large output) |
| `-n` | Does not resolve network addresses (faster) |
| `-o` | Output to a file and to the screen |
| `-t` | Output consists of tables only (SR only) |
| `-c` | Get information about the specified Domain Management Server (Multi-Domain Security Management) |
| `-x` | Get information about the specified VS (VSX) |

**Further Info.** SecureKnowledge solution sk30567 (http://supportcontent.checkpoint.com/solutions?id=sk30567)

DRAFT

# cplic

**Description** This command and all its derivatives relate to Check Point license management.

**Note** - The SmartUpdate GUI is the recommended way of managing licenses.

All `cplic` commands are located in `$CPDIR/bin.` License Management is divided into three types of commands:

- *Local licensing commands* are executed on local machines.
- *Remote licensing commands* are commands which affect remote machines are executed on the Security Management server.
- *License repository commands* are executed on the Security Management server.

**Usage** `cplic`

# cplic check

**Description** Check whether the license on the local machine will allow a given feature to be used.

**Usage** `cplic check [-p <product name>] [-v <product version>] [-c count] [-t <date>] [-r routers] [-S SRusers] <feature>`

**Syntax**

| Argument | Description |
|---|---|
| `-p <product name>` | Product for which license information is requested. For example `fw1, netso` |
| `-v <product version>` | Product version for which license information is requested |
| `-c count` | Output the number of licenses connected to this feature |

| Argument | Description |
|---|---|
| `-t <date>` | Check license status on future date. Use the format **ddmmmyyyy**. A feature may be valid on a given date on one license, but invalid in another |
| `-r routers` | Check how many routers are allowed. The `feature` option is not needed |
| `-S SRusers` | Check how many SecuRemote users are allowed. The `feature` option is not needed |
| `<feature>` | `<feature>` for which license information is requested |

# cplic db_add

**Description** Used to add one or more licenses to the license repository on the Security Management server. When local license are added to the license repository, they are automatically attached to its intended Check Point gateway, central licenses need to undergo the attachment process.

This command is a license repository command, it can only be executed on the Security Management server.

**Usage** `cplic db_add < -l license-file | host expiration-date signature SKU/features >`

**Syntax**

| Argument | Description |
|---|---|
| `-l license-file` | Adds the license(s) from `license-file`. The following options are **NOT** needed:<br>Host Expiration-Date Signature SKU/feature |

**Comments** **Copy/paste** the following parameters from the license received from the User Center. More than one license can be added.

- `host` – the target hostname or IP address.
- `expiration date` – The license expiration date.
- `signature` –The License signature string. For example:

  `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` (Case sensitive. The hyphens are optional.)
- `SKU/features` – The SKU of the license summarizes the features included in the license. For example: `CPSUITE-EVAL-3DES-vNG`

**Example** If the file `192.168.5.11.lic` contains one or more licenses, the command: `cplic db_add -l 192.168.5.11.lic` will produce output similar to the following:

```
Adding license to database ...

Operation Done
```

DRAFT

# cplic db_print

**Description** Displays the details of Check Point licenses stored in the license repository on the Security Management server.

**Usage** `cplic db_print <object name | -all> [-n noheader] [-x print signatures] [-t type] [-a attached]`

**Syntax**

| Argument | Description |
|---|---|
| `Object name` | Print only the licenses attached to `Object name`. `Object name` is the name of the Check Point Security Gateway object, as defined in SmartDashboard. |
| `-all` | Print all the licenses in the license repository |
| `-noheader`<br>(or `-n`) | Print licenses with no header. |
| `-x` | Print licenses with their signature |
| `-t`<br>`(or -type)` | Print licenses with their type: Central or Local. |
| -a<br>(or -`attached`) | Show which object the license is attached to. Useful if the `-all` option is specified. |

**Comments** This command is a license repository command, it can only be executed on the Security Management server.

# cplic db_rm

**Description** The `cplic db_rm` command removes a license from the license repository on the Security Management server. It can be executed ONLY after the license was detached using the `cplic del` command. Once the license has been removed from the repository, it can no longer be used.

**Usage** `cplic db_rm <signature>`

**Syntax**

| Argument | Description |
|---|---|
| `Signature` | The signature string within the license. |

**Example** `cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpwn`

**Comments** This command is a license repository command, it can only be executed on the Security Management server.

# cplic del

**Description** Delete a single Check Point license on a host, including unwanted evaluation, expired, and other licenses. Used for both local and remote machines

**Usage** `cplic del [-F <output file>] <signature> <object name>`

**Syntax**

DRAFT

| Argument | Description |
|---|---|
| `-F <output file>` | Send the output to `<output file>` instead of the screen. |
| `<signature>` | The signature string within the license. |

# cplic del <object name>

**Description** Detach a Central license from a Check Point gateway. When this command is executed, the license repository is automatically updated. The Central license remains in the repository as an unattached license. This command can be executed only on a Security Management server.

**Usage** `cplic del <Object name> [-F outputfile] [-ip dynamic ip] <Signature>`

**Syntax**

| Argument | Description |
|---|---|
| `object name` | The name of the Check Point Security Gateway object, as defined in SmartDashboard. |
| `-F outputfile` | Divert the output to `outputfile` rather than to the screen. |
| `-ip dynamic ip` | Delete the license on the Check Point Security Gateway with the specified IP address. This parameter is used for deleting a license on a DAIP Check Point Security Gateway<br>**Note -** If this parameter is used, then object name must be a DAIP gateway. |
| `Signature` | The signature string within the license. |

**Comments** This is a *Remote Licensing Command* which affects remote machines that is executed on the Security Management server.

# cplic get

**Description** The `cplic get` command retrieves all licenses from a Check Point Security Gateway (or from all Check Point gateways) into the license repository on the Security Management server. Do this to synchronize the repository with the Check Point gateway(s). When the command is run, all local changes will be updated.

**Usage** `cplic get <ipaddr | hostname | -all> [-v41]`

**Syntax**

| Argument | Description |
|---|---|
| `ipaddr` | The IP address of the Check Point Security Gateway from which licenses are to be retrieved. |
| `hostname` | The name of the Check Point Security Gateway object (as defined in SmartDashboard) from which licenses are to be retrieved. |
| `-all` | Retrieve licenses from all Check Point gateways in the managed network. |
| `-v41` | Retrieve version 4.1 licenses from the NF Check Point gateway. Used to upgrade version 4.1 licenses. |

DRAFT

**Example** If the Check Point Security Gateway with the object name `caruso` contains four Local licenses, and the license repository contains two other Local licenses, the command: `cplic get caruso` produces output similar to the following:

```
      Get retrieved 4 licenses.
Get removed 2 licenses.
```

**Comments** This is a *Remote Licensing Command* which affects remote machines that is executed on the Security Management server.

# cplic put

**Description** Install one or more Local licenses on a local machine.

**Usage** `cplic put [-o overwrite] [-c check-only] [-s select] [-F <output file>] [-P Pre-boot] [-k kernel-only] <-l license-file | host expiration date signature SKU/feature>`

**Syntax**

| Argument | Description |
|---|---|
| `-overwrite`<br>(or `-o`) | On a Security Management server this will erase all existing licenses and replace them with the new license(s). On a Check Point Security Gateway this will erase only Local licenses but not Central licenses, that are installed remotely. |
| `-check-only`<br>`(or -c)` | Verify the license. Checks if the IP of the license matches the machine, and if the signature is valid |
| `select`<br>(or `-s`) | Select only the Local licenses whose IP address matches the IP address of the machine. |
| `-F outputfile` | Outputs the result of the command to the designated file rather than to the screen. |
| `-Preboot`<br>(or `-P`) | Use this option after upgrading and before rebooting the machine. Use of this option will prevent certain error messages. |
| -kernel-only<br>(or -k) | Push the current valid licenses to the kernel. For Support use only. |
| `-l license-file` | Installs the license(s) in `license-file`, which can be a multi-license file. The following options are NOT needed: `host expiration-date signature SKU/features` |

**Comments** Copy and paste the following parameters from the license received from the User Center.

- `host` – One of the following:

**All platforms** - The IP address of the external interface (in dot notation); last part cannot be 0 or 255.

**Solaris2** - The response to the `hostid` command (beginning with 0x).

- `expiration date` – The license expiration date. Can be `never`.
- `signature` –The License signature string. For example:

  `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` (Case sensitive. The hyphens are optional.)

- `SKU/features` – A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPMP-EVAL-1-3DES-NG CK0123456789ab`

**Example** `cplic put -l 215.153.142.130.lic` produces output similar to the following:

DRAFT

```
Host              Expiration SKU
215.153.142.130   26Dec2001  CPMP-EVAL-1-3DES-NG
CK0123456789ab
```

# cplic put <object name> ...

**Description** Use the `cplic put` command to attach one or more central or local license remotely.When this command is executed, the license repository is also updated.

**Usage** `cplic put <object name> [-ip dynamic ip] [-F <output file>] < -l license-file | host expiration-date signature SKU/features >`

| Argument | Description |
|---|---|
| `Object name` | The name of the Check Point Security Gateway object, as defined in SmartDashboard. |
| `-ip dynamic ip` | Install the license on the Check Point Security Gateway with the specified IP address. This parameter is used for installing a license on a DAIP Check Point gateway.<br>**NOTE**: If this parameter is used, then object name must be a DAIP Check Point gateway. |
| `-F outputfile` | Divert the output to `outputfile` rather than to the screen. |
| `-l license-file` | Installs the license(s) from `license-file`. The following options are **NOT** needed:<br>`Host Expiration-Date Signature SKU/features` |

DRAFT

**Comments** This is a *Remote Licensing Command* which affects remote machines that is executed on the Security Management server.

This is a Copy and paste the following parameters from the license received from the User Center. More than one license can be attached.

- `host` – the target hostname or IP address.
- `expiration date` – The license expiration date. Can be `never`.
- `signature` –The License signature string. For example:

  `aa6uwknDc-CE6CRtjhv-zipoVWSnm-z98N7Ck3m` (Case sensitive. The hyphens are optional)
- `SKU/features` – A string listing the SKU and the Certificate Key of the license. The SKU of the license summarizes the features included in the license. For example: `CPMP-EVAL-1-3DES-NG CK0123456789ab`

# cplic print

**Description** The `cplic print` command (located in `$CPDIR/bin`) prints details of Check Point licenses on the local machine.

**Usage** `cplic print [-n noheader][-x prints signatures][-t type][-F <outputfile>] [-p preatures]`

**Syntax**

| Argument | Description |
|---|---|
| `-noheader`<br>(or `–n`) | Print licenses with no header. |

| Argument | Description |
|---|---|
| `-x` | Print licenses with their signature |
| `-type`<br>(or -t) | Prints licenses showing their type: Central or Local. |
| `-F <outputfile>` | Divert the output to `outputfile`. |
| `-preatures`<br>(or `-p`) | Print licenses resolved to primitive features. |

**Comments** On a Check Point gateway, this command will print all licenses that are installed on the local machine — both Local and Central licenses.

# cplic upgrade

**Description** Use the `cplic upgrade` command to upgrade licenses in the license repository using licenses in a license file obtained from the User Center.

**Usage** `cplic upgrade <-l inputfile>`

**Syntax**

| Argument | Description |
|---|---|
| `-l inputfile` | Upgrades the licenses in the license repository and Check Point gateways to match the licenses in `<inputfile>` |

**Example** The following example explains the procedure which needs to take place in order to upgrade the licenses in the license repository.

- Upgrade the Security Management server to the latest version.

  Ensure that there is connectivity between the Security Management server and the remote workstations with the previous version products.

- Import all licenses into the license repository. This can also be done *after* upgrading the products on the remote gateways.

- Run the command: `cplic get -all`. For example:

```
Getting licenses from all modules ...

count:root(su) [~] # cplic get -all
golda:
Retrieved 1 licenses.
Detached  0 licenses.
Removed   0 licenses.
count:
Retrieved 1 licenses.
Detached  0 licenses.
Removed   0 licenses.
```

- To see all the licenses in the repository, run the command `cplic db_print -all -a`

DRAFT

```
count:root(su) [~] # cplic db_print -all -a

Retrieving license information from database ...

The following licenses appear in the database:
==================================================

Host           Expiration Features
192.168.8.11   Never      CPFW-FIG-25-41       CK-
49C3A3CC7121 golda
192.168.5.11   26Nov2002  CPSUITE-EVAL-3DES-NG CK-
1234567890 count
```

- In the *User Center (*http://usercenter.checkpoint.com*)* , view the licenses for the products that were upgraded from version 4.1 to NG and create new upgraded licenses.
- Download a file containing the upgraded NG licenses. Only download licenses for the products that were upgraded from version 4.1 to NG.
- If you did not import the version 4.1 licenses into the repository, import the version 4.1 licenses now using the command `cplic get -all -v41`
- Run the license upgrade command: `cplic upgrade –l <inputfile>`

  - The licenses in the downloaded license file and in the license repository are compared.

  - If the certificate keys and features match, the old licenses in the repository and in the remote workstations are updated with the new licenses.

  - A report of the results of the license upgrade is printed.
- In the following example, there are two NG licenses in the file. One does not match any license on a remote workstation, the other matches a version 4.1 license on a remote workstation that should be upgraded:

**Comments** This is a *Remote Licensing Command* which affects remote machines that is executed on the Security Management server.

**Further Info.** See the *SmartUpdate* chapter of the *R75.20 Security Management Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=12277).

DRAFT

# cpstart

**Description** Start all Check Point processes and applications running on a machine.

**Usage** `cpstart`

**Comments** This command cannot be used to start `cprid`. `cprid` is invoked when the machine is booted and it runs independently.

# cpstat

**Description** `cpstat` displays the status of Check Point applications, either on the local machine or on another machine, in various formats.

**Usage** `cpstat [-h host][-p port][-s SICname][-f flavor][-o polling][-c count][-e period][-d] application_flag`

**Syntax**

| Argument | Description |
|---|---|
| `-h host` | A resolvable hostname, a dot-notation address (for example:192.168.33.23), or a DAIP object name. The default is localhost. |

| Argument | Description |
|---|---|
| `-p port` | Port number of the AMON server. The default is the standard AMON port (18192). |
| -s | Secure Internal Communication (SIC) name of the AMON server. |
| `-f flavor` | The flavor of the output (as it appears in the configuration file). The default is the first flavor found in the configuration file. |
| -o | Polling interval (seconds) specifies the pace of the results.<br>The default is 0, meaning the results are shown only once. |
| -c | Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown. |
| -e | Specifies the interval (seconds) over which 'statistical' olds are computed. Ignored for regular olds. |
| `-d` | Debug mode. |
| `application_flag` | One of the following:<br>• `fw` — Firewall component of the Security Gateway<br>• `vpn` — VPN component of the Security Gateway<br>• `fg` — QoS (formerly FloodGate-1)<br>• `ha` — ClusterXL (High Availability)<br>• `os` — OS Status<br>• `mg` — for the Security Management server<br>• `persistency` - for historical status values<br>• `polsrv`<br>• `uas`<br>• `svr`<br>• `cpsemd`<br>• `cpsead`<br>• `asm`<br>• `ls`<br>• `ca` |

DRAFT

The following flavors can be added to the application flags:

- `fw` — `"default", "interfaces", "all", "policy", "perf", "hmem", "kmem", "inspect", "cookies", "chains", "fragments", "totals", "ufp", "http", "ftp", "telnet", "rlogin", "smtp", "pop3", "sync"`
- `vpn` — `"default", "product", "IKE", "ipsec", "traffic", "compression", "accelerator", "nic", "statistics", "watermarks", "all"`
- `fg` — `"all"`
- `ha` — `"default", "all"`
- `os` — `"default", "ifconfig", "routing", "memory", "old_memory", "cpu", "disk", "perf", "multi_cpu", "multi_disk", "all", "average_cpu", "average_memory", "statistics"`

- `mg` — `"default"`
- `persistency` — `"product", "Tableconfig", "SourceConfig"`
- `polsrv` — `"default", "all"`
- `uas` — `"default"`
- `svr` — `"default"`
- `cpsemd` — `"default"`
- `cpsead` — `"default"`
- `asm` — `"default", "WS"`
- `ls` — `"default"`
- `ca` — `"default", "crl", "cert", user", "all"`

**Example**

```
> cpstat fw

Policy name:  Standard
Install time: Wed Nov  1 15:25:03 2000

Interface table
-----------------------------------------------------------------
|Name|Dir|Total *|Accept**|Deny|Log|
-----------------------------------------------------------------
|hme0|in |739041*|738990**|51 *|7**|
-----------------------------------------------------------------
|hme0|out|463525*|463525**| 0 *|0**|
-----------------------------------------------------------------
*********|1202566|1202515*|51**|7**|
```

DRAFT

# cpstop

**Description** Terminate all Check Point processes and applications, running on a machine.

**Usage** `cpstop`

```
cpstop -fwflag [-proc | -default]
```

**Syntax**

| Argument | Description |
|---|---|
| `-fwflag -proc` | Kills Check Point daemons and Security servers while maintaining the active Security Policy running in the kernel. Rules with generic allow/reject/drop rules, based on services continue to work. |
| `-fwflag -default` | Kills Check Point daemons and Security servers. The active Security Policy running in the kernel is replaced with the default filter. |

**Comments** This command cannot be used to terminate `cprid`. `cprid` is invoked when the machine is booted and it runs independently.

# fw

**Description** The `fw` commands are used for working with various aspects of the firewall. All `fw` commands are executed on the Check Point Security gateway.

Typing `fw` at the command prompt sends a list of available fw commands to the standard output.

**Usage** `fw`

# fw -i

**Description** Generally, when Check Point Security gateway commands are executed on a Security gateway they will relate to the gateway as a whole, rather than to an individual kernel instance. For example, the `fw tab` command will enable viewing or editing of a single table of information aggregated for all kernel instances.

This command specifies that certain commands apply to an individual kernel instance. By adding `-i <kern>` after `fw` in the command, where `<kern>` is the kernel instance's number.

**Usage** `fw -i` applies to the following commands:

`fw ctl debug` (when used without the `-buf` parameter)

```
fw ctl get
fw ctl set
fw ctl leak
fw ctl pstat
fw monitor
fw tab
```

For details and additional parameters for any of these commands, refer to the command's entry.

**Example** To view the connections table for kernel instance #1 use the following command:

```
fw -i 1 tab -t connections
```

# fw ctl

**Description** The fw ctl command controls the Firewall kernel module.

**Usage**

```
fw ctl <install|uninstall>
fw ctl debug [-m <module>] [+|-] <options | all | 0>
fw ctl debug -buf [buffer size]
fw ctl kdebug
fw ctl pstat [-h][-k][-s][-n][-l]
fw ctl iflist
fw ctl arp [-n]
fw ctl block <on|off>
fw ctl chain
fw ctl conn
```

| Argument | Description |
|---|---|
| `<Install\|`<br>`Uninstall>` | • `Uninstall` — tells the operating system to stop passing packets to the Security Gateway, and unloads the Security Policy. The networks behind it become unprotected.<br>• `Install` — tells the operating system to start passing packets to the Security Gateway. The command `fw ctl install` runs automatically when `cpstart` is performed.<br>**Note -** If you run `fw ctl uninstall` followed by `fw ctl install`, the Security Policy is not restored. |

DRAFT

| Argument | Description |
|---|---|
| debug | Generate debug messages to a buffer. See fw ctl debug (on page 128). |
| kdebug | Reads the debug buffer and obtains the debug messages. If there is no debug buffer, the command will fail.<br>• [-f] read the buffer every second and print the messages, until Ctrl-C is pressed. Otherwise, read the current buffer contents and end.<br>• [-t/-T] print the time field (seconds/microseconds)<br>• [-p] to print specific fields all\|proc\|pid\|date\|mid\|type\|freq\|topic\|time\|ticks\|tid\|text\|err\|host\|vsid\|cpu<br>• [-m] - number of cyclic files, [-s] - size of each |
| pstat [-h][-k][-s][-n][-l] | Displays Security Gateway internal statistics:<br>-h — Generates additional hmem details.<br>-k — Generates additional kmem details.<br>-s — Generates additional smem details.<br>-n — Generates NDIS information (Windows only).<br>-l — Generates general Security Gateway statistics. |
| iflist | Displays the IP interfaces known to the kernel, by name and internal number. |
| arp [-n] | Displays ARP proxy table.<br>-n — Do not perform name resolution. |
| block <on\|off> | on — Blocks all traffic.<br>off — Restores traffic and the Security Policy. |
| chain | Prints the names of internal Security Gateways that deal with packets. Use to ensure that a gateway is loaded. The names of these gateways can be used in the fw monitor -p command. |
| conn | Prints the names of the connection modules. |

DRAFT

# fw ctl debug

**Description** Generate debug messages to a buffer.

**Usage A number of debug options are available:**

```
fw ctl debug -buf [buffer size]
fw ctl debug [-m module] [+ | -] <options| all|0>
fw ctl debug 0
fw ctl debug [-d <comma separated list of strings>]
fw ctl debug [-d <comma separated list of ^strings>]
fw ctl debug [-s <string>]
fw ctl debug -h
fw ctl debug -x
```

**Syntax**

| Argument | Description |
|---|---|
| -buf [buffer size] | Allocates a buffer of size kilobytes (default 128) and starts collecting messages there. If the -buf argument is not set, the debug messages are printed to the console. |
| -m <module> | Specify the Security Gateway module you wish to debug. The default module is fw.<br>For example: `fw ctl debug -m VPN all` |
| [+ \| -] <options\|all\|0> | Sets or resets debug flags for the requested gateway).<br>• If + is used, the specified flags are set, and the rest remain as they were.<br>• If - is used, the specified flags are reset, and the rest remain as they were.<br>• If neither + nor – are used, the specified flags are set and the rest are reset. |
| -h | Print a list of debug modules and flags. |
| 0 | Returns all flags in all gateways to their default values, releases the debug buffer (if there was one). |
| -d <comma separated list of strings> | Only lines containing these strings are included in the output. (Available in R70 or higher) |
| -d <comma separated list of ^strings> | Lines containing these strings are omitted from the output (Available in R70 or higher)<br>For example:<br>`fw ctl debug -d error,failed,^packet`<br>Output shows only lines containing the words "error" or "failed" and not the word "packet" |
| -s <string> | Stop debug messages when a certain string is issues (Available in R70 or higher)<br>For example: `fw ctl debug -s error` |
| -x | Shuts down the debug. |

DRAFT

# fw ctl affinity

## *fw ctl affinity -s*

**Description** Sets CoreXL affinities when using multiple processors. For an explanation of kernel, daemon and interface affinities, see the *R75.20 Firewall Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=12267).

`fw ctl affinity -s` settings are not persistent through a restart of the Security Gateway. If you want the settings to be persistent, either use:

- `sim affinity` (a Performance Pack command) - for details, see the*R75.20 Performance Pack Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=12274)*.*
- Or edit the `fwaffinity.conf` configuration file - for details, see the *R75.20 Firewall Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=12267)*.*

To set interface affinities, you should use `fw ctl affinity` only if Performance Pack is not running. If Performance Pack is running, you should set affinities by using the Performance Pack `sim affinity` command. These settings will be persistent. If Performance Pack's `sim affinity` is set to Automatic mode (even if Performance Pack was subsequently disabled), you will not be able to set interface affinities by using `fw ctl affinity -s`.

**Usage** `fw ctl affinity -s <proc_selection> <cpuid>`

**Syntax** `<proc_selection>` is one of the following parameters:

| Argument | Description |
|---|---|
| `-p <pid>` | Sets affinity for a particular process, where `<pid>` is the process ID#. |
| `-n <cpdname>` | Sets affinity for a Check Point daemon, where `<cpdname>` is the Check Point daemon name (for example: `fwd`). |
| `-k <instance>` | Sets affinity for a kernel instance, where `<instance>` is the instance's number. |
| -i <interfacename> | Sets affinity for an interface, where `<interfacename>` is the interface name (for example: `eth0`). |

`<cpuid>` should be a processing core number or a list of processing core numbers. To have no affinity to any specific processing core, `<cpuid>` should be: `all`.

**Note** - Setting an Interface Affinity will set the affinities of all interfaces sharing the same IRQ to the same processing core. To view the IRQs of all interfaces, run: `fw ctl affinity -l -v -a`.

**Example** To set kernel instance #3 to run on processing core #5, run:

```
fw ctl affinity -s -k 3 5
```

## *fw ctl affinity -l*

**Description** Lists existing CoreXL affinities when using multiple processors. For an explanation of kernel, daemon and interface affinities, see the *R75.20 Firewall Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=12267).

**Usage** `fw ctl affinity -l [<proc_selection>] [<listtype>]`

**Syntax** `If <proc_selection>` is omitted, `fw ctl affinity -l` lists affinities of all Check Point daemons, kernel instances and interfaces. Otherwise, `<proc_selection>` is one of the following parameters:

| Argument | Description |
|---|---|
| `-p <pid>` | Displays the affinity of a particular process, where `<pid>` is the process ID#. |
| `-n <cpdname>` | Displays the affinity of a Check Point daemon, where `<cpdname>` is the Check Point daemon name (for example: `fwd)`. |
| `-k <instance>` | Displays the affinity of a kernel instance, where `<instance>` is the instance's number. |
| `-i <interfacename>` | Displays the affinity of an interface, where `<interfacename>` is the interface name (for example: `eth0`). |

`If <listtype>` is omitted, `fw ctl affinity -l` lists items with specific affinities, and their affinities. Otherwise, `<listtype>` is one or more of the following parameters:

| Argument | Description |
|---|---|
| `-a` | All: includes items without specific affinities. |

DRAFT

| Argument | Description |
|---|---|
| `-r` | Reverse: lists each processing core and the items that have it as their affinity. |
| `-v` | Verbose: list includes additional information. |

**Example** To list complete affinity information for all Check Point daemons, kernel instances and interfaces, including items without specific affinities, and with additional information, run:

```
fw ctl affinity -l -a -v
```

# fw ctl engine

**Description** Enables the INSPECT2C engine, which dynamically converts INSPECT code to C code.

Run the command on the Check Point Security Gateway.

**Usage** `fw ctl engine {on | off | stat | setdefault}`

**Syntax**

| Argument | Description |
|---|---|
| `on` | Compile the engine if necessary, and activate it.<br>Because the engine may not have been previously compiled, turning the engine ON may not activate it immediately. Instead, the engine is activated in the background after the compilation.<br>After turning the engine ON, the engine recompiles and reactivate itself every policy installation regardless of the values of `inspect2c_compile` and `inspect2c_activate`. |
| `off` | Deactivates the engine if active. Subsequent policy installation on the gateway do NOT auto-activate the engine unless the command is used again. |
| `stat` | Print the status of the engine. For example: "During compilation", "Before auto-activation", "Deactivated". |
| `setdefault` | Restore control to database settings. Security Management server settings are ignored.<br>At the next policy installation, return the control of the engine to the values of the following gateway database attributes:<br>• `inspect2c_compile` (true/false) - controls whether or not the engine is compiled on the gateway during policy installation. Compilation is performed in the background and may take a few minutes.<br>• `inspect2c_activate` (true/false) - controls whether the engine is automatically activated after it is compiled. When set to true, the engine is compiled regardless of the value of `inspect2c_compile`.<br>Use GuiDBEdit to change the values of the attributes. |

DRAFT

# fw ctl multik stat

**Description** Displays multi-kernel statistics for each kernel instance. The state and processing core number of each instance is displayed, along with:

- The number of connections currently being handled.
- The peak number of concurrent connections the instance has handled since its inception.

# fw ctl sdstat

**Description** The IPS performance counters measure the percentage of CPU consumed by each IPS protection. The measurement itself is divided according to the type of protection: Pattern based protections or INSPECT based protections. In addition, the IPS counters measure the percentage of CPU used by each section ("context") of the protocol, and each protocol parser.

**Usage**
```
fw ctl zdebug >& outputfile
fw ctl sdstat start
fw ctl sdstat stop
```

**Syntax**

| Argument | Description |
|---|---|
| `fw ctl zdebug >& outputfile` | Turn on debug mode and specify an output file. |
| `fw ctl sdstat start` | Activate the IPS counters |
| `fw ctl sdstat stop` | Print a report and stop the counters. |

**Example** The workflow is as follows:

Run the following commands on the Check Point Security Gateway (version R70 or higher):

On the Check Point Security Gateway:

- Run `fw ctl zdebug >& outputfile`
- Run `fw ctl sdstat start`

Let the counters run. However- do not leave the counters on for more than 10 minutes.

- Run `fw ctl sdstat stop`

It is important to stop the counters explicitly, otherwise there may be performance penalty

This generates the output file `outputfile` that must be processed on the (SecurePlatform only) Security Management Server.

On the Security Management Server:

- From `$FWDIR/script`, run the script `./sdstat_analyse.csh outputfile`

The output of the script is a report in csv format that can be viewed in Microsoft Excel.

If there is a problem in the report, or if more details are needed, a debug flag is available which prints extra information to outputfile.

- Run `fw ctl zdebug + spii >& outputfile`

| Example Debug Message | Explanation |
|---|---|
| `sdstat_get_stats_all_instances : Smart Defense report objects are not initalized, hence no report can be done.` | User tried to create a report without initializing the counters, or an error occurred during initialization and the user then tried to print a report. |
| `FW-1 - sdstats_print_report: Failed to calculate Smart Defense (total_smart_defense is 0)` | The measurement process failed and the total time units for IPS is zero. |

DRAFT

**Comments**

1. A value in the report of "< 1" means that the percentage of CPU used by a protection is less than 1%.
2. The report generated by the sdstat_analyse script may contain a number instead of a protection name. This is because the original output contains a signature id, but the id is missing from the Security Policy on the Gateway.

# fw fetch

**Description** Fetches the Inspection Code from the specified host and installs it to the kernel.

**Usage** `fw fetch [-n] [-f <filename>] [-c] [-i] master1 [master2] ...`

**Syntax**

| Argument | Description |
|---|---|
| `-n` | Fetch the Security Policy from the Security Management server to the local `state` directory, and install the Policy only if the fetched Policy is different from the Policy already installed. |
| `-f <filename>` | Fetch the Security Policy from the Security Management server listed in <filename>. If filename is not specified, the list in `conf/masters` is used. |
| `-c` | Cluster mode, get policy from one of the cluster members, from the Check Point High Availability (CPHA) kernel list. |
| `-i` | Ignore SIC information (for example, SIC name) in the database and use the information in `conf/masters`. This option is used when a Security Policy is fetched for the first time by a DAIP gateway from a Security Management server with a changed SIC name. |
| `master1` | Execute command on the designated master.<br>The IP address of the Security Management Server from which to fetch the Policy. You can specify one or more servers, which will be searched in the order listed.<br>Corrected according to CR00777654<br>If no `targets` is not specified, or if `targets` is inaccessible, the Policy is fetched from `localhost`. |

DRAFT

# fw fetchlogs

**Description** `fw fetchlogs` fetches Log Files from a remote machine. You can use the `fw fetchlogs` command to transfer Log Files to the machine on which the `fw fetchlogs` command is executed. The Log Files are read from and written to the directory `$FWDIR/log`.

**Usage** `fw fetchlogs [[-f file name] ... ]` *module*

**Syntax**

| Argument | Description |
|---|---|
| `-f filename` | The Log Files to be transferred. The file name can include wildcards. In Solaris, any file containing wildcards should be enclosed in quotes.<br>The default parameter is `*.log`.<br>Related pointer files will automatically be fetched. |
| `module` | The name of the remote machine from where you transfer the Log Files. |

**Comments** The files transferred by the fw fetchlogs command are MOVED from the source machine to the target machine. This means that they are deleted from the source machine once they have been successfully copied.

**Fetching Current Log Data**

The active Log File (`fw.log)` cannot be fetched. If you want to fetch the most recent log data, proceed as follows:

- Run \ to close the currently active Log File and open a new one.
- Run `fw lslogs` to see the newly-generated file name.
- Run `fw fetchlogs -f` *filename* to transfer the file to the machine on which the `fw fetchlogs` command is executed. The file is now available for viewing in the SmartView Tracker.

After a file has been fetched, it is renamed. The gateway name and the original Log File name are concatenated to create a new file name. The new file name consists of the gateway name and the original file name separated by two (underscore) _ _ characters.

**Example** The following command:

```
fw fetchlogs -f 2001-12-31_123414.log module3
```

fetches the Log File `2001-12-31_123414.log` from `Module3`.

After the file has been fetched, the Log File is renamed:

```
module3_ _2001-12-31_123414.log
```

**Further Info.** See the *R75.20 Security Management Administration Guide* (http://supportcontent.checkpoint.com/documentation_download?ID=12277). http://supportcontent.checkpoint.com/documentation_download?ID=8745

# fw hastat

**Description** The `fw hastat` command displays information about High Availability machines and their states.

**Usage** `fw hastat [<target>]`

**Syntax**

| Argument | Description |
|---|---|
| `<target>` | A list of machines whose status will be displayed. If `target` is not specified, the status of the local machine will be displayed. |

# fw isp_link

**Description** Takes down (or up) a redundant ISP link.

**Usage** `fw isp_link [target] link-name {up|down}`

DRAFT

**Syntax**

| Argument | Description |
|---|---|
| `target` | The name of the Check Point gateway. |
| `link-name` | The name of the ISP link as defined in the ISP-redundancy tab. |

**Comments** This command can be executed locally on the Check Point Security Gateway or remotely from the Security Management server. In the latter case, the target argument must be supplied. For this command to work, the Check Point Security Gateway should be using the ISP redundancy feature.

# fw kill

**Description** Prompts the kernel to shut down all firewall daemon processes. The command is located in the `$FWDIR/bin directory` on the Security Management server or gateway machine.

The firewall daemons and Security servers write their `pids` to files in the `$FWDIR/tmp directory` upon startup. These files are named `$FWDIR/tmp/daemon_name.pid`. For example, the file containing the `pid` of the firewall `snmp` daemon is: `$FWDIR/tmp/snmpd.pid`.

**Usage** `fw kill [-t sig_no] proc-name`

**Syntax**

| Argument | Description |
|---|---|
| `-t sig_no` | This Unix only command specifies that if the file `$FWDIR/tmp/proc-name.pid` exists, send `signal sig_no` to the `pid` given in the file.<br>If no signal is specified, signal 15 (`sigterm` or the terminate command) is sent. |
| `proc-name` | Prompt the kernel to shut down specified firewall daemon processes. |

**Comments** In Windows, only the default syntax is supported: `fw kill proc_name.` If the `-t` option is used it is ignored.

# fw lea_notify

**Description** Send a `LEA_COL_LOGS` event to all connected lea clients, see the *LEA Specification* documentation. It should be used after new log files have been imported (manually or automatically) to the `$FWDIR/log` directory in order to avoid the scheduled update which takes 30 minutes.

This command should be run from the Security Management server.

**Usage** `fw lea_notify`

# fw lichosts

**Description** Print a list of hosts protected by Security Gateway products. The list of hosts is in the file `$fwdir/database/fwd.h`

**Usage** `fw lichosts [-x] [-l]`

**Syntax**

| Argument | Description |
|---|---|
| `-x` | Use hexadecimal format. |
| `-l` | Use long format. |

DRAFT

# fw log

**Description** `fw log` displays the content of Log files.

**Usage** `fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert_name|all)] [-g] [logfile]`

**Syntax**

| Argument | Description |
|---|---|
| `-f [-t]` | After reaching the end of the currently displayed file, do not exit (the default behavior), but continue to monitor the Log file indefinitely and display it while it is being written.<br>The `-t` parameter indicates that the display is to begin at the end of the file, in other words, the display will initially be empty and only new records added later will be displayed.<br>`-t` must come with a `-f` flag. These flags are relevant only for active files. |
| -n | Do not perform DNS resolution of the IP addresses in the Log file (the default behavior). This option significantly speeds up the processing. |
| -l | Display both the date and the time for each log record (the default is to show the date only once above the relevant records, and then specify the time per log record). |
| -o | Show detailed log chains (all the log segments a log record consists of). |
| `-c action` | Display only events whose action is action, that is, accept, drop, reject, authorize, deauthorize, encrypt and decrypt. Control actions are always displayed. |
| `-h host` | Display only log whose origin is the specified IP address or name. |
| `-s starttime` | Display only events that were logged after the specified time (see format below). `starttime` may be a date, a time, or both. If date is omitted, then today's date is assumed. |
| `-e endtime` | Display only events that were logged before the specified time (see format below). `endtime` may be a date, a time, or both. |
| `-b starttime endtime` | Display only events that were logged between the specified start and end times (see format below), each of which may be a date, a time, or both. If date is omitted, then today's date is assumed. The start and end times are expected after the flag. |
| -u `unification_scheme_file` | Unification scheme file name. |

DRAFT

| Argument | Description |
|---|---|
| `-m unification_mode` | This flag specifies the unification mode.<br>• `initial` - the default mode, specifying complete unification of log records; that is, output one unified record for each id. This is the default. When used together with `-f`, no updates will be displayed, but only entries relating to the start of new connections. To display updates, use the `semi` parameter.<br>• `semi` - step-by-step unification, that is, for each log record, output a record that unifies this record with all previously-encountered records with the same id.<br>• `raw` - output all records, with no unification. |
| -a | Output account log records only. |
| -k alert_name | Display only events that match a specific alert type. The default is `all`, for any alert type. |
| -g | Do not use a delimited style. The default is:<br>• `:` after field name<br>• `;` after field value |
| `logfile` | Use `logfile` instead of the default Log file. The default Log File is `$FWDIR/log/fw.log`. |

Where the full date and time format is: `MMM DD, YYYY HH:MM:SS`. For example: `May 26, 1999 14:20:00`

It is possible to specify date only in the format `MMM DD, YYYY`, or time only, in the format: `HH:MM:SS`, where time only is specified, the current date is assumed.

**Example**

```
fw log
fw log | more
fw log -c reject
fw log -s "May 26, 1999"
fw log -f -s 16:00:00
```

**Output** `[<date>] <time> <action> <origin> <interface dir and name> [alert] [field name: field value;] ...`

Each output line consists of a single log record, whose fields appear in the format shown above.

**Example**

```
14:56:39 reject jam.checkpoint.com >daemon alert src:
veredr.checkpoint.com; dst: jam.checkpoint.com; user: a; rule: 0;
reason: Client Encryption: Access denied - wrong user name or
password  ; scheme: IKE; reject_category: Authentication error;
product: Security Gateway
      14:57:49 authcrypt jam.checkpoint.com >daemon src:
veredr.checkpoint.com; user: a; rule: 0; reason: Client Encryption:
Authenticated by Internal Password; scheme: IKE; methods: AES-
256,IKE,SHA1; product: Security Gateway;
      14:57:49 keyinst jam.checkpoint.com >daemon src:
veredr.checkpoint.com; peer gateway: veredr.checkpoint.com; scheme:
IKE; IKE: Main Mode completion.; CookieI: 32f09ca38aeaf4a3; CookieR:
73b91d59b378958c; msgid: 47ad4a8d; methods: AES-256 + SHA1, Internal
Password; user: a;  product: Security Gateway;
```

DRAFT

# fw logswitch

**Description** `fw logswitch` creates a new active Log File. The current active Log File is closed and renamed by default `$FWDIR/log/`*current_time_stamp*`.log` unless you define an alternative name that is unique. The format of the default name *current_time_stamp*`.log` is `YYYY-MM-DD_HHMMSS.log`. For example: `2003-03-26_041200.log`

**Warning:**

- The Logswitch operation fails if a log file is given an pre-existing file name.
- The rename operation fails on Windows if the active log that is being renamed, is open at the same time that the rename operation is taking place; however; the Logswitch will succeed and the file will be given the default name `$FWDIR/log/current_time_stamp.log`.

The new Log File that is created is given the default name `$FWDIR/log/fw.log`. Old Log Files are located in the same directory.

A Security Management server can use `fw logswitch` to switch a Log File on a remote machine and transfer the Log File to the Security Management server. This same operation can be performed for a remote machine using fw lslogs (on page 143) and fw fetchlogs (on page 133).

When a log file is sent to the Security Management server, the data is compressed.

**Usage** `fw logswitch [-audit] [`*filename*`]`

`fw logswitch -h hostname [+|-][`*filename*`]`

**Syntax**

| Argument | Description |
|---|---|
| `-audit` | Does logswitch for the Security Management server audit file. This is relevant for local activation. |
| `filename` | The name of the file to which the log is saved. If no name is specified, a default name is provided. |
| `-h hostname` | The resolvable name or IP address of the remote machine (running either a Security Gateway or a Security Management server) on which the Log File is located. The Security Management server (on which the `fw logswitch` command is executed) must be defined as one of `host`'s Security Management servers. In addition, you must initialize SIC between the Security Management server and the `host`. |
| `+` | Switch a remote log and copy it to the local machine. |
| `-` | Switch a remote log and move it to the local machine thereby deleting the log from the remote machine. |

**Comments** Files are created in the `$FWDIR/log` directory on both `host` and the Security Management server when the `+` or `-` parameters are specified. Note that if `-` is specified, the Log File on the host is deleted rather than renamed.

`hostname` specified:

- `filename` specified - On `hostname`, the old Log File is renamed to `old_log`. On the Security Management server, the copied file will have the same name, prefixed by `hostname`'s name. For example, the command `fw logswitch -h venus +xyz` creates a file named `venus_xyz.log` on the Security Management server.
- `filename` not specified - On `hostname`, the new name is
  the current date, for example: `2003-03-26_041200.log`.
  On the Security Management server, the copied file will have the same name, but prefixed by `hostname_`. For example, `target_2003-03-26_041200.log`.

DRAFT

`hostname` not specified:

- `filename` specified - On the Security Management server, the old Log File is renamed to `old_log`.
- `filename` not specified - On the Security Management server, the old Log File is renamed to the current date.

**Compression**

When log files are transmitted from one machine to another, they are compressed using the zlib package, a standard package used in the Unix `gzip` command (see RFC 1950 to RFC 1952 for details). The algorithm is a variation of LZ77 method.

The compression ratio varies with the content of the log records and is difficult to predict. Binary data are not compressed, but string data such as user names and URLs are compressed.

# fw mergefiles

**Description** Merge several Log Files into a single Log File. The merged file can be sorted according to the creation time of the Log entries, and the times can be "fixed" according to the time zones of the origin Log servers.

Logs entries with the same Unique-ID are unified. If a Log switch was performed before all the segments of a specific log were received, this command will merge the records with the same Unique-ID from two different files, into one fully detailed record.

**Usage**
```
fw mergefiles [-s] [-t time_conversion_file]
log_file_name_1 [... log_file_name_n] output_file
```

**Syntax**

| Argument | Description |
|---|---|
| `-s` | Sort merged file by log records time field. |
| `-t time_conversion_file` | Fix different GMT zone log records time in the event that the log files originated from Log Servers in different time zone.<br>The time_conversion_file format is as follows:<br>ip-address signed_date_time_in_seconds<br>ip-address signed_date_time_in_seconds |
| log_file_name_n | *Full pathnames* of the Log File(s). |
| *output_file* | Full pathname of the output Log File. |

**Comments** It is not recommended to merge the current active `fw.log file` with other Log Files. Instead, run the `fw logswitch` command and then run `fw mergefiles`.

# fw monitor

**Description** Inspecting network traffic is an essential part of troubleshooting network deployments. `fw monitor` is a powerful built-in tool to simplify the task of capturing network packets at multiple capture points within the firewall chain. These packets can be inspected using industry-standard tools later on.

In many deployment and support scenarios capturing network packets is an essential functionality. tcpdump or snoop are tools normally used for this task. `fw monitor` provides an even better functionality but omits many requirements and risks of these tools.

- *No Security Flaws* — tcpdump and snoop are normally used with network interface cards in promiscuous mode. Unfortunately the promiscuous mode allows remote attacks against these tools. fw monitor does not use the promiscuous mode to capture packets. In addition most FireWalls' operating systems are hardened. In most cases this hardening includes the removal of tools like tcpdump or snoop because of their security risk.

DRAFT

- *Available on all Security Gateway installations* — `fw monitor` is a built-in firewall tool which needs no separate installation in case capturing packets is needed. It is a functionality provided with the installation of the FireWall package.
- *Multiple capture positions within the firewall kernel module chain* — `fw monitor` allows you to capture packets at multiple capture positions within the firewall kernel module chain; both for inbound and outbound packets. This enables you to trace a packet through the different functionalities of the firewall.
- *Same tool and syntax on all platforms* — Another important fact is the availability of `fw monitor` on different platforms. Tools like snoop or tcpdump are often platform dependent or have specific "enhancements" on certain platforms. `fw monitor` and all its related functionality and syntax is absolutely identical across all platforms. There is no need to learn any new "tricks" on an unknown platform.

Normally the Check Point kernel modules are used to perform several functions on packets (like filtering, encrypting and decrypting, QoS …). `fw monitor` adds its own modules to capture packets. Therefore fw monitor can capture all packets which are seen and/or forwarded by the FireWall.

Only one instance of `fw monitor` can be run at a time.

Use ^C (that is Control + C) to stop fw monitor from capturing packets.

**Usage** `fw monitor [-u|s] [-i] [-d] [-D] <{-e expr}+|-f <filter-file|->> [-l len] [-m mask] [-x offset[,len]] [-o <file>] <[-pi pos] [-pI pos] [-po pos] [-pO pos] | -p all > [-a] [-ci count] [-co count] [-vs vsid or vsname] [-h] -T`

**Syntax**

| Argument | Description |
|---|---|
| -u\|s | **Printing the UUID or the SUUID:** The option –u or –s is used to print UUIDs or SUUIDs for every packet. Please note that it is only possible to print the UUID or the SUUID – not both. |
| -i | **Flushing the standard output:** Use to make sure that captured data for each packet is at once written to standard output. This is especially useful if you want to kill a running fw monitor process and want to be sure that all data is written to a file. |
| [-d] [-D] | **Debugging fw monitor:** The -d option is used to start fw monitor in debug mode. This will give you an insight into `fw monitor`'s inner workings. This option is only rarely used outside Check Point. It is also possible to use `-D` to create an even more verbose output. |
| <{-e expr}+\|-f <filter-file\|->> | **Filtering fw monitor packets:** fw monitor has the ability to capture only packets in which you are interested. fw monitor filters use a subset of INSPECT to specify the packets to be captured. Set the filter expression:<br>• on the command line using the `-e` switch.<br>• by reading it from a file using the `-f` switch.<br>• by reading it from standard input using the `-f -` switch. |

DRAFT

| Argument | Description |
|---|---|
| -l len | **Limiting the packet length:** fw monitor allow you to limit the packet data which will be read from the kernel with -l. This is especially useful if you have to debug high sensitive communication. It allows you to capture only the headers of a packet (e.g. IP and TCP header) while omitting the actual payload. Therefore you can debug the communication without seeing the actual data transmitted. Another possibility is to keep the amount of data low. If you don't need the actual payload for debugging you can decrease the file site by omitting the payload. It's also very useful to reduce packet loss on high-loaded machines. fw monitor uses a buffer to transfer the packets from kernel to user space. If you reduce the size of a single packet this buffer won't fill up so fast. |
| -m mask | **Setting capture masks:** By default fw monitor captures packets before and after the virtual machine in both directions. These positions can be changed. This option allows you to specify in which of the four positions you are interested. |
| -x offset[,len] | **Printing packet/payload data:** In addition to the IP and Transport header fw monitor can also print the packets' raw data using the –x option. Optionally it is also possible to send all data that is written only to the screen the data written. |
| -o &lt;file&gt; | **Write output to file:** Save the raw packet data to a file in a standard (RFC 1761) format. The file can be examined using by tools like snoop, tcpdump or Ethereal.<br>**Note -** The snoop file format is normally used to store Layer 2 frames. For "normal" capture files this means that the frame includes data like a source and a destination MAC address. fw monitor operates in the firewall kernel and therefore has no access to Layer 2 information like MAC addresses. Instead of writing random MAC addresses, fw monitor includes information like interface name, direction and chain position as "MAC addresses". |
| -T | Print time stamp in microseconds. -T is needed only when -o is not used. When -o is used the exact time is written to the snoop file by default as of Corsica. |
| &lt;[-pi pos] [-pI pos] [-po pos] [-pO pos] \| -p all &gt; | **Insert fw monitor chain module at a specific position:** In addition to capture masks (which give the ability to look at packets in a specific position) fw monitor has the ability to define where exactly in the firewall chain the packets should be captured. This can be defined using these options. |
| -a | **Use absolute chain positions:** If you use fw monitor to output the capture into a file (option –o), one of the fields written down to the capture file is the chain position of the fw monitor chain module. Together with a simultaneous execution of `fw ctl` chain you can determine where the packet was captured. Especially when using –p all you will find the same packet captured multiples times at different chain positions. The option –a changes the chain id from an relative value (which only makes sense with the matching `fw ctl` chain output) to an absolute value. These absolute values are known to CPEthereal and can be displayed by it. |

DRAFT

| Argument | Description |
|---|---|
| [-ci count] [-co count] | **Capture a specific number of packets:** fw monitor enables you to limit the number of packets being captured. This is especially useful in situations where the firewall is filtering high amounts of traffic. In such situations fw monitor may bind so many resources (for writing to the console or to a file) that recognizing the break sequence (Control-C) might take very long. |
| [-vs vsid or vsname] | **Capture on a specific Virtual Router or Virtual Machine:** VPN-1 Power VSX enables you to run multiple Virtual Routers and FireWalls on one physical machine. Using the option –vs you can specify on which virtual component the packets should be captured. This option is only available on a VPN-1 Power VSX module. Please refer to fw monitor on FireWall-1 VSX for more information. |
| -h | Displays the usage. |

**Example** The easiest way to use `fw monitor` is to invoke it without any parameter. This will output every packet from every interface that passes (or at least reaches) the Check Point gateway. Please note that the same packet is appearing several times (two times in the example below). This is caused by `fw monitor` capturing the packets at different capture points.

**Output**

```
cpmodule]# fw monitor
 monitor: getting filter (from command line)
 monitor: compiling
monitorfilter:
Compiled OK.
 monitor: loading
 monitor: monitoring (control-C to stop)
eth0:i[285]: 172.16.1.133 -> 172.16.1.2 (TCP) len=285 id=1075
TCP: 1050 -> 18190 ...PA. seq=bf8bc98e ack=941b05bc
eth0:I[285]: 172.16.1.133 -> 172.16.1.2 (TCP) len=285 id=1075
TCP: 1050 -> 18190 ...PA. seq=bf8bc98e ack=941b05bc
eth0:o[197]: 172.16.1.2 -> 172.16.1.133 (TCP) len=197 id=44599
TCP: 18190 -> 1050 ...PA. seq=941b05bc ack=bf8bca83
eth0:O[197]: 172.16.1.2 -> 172.16.1.133 (TCP) len=197 id=44599
TCP: 18190 -> 1050 ...PA. seq=941b05bc ack=bf8bca83
eth0:o[1500]: 172.16.1.2 -> 172.16.1.133 (TCP) len=1500 id=44600
TCP
^C
: 18190 -> 1050 ....A. seq=941b0659 ack=bf8bca83
monitor: caught sig 2
 monitor: unloading
```

The first line of the `fw monitor` output is

```
eth0:i[285]: 172.16.1.133 -> 172.16.1.2 (TCP) len=285 id=1075
```

This packet was captured on the first network interface (eth0) in inbound direction before the virtual machine (lowercase i). The packet length is 285 bytes (in square parenthesis; repeated at the end of the line. Note that these two values may be different. The packets ID is 1075. The packet was sent from 172.16.1.133 to 172.16.1.2 and carries a TCP header/payload.

The second line of the fw monitor output is

```
TCP: 1050 -> 18190 ...PA. seq=bf8bc98e ack=941b05bc
```

The second line tells us that this is an TCP payload inside the IP packet which was sent from port 1050 to port 18190. The following element displays the TCP flags set (in this case PUSH and ACK). The last two elements are showing the sequence number (seq=bf8bc98e) of the TCP packet and the acknowledged sequence number (ack=941b05bc). You will see similar information for UDP packets.

You will only see a second line if the transport protocol used is known to fw monitor. Known protocols are for example TCP, UDP and ICMP. If the transport protocol is unknown or can not be analyzed because it is encrypted (e.g. ESP or encapsulated (e.g. GRE) the second line is missing.

**Further Info.** See SecureKnowledge solution sk30583 (http://supportcontent.checkpoint.com/solutions?id=sk30583).

# fw lslogs

**Description** Display a list of Log Files residing on a remote or local machine. You must initialize SIC between the Security Management server and the remote machine.

**Usage** `fw lslogs [[-f file name] ...] [-e] [-s name | size | stime | etime] [-r]` [*machine*]

**Syntax**

| Argument | Description |
|---|---|
| `-f filename` | The list of files to be displayed. The file name can include wildcards. In Unix, any file containing wildcards should be enclosed in quotes.<br>The default parameter is `*.log`. |
| -e | Display an extended file list. It includes the following data:<br>• `Size` - The size of the file and its related pointer files together.<br>• `Creation Time` - The time the Log File was created.<br>• `Closing Time` - The time the Log File was closed.<br>• `Log File Name` - The file name. |
| -s | Specify the sort order of the Log Files using one of the following sort options:<br>• `name` - The file name.<br>• `size` - The file size.<br>• `stime` - The time the Log File was created.<br>• `etime` - The time the Log File was closed.<br>The default is `stime`. |
| -r | Reverse the sort order (descending order). |
| *module* | The name of the machine on which the files are located. It can be a gateway or a Log Server. The default is localhost. |

**Example** This example shows the extended file list you see when you use the `fw lslogs -e` command:

```
fw lslogs -e module3
Size   Creation Time        Closing Time          Log file
name
99KB   10Jan2002 16:46:27   10Jan2002 18:36:05    2002-01-
10_183752.log
16KB   10Jan2002 18:36:05     --                  fw.log
```

DRAFT

# fw putkey

**Description** Install a Check Point authentication password on a host. This password is used to authenticate internal communications between Security Gateways and between a Check Point Security Gateway and its Security Management server. A password is used to authenticate the control channel the first time communication is established. This command is required for backward compatibility scenarios.

**Usage** `fw putkey [-opsec] [-no_opsec] [-ssl] [-no_ssl] [-k num] [-n <myname>] [-p <pswd>] host...`

**Syntax**

| Argument | Description |
|---|---|
| `-opsec` | Only control connections are enabled. |
| `-no_opsec` | Only OPSEC control connections are enabled. |
| `-ssl` | The key is used for an SSL connection. |
| `-no_ssl` | The key is not used for an SSL connection. |
| `-k num` | The length of the first S/Key password chain for fwa1 authentication (Check Point's proprietary authentication protocol). The default is 7. When fewer than 5 passwords remain, the hosts renegotiate a chain of length 100, based on a long random secret key. The relatively small default value ensures that the first chain, based on a short password entered by the user, is quickly exhausted. |
| `-n` <myname> | The IP address (in dot notation) to be used by the Check Point Security Gateway when identifying this host to all other hosts, instead of, for example, the resolution of the `hostname` command. |
| `-p <psw>` | The key (password). If you do not enter the password on the command line, you will be prompted for it. |
| `host` | The IP address(es) or the resolvable name(s) of the other host(s) on which you are installing the key (password). This should be the IP address of the interface "closest" to the host on which the command is run. If it is not, you will get error messages such as the following:<br>"`./fwd: Authentication with hostname for command sync failed`" |

**Comments** This command is never used in a script.

DRAFT

# fw repairlog

**Description** `fw repairlog` rebuilds a Log file's pointer files. The three files: *name*`.logptr`, *name*`.loginitial_ptr` and *name*`.logaccount_ptr` are recreated from data in the specified Log file. The Log file itself is modified only if the `-u` flag is specified.

**Usage** `fw repairlog [-u] logfile`

**Syntax**

| Argument | Description |
|---|---|
| `-u` | Indicates that the unification chains in the Log file should be rebuilt. |
| `logfile` | The name of the Log file to repair. |

# fw sam

**Description** Manage the Suspicious Activity Monitoring (SAM) server. Use the SAM server to block connections to and from IP addresses without the need to change the Security Policy.

SAM commands are logged. Use this command to (also) monitor active SAM requests (see `-M` option).

**To configure the SAM server** on the Security Management server or Security Gateway, use SmartDashboard to edit the **Advanced > SAM** page of the Check Point Security Gateway object.

**Usage** Add/Cancel SAM rule according to criteria:

```
fw sam [-v][-s <sam server>][-S <server sic name>][-f <fw host>][-t timeout][-l
log][-C] -<n|i|I|j|J> <Criteria>
```

Delete all SAM rules:

```
fw sam [-v][-s <sam server>][-S <server sic name>][-f <fw host>] -D
```

Monitor all SAM rules:

```
fw sam [-v][-s <sam server>][-S <server sic name>][-f <fw host>] -M -ijn all
```

Monitor SAM rules according to criteria:

```
fw sam [-v][-s <sam server>][-S <server sic name>][-f <fw host>] -M -ijn
<Criteria>
```

**Syntax**

| Parameter | Meaning |
|---|---|
| `-v` | Verbose mode. Writes one message (describing whether the command was successful or not) to `stderr` for each Security Gateway machine on which the command is enforced. |
| `-s sam_server` | The IP address (in dot format) or the resolvable name of the FireWalled host that will enforce the command. The default is `localhost`. |
| `-S server_sic_name` | The SIC name for the SAM server to be contacted. It is expected that the SAM server will have this SIC name, otherwise the connection will fail. If no server SIC name is supplied the connection will proceed without SIC names comparison. For more information about enabling SIC refer to the OPSEC API Specification. |
| `-f <fw host>` | Specify the `host`, the Security Gateway machine on which to enforce the action.<br>`host` can be one of the following (default is `All`):<br>• `localhost`—Specify the computer running the SAM server to enforce the action on it.<br>• The name of the object or group—the action is enforced on this object; if this object is a group, on every object in the group.<br>• `Gateways`—Action enforced on FireWalls defined as gateways and managed by Security Management server where the SAM server runs.<br>• `All`—Enforced on FireWalls managed by Smart- Center server where SAM server runs. |
| `-D` | Cancel all inhibit (`-i`, -j,`-I`,`-J`) and notify (`-n`) commands.<br>To "uninhibit" inhibited connections, execute `fw sam` with the `-C` or –`D` parameters. It is also possible to use this command for active SAM requests. |

DRAFT

| Parameter | Meaning |
|---|---|
| `-C` | Cancel the command to inhibit connections with the specified parameters. These connections will no longer be inhibited (rejected or dropped). The command parameters must match the ones in the original command, except for the `-t` (timeout) parameter. |
| `-t timeout` | The time period (in seconds) for which the action will be enforced. The default is forever or until cancelled. |
| `-l log` | The type of the log for enforced actions can be one of the following: `nolog`, `long_noalert`, `long_alert`. The default is `long_alert`. |
| `-n` | Notify, or generate, a long-format log entry. Generates an alert when connections that match the specified services or IP addresses pass through the FireWall. This action does not inhibit or close connections. |
| `-i` | Inhibit (do not allow) new connections with the specified parameters. Each inhibited connection is logged according to log type. Matching connections will be *rejected*. |
| `-I` | Inhibit new connections with the specified parameters, and close all existing connections with the specified parameters. Each inhibited connection is logged according to the log type. Matching connections will be *rejected*. |
| `-j` | Inhibit new connections with the specified parameters. Each inhibited connection is logged according to the log type. Connections will be *dropped*. |
| `-J` | Inhibit new connections with the specified parameters, and close all existing connections with the specified parameters. Each inhibited connection is logged according to the log type. Connections will be *dropped*. |
| `-M` | Monitor the active SAM requests with the specified actions and criteria. |
| `all` | Get all active requests. For monitoring purposes only. |

DRAFT

**Usage  Criteria are used to match connections, and are composed of various combinations of the following parameters:**

```
<source ip><source netmask><destination ip><destination netmask>
<service><protocol>
```

Possible combinations are:

```
src <ip>
dst <ip>
any <<ip>
subsrc <ip><netmask>
subdst <ip><netmask>
subany <ip><netmask>
srv <src ip><dest ip><service><protocol>
subsrv <src ip><src netmask><dest ip><dest netmask><service>
<protocol>
subsrvs <src ip><src netmask><dest ip><service><protocol>
subsrvd <src ip><dest ip><dest netmask><service><protocol>
dstsrv <dest ip><service><protocol>
subdstsrv <dest ip><dest netmask><service><protocol>
srcpr <ip><protocol>
dstpr <ip><protocol>
subsrcpr <ip><netmask><protocol>
subdstpr <ip><netmask><protocol>
```

**Syntax**

| Criteria Parameters | Description |
|---|---|
| `src <ip>` | Match the source IP address of the connection. |
| `dst <ip>` | Match the destination IP address of the connection. |
| `any <ip>` | Match either the source IP address or the destination IP address of the connection. |
| `subsrc <ip> <netmask>` | Match the source IP address of the connections according to the netmask. |
| `subdst <ip> <netmask>` | Match the destination IP address of the connections according to the netmask. |
| `subany <ip> <netmask>` | Match either the source IP address or destination IP address of connections according to the netmask. |
| `srv <src ip> <dst ip> <service> <protocol>` | Match the specific source IP address, destination IP address, service and protocol. |
| `subsrv <src ip> <netmask>`<br>`<dst ip> <netmask> <service> <protocol>` | Match the specific source IP address, destination IP address, service and protocol. Source and destination IP addresses are assigned according to the netmask. |
| `subsrvs <src ip> <src netmask> <dest ip> <service> <protocol>` | Match the specific source IP address, source netmask, destination netmask, service and protocol. |
| `subsrvd <src ip> <dest ip>`<br>`<dest netmask> <service> <protocol>` | Match specific source IP address, destination IP, destination netmask, service and protocol. |
| `dstsrv <dst ip> <service> <protocol>` | Match specific destination IP address, service and protocol. |
| `subdstsrv <dst ip> <netmask> <service> <protocol>` | Match specific destination IP address, service and protocol. Destination IP address is assigned according to the netmask. |
| `srcpr <ip> <protocol>` | Match the source IP address and protocol. |
| `dstpr <ip> <protocol>` | Match the destination IP address and protocol. |

DRAFT

| Criteria Parameters | Description |
|---|---|
| `subsrcpr <ip> <netmask> <protocol>` | Match the source IP address and protocol of connections. Source IP address is assigned according to the netmask. |
| `subdstpr <ip> <netmask> <protocol>` | Match the destination IP address and protocol of connections. Destination IP address is assigned according to the netmask. |

**Example** This command inhibits all connections originating on `louvre` for 10 minutes. Connections made during this time will be rejected:

```
fw sam -t 600 -i src louvre
```

This command inhibits all FTP connections from the `louvre` subnet to the `eifel` subnet. All existing open connections will be closed. New connection will be dropped, a log is kept and an alert is sent:

```
fw sam -l long_alert -J subsrvs louvre 255.255.255.0 eifel 21 6
```

The previous command will be enforced forever - or until canceled by the following command:

```
fw sam -C -l long_alert -J subsrvs louvre 255.255.255.0 eifel 21 6
```

This command monitors all active "inhibit" or "notify SAM" requests for which `lourve` is the source or destination address:

```
fw sam -M -nij any lourve
```

This command cancels the command in the first example:

```
fw sam -C -i src louvre
```

# fw stat

**Description** State tables are used to keep state information which the firewall virtual machine, and other components of the Security Gateway need in order to correctly inspect the packet. The tables are actually the 'memory' of the virtual machine in the kernel, and are the key component of Check Point Stateful Inspection technology. State tables are implemented as dynamic hash tables in kernel memory. All field values are in hexadecimal, apart from the time-out value at the end of the entry, when present.

The `fw tab` command displays the content of state tables on the target hosts in various formats. For each host, the default format displays the host name and a list of all tables with their elements.

**Usage** `fw tab [-all |-conf conffile] [-s][-m number][-u][-t tname][-x tname][-d] <targets>`

**Syntax**

| Argument | Description |
|---|---|
| `-all` | The command is to be executed on all targets specified in the default system configuration file (`$FWDIR/conf/sys.conf`). |
| `-conf conffile` | The command is to be executed on the targets specified in conffile. |
| `-s` | Summary of the number of entries in each table: host name, table name, table ID, and its number of entries |
| `-m number` | For each table, display only its first number of elements  (default is 16 entries at most). |
| `-u` | Do not limit the number of entries displayed for each table. |
| `-t tname` | Display only tname table. |
| `-x tname` | Delete all entries in all tables |

DRAFT

| Argument | Description |
|---|---|
| `-d` | Debug mode |
| `targets` | The command is executed on the designated targets. |

A table has a list of associated attributes.

**Example** To display only the `arp_table` table,

**Comments** `fw tab -t arp_table`

`fw sam -C -i src louvre`

# fw tab

**Description** The fw tab command enables you to view kernel table contents and change them (that is, only dynamic tables since the content of a static table is indeed static).

**Usage** `fw tab [-t <table>] [-s] -c] [-f] [-o <filename>] [-r] [-u | -m <maxvals>] [[-x | -a} -e entry] [-y] [hostname]"`

**Syntax**

| Argument | Description |
|---|---|
| `- t <table>` | Specifies a table for the command. |
| `-s` | Displays a short summary of the table (s) information. |
| `-y` | Specifies to not prompt a user before executing any commands. |
| `-f` | Displays a formatted version of the table content. Every table may have its own specific format style. |
| `-o <filename>` | Dumps CL formatted output to filename, which can later be read by fw log or any other entity that can read FW log formats. |
| `-c` | Displays formatted table information in common format. |
| `-r` | Resolves IP addresses in formatted output. |
| `-x, -a, -e` | It is possible to add or remove an entry from an existing dynamic table by using the -a or the -x flags, respectively. These flags must be followed by the -e flag and an entry description (<entry>).<br>⚠ **Caution** - Improper use of the -a and -x flags may cause system instability. |
| `[hostname]` | A list of one or more targets. When not used, the local machine is used as the default target. |

**Example** `fw tab -t <table-name> -a -e "1,2;3,4,5"` or
`fw tab -t <table-name> -a -e "<1,2;3,4,5>"`
Adds an entry: `<00000001,00000002,00000003,00000004,00000005,>to<table-name>`

`fw tab -t <table-name> -a -e "1,2,"` or
`fw tab -t <table-name> -a -e "<1,2>"`
Adds an entry with only a key field: `<00000001,00000002>`

If table`<table-name>` contains the following entry:
`<0000000,00000001,00000002>`
`fw tab -t <table-name> -x -e "0,1"` or
`fw tab -t <table-name> -x -e "0,1;2"`

DRAFT

Removes the entry from the specified table.

**Comments** If table has the 'expire' attribute, entries added using the -a flag will receive the default table timeout.
This feature only works on local machine kernel tables and does not work on a remote machine's tables like additional fw tab commands.
The -x flag can be used independently of the -e flag in which case the entire table content is deleted.
This feature should only be used for debug purposes. It is not advisable to arbitrarily change the content of any kernel table since doing so may have unexpected results including unexpected security and connectivity impacts.

# fw ver

**Description** Display the Security Gateway major and minor version number and build number.

**Usage** `fw ver [-k][-f <filename>]`

**Syntax**

| Argument | Description |
|---|---|
| -k | Print the version name and build number of the Kernel module. |
| `-f <filename>` | Print the version name and build number to the specified file. |

# fwm

**Description** Perform management operations on the Security Gateway. It controls *fwd* and all Check Point daemons.

**Usage** `fwm`

# fwm dbimport

**Description** Imports users into the Check Point User Database from an external file. You can create this file yourself, or use a file generated by `fwm dbexport`.

**Usage** `fwm dbimport [-m] [-s] [-v] [-r] [-k` *errors*`] [-f file] [-d` *delim*`]`

**Syntax**

| Argument | Description |
|---|---|
| `-m` | If an existing user is encountered in the import file, the user's default values will be replaced by the values in the template (the default template or the one given in the attribute list for that user in the import file), and the original values will be ignored. |
| `-s` | Suppress the warning messages issued when an existing user's values are changed by values in the import file. |
| `-v` | verbose mode |
| `-r` | `fwm dbimport` will delete all existing users in the database. |

DRAFT

| Argument | Description |
|---|---|
| `-k errors` | Continue processing until nerror errors are encountered.<br>The line count in the error messages starts from 1 including the attributes line and counting empty or commented out lines. |
| `-f file` | The name of the import file. The default import file is `$FWDIR/conf/user_def_file`. Also see the requirements listed under "File Format" on page 72. |
| `-d delim` | Specifies a delimiter different from the default value (`;`). |

**Comments** The IKE pre shared secret does not work when exporting from one machine and importing to another.

To ensure that there is no dependency on the previous database values, use the`-r` flag together with the `-m` flag.

**File Format**

The import file must conform to the following Usage:

- The first line in the file is an attribute list.
  - The attribute list can be any partial set of the following attribute set, as long as `name` is included:

    ```
    {name; groups; destinations; sources; auth_method;
    fromhour; tohour; expiration_date; color; days;
    internal_password; SKEY_seed; SKEY_passwd;
    SKEY_gateway; template; comments; userc}
    ```

- The attributes must be separated by a delimiter character.
  - The default delimiter is the `;` character. However, you can use a different character by specifying the `-d` option in the command line.
- The rest of the file contains lines specifying the values of the attributes per user. The values are separated by the same delimiter character used for the attribute list. An empty value for an attribute means use the default value.
- For attributes that contain a list of values (for example, days), enclose the values in curly braces, that is,`{}`. Values in a list must be separated by commas. If there is only one value in a list, the braces may be omitted. A `+` or `-` character appended to a value list means to add or delete the values in the list from the current default user values. Otherwise the default action is to replace the existing values.
- Legal values for the days attribute are: `MON`, `TUE`, `WED`, `THU`, `FRI`, `SAT`, `SUN`.
- Legal values for the authentication method are: `Undefined`, `S/Key`, `SecurID`, `Unix Password`, `VPN-1 & FireWall-1 Password, RADIUS, Defender`.
- Time format is `hh:mm`.
- Date format is `dd-mmm-yy,` where `mmm` is one of {`Jan`, `Feb`, `Mar`, `Apr`, `May`, `Jun`, `Jul`, `Aug`, `Sep`, `Oct`, `Nov`, `Dec`}.
- If the S/Key authentication method is used, all the other attributes regarding this method must be provided.
- If the Check Point password authentication method is used, a valid Check Point password should be given as well. The password should be encrypted with the C language `encrypt` function.
- Values regarding authentication methods other than the one specified are ignored.
- The `userc` field specifies the parameters of the user's SecuRemote connections, and has three parameters, as follows:
  - **key encryption method** – DES, CLEAR, Any
  - **data encryption method** – DES, CLEAR, Any
  - **integrity method - MD5,[blank]** = no data integrity.

DRAFT

    - "Any" means the best method available for the connection. This depends on the encryption methods available to both sides of the connection. For example,

      `{DES,CLEAR,}` means: key encryption method is DES; no data encryption; no data integrity.

- A line beginning with the `!` character is considered a comment.

# fwm expdate

**Description** Modify the expiration date of all users and administrators.

**Usage** `fw expdate dd-mmm-1976`

**Comments** The date can be modified using a filter.

**Example** `fw expdate 02-mar-2003 -f 01-mar-2003`

# fwm dbexport

**Description** Export the Check Point User Database to a file. The file may be in one of the following formats:

- the same Usage as the import file for `fwm dbimport`
- LDIF format, which can be imported into an LDAP server using `ldapmodify`

**Usage** To export the User Database to a file that can be used with `fwm dbimport`:

```
      fwm dbexport [ [-g group | -u user] [-d delim]
[-a {attrib1, attrib2, ...} ] [-f file] ]
```

To export the User Database as an LDIF file:

```
      fwm dbexport -l -p [-d] -s subtree [-f file]  [-k IKE-shared-secret]
```

**Syntax**

| Argument | Description |
|---|---|
| `-g group` | Specifies a group (`group`) to be exported. The users in the group are not exported. |
| `-u user` | Specifies that only one user (`user`) is to be exported. |
| `-d` | Debug flag |
| `-a {attrib1, attrib2, ...}` | Specifies the attributes to export, in the form of a comma-separated list, between {} characters, for example, `-a {name,days}`. If there is only one attribute, the {} may be omitted. |
| `-f file` | file specifies the name of the output file. The default output file is $FWDIR/conf/user_def_file. |
| `-l` | Create an LDIF format file for importation by an LDAP server. |
| `-p` | The profile name. |
| `-s` | The branch under which the users are to be added. |
| `-k` | This is the Account Unit's IKE shared secret (**IKE Key** in the **Encryption** tab of the **Account Unit Properties** window.) |

**Comments** Note:

DRAFT

- The IKE pre shared secret does not work when exporting from one machine and importing to another.
- If you use the `-a` parameter to specify a list of attributes, and then import the created file using `fwm dbimport`, the attributes not exported will be deleted from the user database.
- `fwm dbexport` and `fwm dbimport` (non-LDIF Usage) cannot export and import user groups. To export and import a user database, including groups, proceed as follows:

  * Run `fwm dbexport` on the source Security Management server.

  * On the destination Security Management server, create the groups manually.

  * Run `fwm dbimport` on the destination Security Management server.

The users will be added to the groups to which they belonged on the source Security Management server.

- If you wish to import different groups of users into different branches, run `fwm dbexport` once for each subtree, for example:

```
fwm dbexport -f f1 -l -s
ou=marketing,o=WidgetCorp,c=us

fwm dbexport -f f2 -l -s ou=rnd,o=WidgetCorp,c=uk
```

  Next, import the individual files into the LDAP server one after the other. For information on how to do this, refer to the documentation for your LDAP server.

- The LDIF file is a text file which you may wish to edit before importing it into an LDAP server. For example, in the Check Point user database, user names may be what are in effect login names (such as "maryj") while in the LDAP server, the DN should be the user's full name ("Mary Jones") and "maryj" should be the login name.

**Example** Suppose the User Database contains two users, "maryj" and "ben".

```
fwm dbexport -l -s o=WidgetCorp,c=us
```

creates a LDIF file consisting of two entries with the following DNs:

```
cn=ben,o=WidgetCorp,c=us

cn=maryj,o=WidgetCorp,c=us
```

# fwm dbload

**Description** Download the user database and network objects information to selected targets. If no target is specified, then the database is downloaded to localhost.

**Usage** `fwm dbload [-all | -conf conffile] [targets]`

**Syntax**

| Argument | Description |
|---|---|
| -all | Execute command on all targets specified in the default system configuration file (`$FWDIR/conf/sys.conf`). This file must be manually created. |
| -conf *conffile* | Only OPSEC control connections are enabled. |
| targets | Execute command on the designated targets. |

# fwm ikecrypt

**Description** `fwm ikecrypt` command line encrypts the password of a SecuRemote user using IKE. The resulting string must then be stored in the LDAP database.

DRAFT

**Usage** `fwm ikecrypt shared-secret user-password`

**Syntax**

| Argument | Description |
|---|---|
| `shared-secret` | The IKE Key defined in the **Encryption** tab of the **LDAP Account Unit Properties** window. |
| `user-password` | The SecuRemote user's password. |

**Comments** An internal CA must be created before implementing IKE encryption. An Internal CA is created during the initial configuration of the Security Management server, following installation.

## fw getcap

**Description** `fwm getcap` command line fetches the packet capture.

**Usage** `fwm getcap -g <gw> -u "{CAP_ID}" [-p <path>] [-c <domain>]`

**Syntax**

| Argument | Description |
|---|---|
| -g | host name of the gateway |
| -u | capture UID |
| -p | output pathname |
| -c | host name of the Domain Management Server |

## fwm load

**Description** Compile and install a Security Policy or a specific version of the Security Policy on the target's Security Gateways. This is done in one of two ways:

- `fwm load` compiles and installs an Inspection Script (`*.pf`) file on the designated Security Gateways.
- `fwm load` converts a Rule Base (`*.W`) file created by the GUI into an Inspection Script (`*.pf`) file then installs it to the designated Security Gateways.

Versions of the Security Policy and databases are maintained in a version repository on the Security Management server. Using this command specific versions of the Security Policy can be installed on a gateway (local or remote) without changing the definition of the current active database version on the Security Management server.

To protect a target, you must load a Policy that contains rules whose scope matches the target. If none of the rules are enforced on the target, then all traffic through the target is blocked.

**Usage** `fwm load [-p <plug-in product name>] [-S] <rulebase version name> <targets>`

**Syntax**

| Argument | Description |
|---|---|
| -S | The targets are UTM-1 Edge gateways. |
| -p | Specifies the product name if applicable. |
| rulebase | A Rule Base created by the GUI. Specify the name of the rulebase, such as `Standard` (case sensitive). |

DRAFT

| Argument | Description |
|---|---|
| -v version number | Retrieve the Security Policy from the version repository. The version number represents the number of the Security Policy as it is saved in the version repository. |
| targets | Execute command on the designated target. |

**Example** The following command installs the Security Policy `standard` in the target gateway `johnny.`

```
fwm load -v18 Standard johnny
```

# fwm lock_admin

**Description** View and unlock locked administrators.

**Usage** `fwm lock_admin [-v][-u administrator][-ua]`

**Syntax**

| Argument | Description |
|---|---|
| `-v` | View the names of all locked administrators. |
| `-u administrator` | Unlock a single administrator. |
| `-ua` | Unlock all locked administrators. |

# fwm logexport

**Description** `fwm logexport` exports the Log file to an ASCII file.

**Usage** `fwm logexport [-d delimiter] [-i filename] [-o outputfile] [-n] [-p] [-f] [-m <initial | semi | raw>] [-a]`

**Syntax**

| Argument | Description |
|---|---|
| `-d delimiter` | Set the output delimiter. The default is a semicolon (`;`). |
| `-i filename` | The name of the input Log file. The default is the active Log file, `fw.log` |
| `-o outputfile` | The name of the output file. The default is printing to the screen. |
| -n | Do not perform DNS resolution of the IP addresses in the Log file (this option significantly speeds the processing). |
| -p | Do not perform service resolution. A service port number is displayed. |
| -f | If this is the active Log file (`fw.log`), wait for new records and export them to the ASCII output file as they occur. |

DRAFT

| Argument | Description |
|---|---|
| -m | This flag specifies the unification mode.<br>• `initial` - the default mode. Complete the unification of log records; that is, output one unified record for each id.<br>• `semi` - step-by-step unification, that is, for each log record, output a record that unifies this record with all previously-encountered records with the same id.<br>• `raw` - output all records, with no unification. |
| -a | Show account records only (the default is to show all records). |

**Comments** **Controlling the Output of** `fwm logexport` **using** `logexport.ini`

The output of `fwm logexport` can be controlled by creating a file called `logexport.ini` and placing it in the `conf` directory: `$FWDIR/conf`.The `logexport.ini` file should be in the following format:

```
[Fields_Info]
included_fields =
field1,field2,field3,<REST_OF_FIELDS>,field100
excluded_fields = field10,field11
```

note that:

- the `num` field will always appear first, and cannot be manipulated using `logexport.ini`
- `<REST_OF_FIELDS>` is a reserved token that refers to a list of fields. It is optional. If `-f` option is set, `<REST_OF_FIELDS>` is based on a list of fields taken from the file `logexport_default.C`.
- If `-f` is not set, `<REST_OF_FIELDS>` will be based on the given input log file.
- It is not mandatory to specify *both* `included_fields` and `excluded_fields`.

**Format:**

The `fwm logexport` output appears in tabular format. The first row lists the names of all fields included in the subsequent records. Each of the subsequent rows consists of a single log record, whose fields are sorted in the same order as the first row. If a records has no information on a specific field, this field remains empty (as indicated by two successive semi-colons).

**Example**

```
num;date;time;orig;type;action;alert;i/f_name;i/f_dir;product;sys_message:;
service;s_port;src;dst;

      0; 5Dec2002;9:08:44;jam.checkpoint.com;control; ;;daemon;inbound;VPN-
1 & FireWall-1;The hme0 interface is not protected by the anti-spoofing
feature. Your network may be at risk;;;;;

      1; 5Dec2002;9:08:44;jam.checkpoint.com;control; ;;daemon;inbound;VPN-
1 & FireWall-1;;ftp;23456;1.2.3.4;3.4.5.6;
```

# fwm sic_reset

**Description** Reset the Internal CA and delete all the certificates from the Internal CA and the Internal CA itself. After running `sic_reset`, the ICA should be initialized through the `cpconfig` command. If this command is run all the certified IKE from the Internal CA should be removed (using the SmartConsole).

**Usage** `fwm sic_reset`

**Syntax**

| Argument | Description |
|---|---|
| sic_reset | Resets the internal CA SIC certificates and deletes the Internal CA. |

DRAFT

# fwm unload <targets>

**Description** Uninstall the currently loaded Inspection Code from selected targets.

**Usage** `fwm unload <targets>[-all | -conf conffile]`

**Syntax**

| Argument | Description |
|---|---|
| `targets` | Execute command on the designated targets. |
| `-all` | Execute command on all targets specified in the default system configuration file (`$FWDIR/conf/sys.conf`). This file must be manually created. |
| `conf conffile` | Execute command on targets specified in the `conffile`. |

# fwm ver

**Description** `fwm ver` displays the build number.

**Usage** `fwm ver [-f <filename>]`

# fwm verify <policy-name>

**Description** The `fwm verify <policy-name>` command verifies the specified policy package without installing it.

**Usage** `fwm verify <policy-name>`

**Syntax**

| Argument | Description |
|---|---|
| <policy-name> | The name of an available policy package. |

DRAFT

# Chapter 11

# VPN Commands

In This Chapter

## VPN

**Description** VPN commands generate status information regarding VPN processes, or are used to stop and start specific VPN services. All VPN commands are executed on the Security Gateway. The vpn command sends to the standard output a list of available commands.

**Usage** `vpn`

**Comments** Sends to the standard output a list of available commands.

## vpn accel

**Description** Perform operations on VPN accelerator cards (encryption only cards, not the full SecureXL cards). The command comes in three flavours -- for turning the accelerator card on and off, for collecting statistics, and enabling or disabling the accelerator card or acceleration software.

**Usage**

```
vpn accel [-d vpnx] on|off
vpn accel [-d vpnx] stat[-l]
vpn accel -d vpnx autostart on|off
```

**Syntax**

| Argument | Description |
|---|---|
| `autostart on|off` | Automatically starts/stops the vpnx accelerator software |
| `on/off` | Enable/disable accelerator card or vpnx accelerator module |
| `stat [-l]` | Reports the status of the accelerator card in long format |

**Example** `vpn accel -d vpnx stat`

**Output**

DRAFT

```
VPN-1: VPNx started
  Number of initialization errors: 0
  Number of processing errors: 0

vpn accel -d vpnx stat -l
VPN-1: VPNx started
  Number of initialization errors: 0
  Number of processing errors: 0
  Number of ESP valid contexts: 0
  Number of packets queued to the accelerator: 0
  High water mark of number of packets in queue: 1
```

**Example** `vpn accel -d vpnx stat -l`

**Output**

```
VPN-1: VPNx started
  Number of initialization errors: 0
  Number of processing errors: 0

vpn accel -d vpnx stat -l
VPN-1: VPNx started
  Number of initialization errors: 0
  Number of processing errors: 0
  Number of ESP valid contexts: 0
  Number of packets queued to the accelerator: 0
  High water mark of number of packets in queue: 1



  Number of packets and bytes since last activation
 --------------------------------------------------------------
                                   Packets                  Bytes
 --------------------------------------------------------------
    ESP decrypted                       52                   7072
    ESP encrypted                       52                   7072
    ESP total                          104                  14144
    Total                              104                  14144



  Average rates for the last 42.343 seconds
 --------------------------------------------------------------
                               Packets/sec               Kbit/sec
 --------------------------------------------------------------
    ESP decrypted                        0                   0.00
    ESP encrypted                        0                   0.00
    ESP total                            0                   0.00
    Total                                0                   0.00
```

# vpn compreset

**Description** Reset the compression/decompression statistics to zero.

**Usage** `vpn compreset`

**Comments** Run this command before running `vpn compstat`. This command is mostly obsolete. More compression/decompression information is available via `cpstat`.

# vpn compstat

**Description** Display compression/decompression statistics.

**Usage** `vpn compstat`

**Comments** This command is mostly obsolete. More compression/decompression information is available via `cpstat`.

# vpn crl_zap

**Description** Erase all Certificate Revocation Lists (CRLs) from the cache.

**Usage** `vpn crl_zap`

**Return Value** 0 for success; any other value equals failure.

# vpn crlview

**Description** Retrieve the Certificate Revocation List (CRL) from various distribution points and displays it for the user. The command comes in three flavors:

- `vpn crlview -obj <MyCA> -cert <MyCert>`. The VPN daemon contacts the Certificate Authority called **MyCA** and locates the certificate called **MyCert**. The VPN daemon extracts the certificate distribution point from the certificate then goes to the distribution point, which might be an LDAP or HTTP server. From the distribution point, the VPN daemon retrieves the CRL and displays it to the standard output.
- `vpn crlview -f d:\temp\MyCert`. The VPN daemon goes to the specified directory, extracts the certificate distribution point from the certificate, goes to the distribution point, retrieves the CRL, and displays the CRL to the standard output.
- `vpn crlview -view <lastest_CRL>`. If the CRL has already been retrieved, this command instructs the VPN daemon to display the contents to the standard output.

**Usage**

```
vpn crlview -obj <object name> -cert <certificate name>
vpn crlview -f <filename>
vpn crlview -view
```

**Syntax**

| Argument | Description |
|---|---|
| `-obj -cert` | • -obj refers to the name of the CA network object<br>• -cert refers to the name of the certificate |
| `-f` | Refers to the filename of the certificate |
| `-view` | Views the CRL |
| `-d` | Debug option |

**Return Value** 0 for success; any other value equals failure.

# vpn debug

**Description** Instruct the VPN daemon to write debug messages to the VPN log file: in `$FWDIR/log/vpnd.elg`. Debugging of the VPN daemon takes place according to topics and levels. A topic is a specific area on which to perform debugging, for example if the topic is LDAP, all traffic between the VPN daemon and the LDAP server are written to the log file. Levels range from 1-5, where 5 means "write all debug messages".

This command makes use of **TdError**, a Check Point infrastructure for reporting messages and debug information. There is no legal list of topics. It depends on the application or module being debugged.

To debug all available topics, use: ALL for the debug topic.

IKE traffic can also be logged. IKE traffic is logged to `$FWDIR/log/IKE.elg`

**Usage**

```
Usage: vpn debug < on [ DEBUG_TOPIC=level ] | off | ikeon | ikeoff |
trunc | timeon <SECONDS>| timeoff
```

DRAFT

```
vpn debug on DEBUG_TOPIC=level |off timeon<SECONDS>]|timeoff
vpn debug ikeon | ikeoff timeon|timeoff
vpn debug trunc
```

**Syntax**

| Argument | Description |
|---|---|
| `on` | Turns on high level vpn debugging. |
| `on topic=level` | Turns on the specified debug topic on the specified level. Log messages associated with this topic at the specified level (or higher) are sent to `$FWDIR/log/vpnd.elg` |
| `off` | Turns off all vpn debugging. |
| `timeon/timeoff` | Number of seconds to run the debug command |
| `ikeon` | Turns on IKE packet logging to: `$FWDIR/log/IKE.elg` |
| `ikeoff` | Turns of IKE logging |
| `trunc` | Truncates the `$FWDIR/log/IKE.elg` file, switches the cyclic vpnd.elg (changes the current `vpnd.elg` file to `vpnd0.elg` and creates a new `vpnd.elg`),enables vpnd and ike debugging and adds a timestamp to the `vpnd.elg` file. |

**Return Value** 0= success, failure is some other value, typically -1 or 1.

**Example** `vpn debug on all=5 timeon 5.`

This writes all debugging information for all topics to the vpnd.elg file for five seconds.

**Comments** IKE logs are analyzed using the support utility `IKEView.exe.`

DRAFT

# vpn drv

**Description** Install the VPN kernel (vpnk) and connects to the firewall kernel (fwk), attaching the VPN driver to the Firewall driver.

**Usage** `vpn drv on|off`

```
vpn drv stat
```

**Syntax**

| Argument | Description |
|---|---|
| `on/off` | Starts/stops the VPN kernel |
| `stat` | Returns the status of the VPN kernel, whether the kernel is on or off |

# vpn export_p12

**Description** Export information contained in the network objects database and writes it in the PKCS#12 format to a file with the p12 extension.

**Usage** `vpn export_12 -obj <network object> -cert <certificate object> -file <filename> -passwd <password>`

**Syntax**

| Argument | Description |
|---|---|
| -obj | Name of the gateway network object |
| -cert | Name of the certificate |
| -file | What the file with the p12 should be called |
| -passwd | Password required to open the encrypted p12 file |

**Return Value** 0 for success; any other value equals failure.

**Example** `vpn export_p12 -obj Gateway1 -cert MyCert -file mycert.p12 -passwd kdd432`

# vpn macutil

This command is related to Remote Access VPN, specifically Office mode, generating a MAC address per remote user. This command is relevant only when allocating IP addresses via DHCP.

Remote access users in Office mode receive an IP address which is mapped to a hardware or MAC address. This command displays a generated hardware or MAC address for each name you enter.

**Usage** `vpn macutil <username>`

**Example** vpn macutil John

**Output**

```
20-0C-EB-26-80-7D, "John"
```

# vpn nssm_toplogy

**Description** Generate and upload a topology (in NSSM format) to a Nokia NSSM server for use by Nokia clients.

**Usage** `vpn nssm_topology -url <"url"> -dn <"dn"> -name <"name"> -pass <"password"> [-action <bypass|drop>][-print_xml]`

**Syntax**

| Argument | Description |
|---|---|
| `-url` | URL of the Nokia NSSM server |
| `-dn` | Distinguished name of the NSSM server needed to establish an SSL connection |
| `-name` | Valid Login name for NSSM server |
| `-pass` | Valid password for NSSM server |
| `-action` | Specifies the action the symbian client should take if the packet is not destined for an IP address in the VPN domain. Legal options are **Bypass** (default) or **Drop** |
| `-print_xml` | The topology is in XLM format. This flag writes that topology to a file in XLM format. |

DRAFT

# vpn overlap_encdom

**Description** Display all overlapping VPN domains. Some IP addresses might belong to two or more VPN domains. The command alerts for overlapping encryption domains if one or both of the following conditions exist:

- The same VPN domain is defined for both gateway
- If the gateway has multiple interfaces, and one or more of the interfaces has the same IP address and netmask.

If the gateway has multiple interfaces, and one or more of the interfaces have the same IP address and netmask

**Usage** `vpn overlap_encdom [communities | traditional]`

**Syntax**

| Argument | Description |
|---|---|
| `Communities` | With this flag, all pairs of objects with overlapping VPN domains are displayed -- but only if the objects (that represent VPN sites) are included in the same VPN community. This flag is also used if the same destination IP can be reached via more than one community. |
| `Traditional` | Default flag. All pairs of objects with overlapping VPN domains are displayed. |

**Example** `vpn overlap_encdom communities`

**Output**

```
c:\> vpn overlap_encdom communitie
The objects Paris and London have overlapping encryption
domains.
The overlapping domain is:
10.8.8.1 - 10.8.8.1
10.10.8.0 - 10.10.9.255
- This overlapping encryption domain generates a multiple entry
points configuration in MyIntranet and RemoteAccess communities.
- Same destination address can be reached in more than one
community (Meshed, Star). This configuration is not supported.

The objects Paris and Chicago have overlapping encryption
domains. The overlapping domain is:
10.8.8.1 - 10.8.8.1
- Same destination address can be reached in more than one
community (MyIntranet, NewStar). This configuration is not
supported.

The objects Washington and Tokyo have overlapping encryption
domains.
The overlapping domain is:
10.12.10.68 - 10.12.10.68
10.12.12.0 - 10.12.12.127
10.12.14.0 - 10.12.14.255
- This overlapping encryption domain generates a multiple entry
points configuration in Meshed, Star and NewStar communities.
```

# vpn sw_topology

**Description** Download the topology for a SofaWare gateway.

**Usage** `vpn [-d] sw_toplogy -dir <directory> -name <name> -profile <profile> [-filename <filename>]`

**Syntax**

| Argument | Description |
|---|---|
| `-d` | Debug flag |
| `-dir` | Output directory for file |
| `-name` | Nickname of site which appears in remote client |
| `-profile` | Name of the sofaware profile for which the topology is created |
| `-filename` | Name of the output file |

# vpn tu

**Description** Launch the TunnelUtil tool which is used to control VPN tunnels.

**Usage** `vpn tu`

`vpn tunnelutil`

**Example** vpn tu

**Output**

```
**********      Select Option     **********

(1)              List all IKE SAs
(2)              List all IPsec SAs
(3)              List all IKE SAs for a given peer
(4)              List all IPsec SAs for a given peer
(5)              Delete all IPsec SAs for a given peer
(6)              Delete all IPsec+IKE SAs for a given
peer
(7)              Delete all IPsec SAs for ALL peers
(8)              Delete all IPsec+IKE SAs for ALL peers

(A)              Abort

*******************************************     vpn
debug
1
In Progress ...

ALL IKE SA
----------



Peer: 194.29.40.225     Cookies ebc5cf1c68c2925b-
27cb65c1afd28bc6

Peer: 194.29.40.225     Cookies 8670f30aa0a04a30-
4672a6998758071d
Hit <Enter> key to continue ...
```

**Further Info.** When viewing Security Associations for a specific peer, the IP address must be given in dotted decimal notation.

# vpn ver

**Description** Display the VPN major version number and build number.

**Usage** `vpn ver [-k] -f <filename>`

**Syntax**

| Argument | Description |
|---|---|
| `ver` | Displays the version name and version build number |
| `-k` | Displays the version name and build number and the kernel build number |
| `-f` | Prints the version number and build number to a text file. |

DRAFT

# Chapter 12

# SmartView Monitor Commands

In This Chapter

## RTM

**Description** This command and all its derivatives are used to execute SmartView Monitor operations.

### rtm debug

**Description** Send debug printouts to the $FWDIR/log/rtmd.elg file.

**Usage** `rtm debug <on | off> [OPSEC_DEBUG_LEVEL | TDERROR_<AppName>_<Topic>=<ErrLevel>]`

**Syntax**

| Argument | Description |
|---|---|
| on | Start debug mode |
| off | Stop debug mode |
| OPSEC_DEBUG_LEVEL | Turn on OPSEC debug printouts |
| TDERROR_RTM_ALL | Turn on SmartView Monitor debug printouts |

### rtm drv

**Description** Start, stop or check the status of the SmartView Monitor kernel driver.

**Usage** `rtm drv <on | off | stat>`

**Syntax**

| Argument | Description |
|---|---|
| on | Start the SmartView Monitor kernel driver |
| off | Stop the SmartView Monitor kernel driver |
| stat | SmartView Monitor kernel driver status |

DRAFT

# rtm monitor <module_name><interface_name> or rtm monitor <module_name>-filter

**Description** Starts the monitoring process and specify parameters for monitoring an interface.

**Usage**
```
rtm monitor <module_name><interface_name>[options]-g<grouping>
[entity-1...entity-n]
```
or
```
rtm monitor <module_name>-filter["complex filter"][options]-g<grouping>
[entity-1...entity-n]
```

**Syntax**

| Argument | Description |
|---|---|
| `-a` | <aggregate\|individual> |
| `-w` | <bandwidth\|loss\|rtt> |
| `-t` | <wire\|application> |
| `-i` | <number of seconds> |
| `@@` | specifies subrule<br>(for example, 'rule@@subrule') |
| `default values` | '-y bytes -a aggregate -w bandwidth -i2 |
| `grouping types` | svc\|src\|dst\|ip\|fgrule\|topsvc\|topsrc\|topdst\|topip\|topfw\|topfgrule |
| `module-name` | The name of the SmartView Monitor module. |
| `interface-name` | The name of the monitored interface. |
| `-d` | Specifies one of the following monitor directions:<br>- inbound<br>- outbound<br>- eitherbound |
| `inbound` | Monitors the inbound direction. |
| `outbound` | Monitors the outbound direction. |
| `eitherbound` | Monitors both directions. |
| `-y` | Specifies one of the following measurement units:<br>- bytes<br>- pkts<br>- line |
| `c` | Indicates the number of new connections opened per second. |
| `C` | Average concurrent connections |
| `-a` | Aggregate - displays a specific type of connections as an aggregate.<br>Individual - displays a specific type of connections as an individual. The defualt is eitherbound. |

DRAFT

| Argument | Description |
|---|---|
| -g | Specifies one of the following grouping options for monitored traffic:<br>- svc<br>- src<br>- dst<br>- ip<br>- fgrule<br>- topsvc<br>- topsrc<br>- topdst<br>- topdst<br>- topfwm<br>- topfgrule |
| svc | Monitors according to a service. |
| src | Monitors according to a network object (source only). |
| dst | Monitors according to a network object (destination only). |
| ip | Monitors according to a network object (source and destination). |
| fgrule | Monitors according to a QoS Policy rule. |
| topsvc | Monitors the traffic of the top 50 services. |
| topsrc | Monitors the traffic of the top 50 sources. |
| topdst | Monitors the traffic of the top 50 destinations. |
| topdst | Monitors traffic to and from the top 50 IP addresses (source of destination). |
| topfwn | Monitors according to the top 50 Firewall rules. |
| topfgrule | Monitors according to the top 50 QoS Policy rules. |
| -p | Specifies whether or not thousands will be separated by commas. |
| -filter | ["<complex filter>"] Only monitors traffic that matches the complex -filter boolean expression. |

DRAFT

**Example** The following command line displays monitoring data in bytes-per-sec for the top 50 services passed on any interface in both directions:

rtm monitor localhost -filter -g topsvc

The following command will display monitoring data in Conncurrent-Connections for the top 50 sources passed on interface eth0, inbound (that is, not telnet of http).

```
rtm monitor localhost -filter "[and[[interface 0 [[eth0in]]][svc 1 [telnet
http]]]" -y C -g topsrc
```

The default monitors all traffic on any interface in both directions.

**Comments** The specified entities should correspond to the specified grouping option. For example, if the monitoring process works according to a service (svc), all of the monitored services should be listed and separated by single spaces.

When monitoring occurs according to the QoS Policy rule (fgrule), 'rule@@subrule" should be used to specify a subrule entity.

There is no need to specify the top grouping options since they automatically monitor the top 50 entities according to the specified group.

**Example** The following command displays monitoring data in bytes-per-sec for the top 50 services passed on interface hme1.

```
rtm monitor localhost hme1 -g topsvc -y b
```

# rtm monitor <module_name>-v<virtual_link_name>

**Description** Start the monitoring process and specifies parameters for monitoring a Virtual Link.

**Usage** `rtm monitor <module_name>-v<virtual_link_name>[options]entity-1... entity-n`

**Syntax**

| Argument | Description |
|---|---|
| `module-name` | The name of the SmartView Monitor module. |
| `-virtual-link-name` | The name of the monitored Virtual Link. |
| `-d` | Specifies one of the following monitoring directions:<br>- a2b<br>- b2a<br>- a2b_b2a |
| `a2b` | Monitors End Point A to End Point B. |
| `b2a` | Monitors End Point B to End Point A. |
| `a2b_b2a` | Monitors both directions. |
| `-y` | Specifies one of the following measurement units. It is only required when the -w value is bandwidth.<br>- bytes<br>- pkts |
| `-w` | Specifies the displayed data type. |
| `bandwidth` | Displays the effective bandwidth. |
| `loss` | Displays the difference between the transmission rate and the receiving rate. |
| `rtt` | Displays the time required to make the round trip between the two End Points. |
| `-t` | Specifies the data type. It is only required when the -w value is bandwidth. |
| `wire` | Shows the data on the wire after compression or encryption. |

DRAFT

| Argument | Description |
|---|---|
| `application` | Shows the data as the application sees it (that is, not compressed and not encrypted). |

## rtm rtmd

**Description** Start the SmartView Monitor daemon manually. This also occurs manually when rtmstart is run.

**Usage** `rtm rtmd`

## rtm stat

**Description** Display the general SmartView Monitor status. In addition, it displays the status of the daemon, driver, opened views and active virtual links.

**Usage** `rtm stat [flavor(s)] [-h] [-v[v][v]]`

**Syntax**

| Argument | Description |
|---|---|
| `-h` | Help |
| `-v` | Verbose |
| `vl` | Current virtual links |
| `view` | Current views |

## rtm ver

**Description** Display the SmartView Monitor version.

**Usage** `rtm ver [-k]`

**Syntax**

| Argument | Description |
|---|---|
| `-k` | Displays the SmartView Monitor kernel version. |

## rtmstart

**Description** Load the SmartView Monitor kernel module and starts the SmartView Monitor daemon.

**Usage** `rtmstart`

## rtmstop

**Description** Kill the SmartView Monitor daemon and unloads the SmartView Monitor kernel module.

**Usage** `rtmstop`

DRAFT

# Chapter 13

# ClusterXL Commands

In This Chapter

DRAFT

## cphaconf

**Description** The cphaconf command configures ClusterXL.

⚠ **Important** - Running this command is not recommended. It should be run automatically, only by the Security Gateway or by Check Point support. The only exception to this rule is running this command with `set_cpp` option, as described below.

**Usage**

```
cphaconf [-i <machine id>] [-p <policy id>] [-b <db_id>] [-n
<cluster num>][-c <cluster size>] [-m <service >]
[-t <secured IF 1>...] start

cphaconf [-t <secured IF 1>...] [-d <disconnected IF 1>...] add
cphaconf clear-secured
cphaconf clear-disconnected
cphaconf stop
cphaconf init
cphaconf forward <on/off>
cphaconf debug <on/off>
cphaconf set_ccp <broadcast/multicast>
cphaconf mc_reload
cphaconf debug_data
```

**Syntax**

| Argument | Description |
|---|---|
| `cphaconf set_ccp <broadcast/multicast>` | Sets whether Cluster Control Protocol (CCP) packets should be sent with a broadcast or multicast destination MAC address. The default behavior is multicast. The setting created using this command will survive reboot.<br>Note, the same value (either broadcast or multicast) should be set on all cluster members. |

# cphaprob

**Description** The `cphaprob` command verifies that the cluster and the cluster members are working properly.

**Usage**

```
cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem> [-p] register
cphaprob -f <file> register
cphaprob -d <device> [-p] unregister
cphaprob -a unregister
cphaprob -d <device> -s <ok|init|problem> report
cphaprob [-i[a]] [-e] list
cphaprob state
cphaprob [-a] if
```

**Syntax**

| Argument | Description |
|---|---|
| cphaprob -d <device> -t <timeout(sec)> -s <ok\|init\|problem> [-p] register | Register <device> as a critical process, and add it to the list of devices that must be running for the cluster member to be considered active. |
| cphaprob -f <file> register | Register all the user defined critical devices listed in <file>. |
| cphaprob -d <device> [-p] unregister | Unregister a user defined <device> as a critical process. This means that this device is no longer considered critical. |
| cphaprob -a unregister | Unregister all the user defined <device>. |
| cphaprob -d <device> -s <ok\|init\|problem> report | Report the status of a user defined critical device to ClusterXL. |
| cphaprob [-i[a]] [-e] list | View the list of critical devices on a cluster member, and of all the other machines in the cluster. |
| cphaprob state | View the status of a cluster member, and of all the other members of the cluster.. |
| cphaprob [-a] if | View the state of the cluster member interfaces and the virtual cluster interfaces. |

DRAFT

# cphastart

**Description** Running `cphastart` on a cluster member activates ClusterXL on the member. It does not initiate full synchronization. `cpstart` is the recommended way to start a cluster member.

# cphastop

**Description** Running `cphastop` on a cluster member stops the cluster member from passing traffic. State synchronization also stops. It is still possible to open connections directly to the cluster member. In High Availability Legacy mode, running `cphastop` may cause the entire cluster to stop functioning.

# Index

DRAFT

DRAFT

DRAFT