Command Line Interface

Reference Guide
Version R70

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

703615 May 25, 2010
# Contents

**Preface**
- About his Guide............................................................................................... 12
- Who Should Use This Guide.............................................................................. 13
- Summary of Contents....................................................................................... 14
- Related Documentation.................................................................................... 15
- More Information............................................................................................. 17
- Feedback........................................................................................................ 18

**Chapter 1**

## Security Management Server and Firewall Commands

- `comp_init_policy` ............................................................................................ 21
- `cp_admin_convert` .......................................................................................... 22
- `c pca_client` ................................................................................................... 23
- `c pca_client create_cert` ................................................................................. 23
- `c pca_client revoke_cert` ............................................................................... 23
- `c pca_client lscert` ....................................................................................... 24
- `c pca_client set_mgmt_tools` .......................................................................... 24
- `cp_conf` ......................................................................................................... 26
- `cp_conf sic` .................................................................................................. 26
- `cp_conf admin` ............................................................................................. 26
- `cp_conf ca` .................................................................................................... 27
- `cp_conf finger` ............................................................................................. 27
- `cp_conf lic` .................................................................................................... 27
- `cp_conf client` ............................................................................................. 27
- `cp_conf ha` .................................................................................................... 28
- `cp_conf snmp` ............................................................................................... 28
- `cp_conf auto` ................................................................................................ 28
- `cp_conf sxl` .................................................................................................. 28
- `cpconfig` ......................................................................................................... 29
- `cpinfo` .............................................................................................................. 30
- `cpl ic` ............................................................................................................. 31
- `cpl ic check` .................................................................................................. 31
- `cpl ic db_add` ................................................................................................. 32
- `cpl ic db_print` ............................................................................................... 33
- `cpl ic db_rm` .................................................................................................. 34
- `cpl ic del` ....................................................................................................... 35
- `cpl ic del <object name>` .............................................................................. 35
- `cpl ic get` ...................................................................................................... 36
- `cpl ic put` ...................................................................................................... 37
- `cpl ic put <object name>` .............................................................................. 39
- `cpl ic print` .................................................................................................... 40
cplic upgrade ............................................................................................. 41

cp_merge ............................................................................................. 44
cp_merge delete_policy ............................................................................. 44

cp_merge export_policy ........................................................................... 45

cp_merge import_policy and cp_merge restore_policy .................................. 46

cp_merge list_policy ............................................................................... 47

cppkg ....................................................................................................... 48
cppkg add ............................................................................................. 48

cppkg delete .......................................................................................... 50
cppkg get .............................................................................................. 50

cppkg getroot .......................................................................................... 50
cppkg print ............................................................................................. 51

cppkg setroot .......................................................................................... 51

cpridrestart ............................................................................................ 53

cpridstart .............................................................................................. 54

cpridstop ............................................................................................... 55

cprinstall ............................................................................................... 56

cprinstall boot ......................................................................................... 56

cprinstall cpstart ..................................................................................... 57

cprinstall cpstop ...................................................................................... 57

cprinstall get .......................................................................................... 58


cprinstall install ...................................................................................... 58

cprinstall uninstall .................................................................................. 60

cprinstall verify ....................................................................................... 61

cprinstall snapshot .................................................................................. 62

cprinstall show ......................................................................................... 62

cprinstall revert ...................................................................................... 63

cprinstall transfer ................................................................................... 63

cpstart ..................................................................................................... 64

cpstat ....................................................................................................... 65

cpstat ....................................................................................................... 68

cpwd_admin ............................................................................................ 69

cpwd_admin start ..................................................................................... 69

cpwd_admin stop ...................................................................................... 70

cpwd_admin list ....................................................................................... 71

cpwd_admin exist ..................................................................................... 71

cpwd_admin kill ....................................................................................... 71

cpwd_admin config ............................................................................... 71

dedit ......................................................................................................... 74

dbver ....................................................................................................... 78

dbver create ............................................................................................ 78

dbver export ........................................................................................... 79

dbver import ............................................................................................ 79
Chapter 2

VPN Commands

VPN

- vpn accel ................................................................. 164
- vpn compreset ....................................................... 165
- vpn compstat .......................................................... 166
- vpn crl_zap .............................................................. 166
- vpn crlview .............................................................. 166
- vpn debug ............................................................... 167
- vpn drv ................................................................. 169
- vpn export_p12 ....................................................... 169
- vpn macutil ............................................................ 170
- vpn nssm_toplogy ..................................................... 170
- vpn overlap_encdom ............................................... 171
- vpn sw_toplogy ........................................................ 172
- vpn tu ................................................................. 173
- vpn ver ............................................................... 173

Chapter 3

SmartView Monitor Commands

RTM

- rtm debug ............................................................. 176
- rtm drv ............................................................... 176
- rtm monitor <module_name><interface_name> or rtm monitor <module_name>-filter ................................ 176
- rtm monitor <module_name>-v<virtual_link_name> ......................................................... 180
- rtm rtmd ................................................................ 181
- rtm stat ............................................................... 181
- rtm ver ................................................................ 181
- rtmstart ................................................................ 182
- rtmstop ................................................................ 182

Chapter 4

SecureClient Commands

SCC................................................................. 183
- scc connect ............................................................... 184
- scc connectnowait .................................................. 184
Preface

In This Chapter

About his Guide  page 12
Who Should Use This Guide  page 13
Summary of Contents  page 14
Related Documentation  page 15
More Information  page 17
Feedback  page 18
About his Guide

This guide documents the Command Line Interface (CLI) commands for Check Point Products and features. The commands are documented by product.

For each product, the commands are arranged alphabetically.
Who Should Use This Guide

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

This guide assumes a basic understanding of

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

This guide contains the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2, “VPN Commands”</td>
<td>The vpn command and its subcommands, used for controlling the VPN component of Check Point gateways.</td>
</tr>
<tr>
<td>Chapter 3, “SmartView Monitor Commands”</td>
<td>The rtm command its subcommands, used to execute SmartView Monitor operations.</td>
</tr>
<tr>
<td>Chapter 4, “SecureClient Commands”</td>
<td>The scc command and its subcommands are VPN commands that are executed on SecureClient. They are used to generate status information, stop and start services, or connect to defined sites using specific user profiles.</td>
</tr>
<tr>
<td>Chapter 5, “ClusterXL Commands”</td>
<td>Commands used for controlling, monitoring and troubleshooting ClusterXL gateway clusters.</td>
</tr>
<tr>
<td>Chapter 6, “Debugging SmartConsole Clients”</td>
<td>Commands for debugging SmartConsole clients.</td>
</tr>
<tr>
<td>Chapter 7, “CLI for Other Products”</td>
<td>References to other guides that document CLI commands for: CoreXL, SmartProvisioning and SmartLSM Security Gateways, Provider-1/SiteManager-1, and QoS</td>
</tr>
</tbody>
</table>
Related Documentation

This release includes the following documentation

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Security Installation and Upgrade Guide</td>
<td>Contains detailed installation instructions for Check Point network security products. Explains the available upgrade paths from versions R60-65 to the current version.</td>
</tr>
<tr>
<td>High-End Installation and Upgrade Guide</td>
<td>Contains detailed installation instructions for the Provider-1 and VSX products, including hardware and software requirements and licensing requirements. Explains all upgrade paths for Check Point products specifically geared towards upgrading to the current version.</td>
</tr>
<tr>
<td>Firewall Administration Guide</td>
<td>Describes how to control and secure network access and VoIP traffic; how to use integrated web security capabilities; and how to optimize Application Intelligence with capabilities such as Content Vectoring Protocol (CVP) applications, URL Filtering (UFP) applications.</td>
</tr>
<tr>
<td>IPS Administration Guide</td>
<td>Describes how to use IPS to protect against attacks.</td>
</tr>
<tr>
<td>Virtual Private Networks Administration Guide</td>
<td>Describes the basic components of a VPN and provides the background for the technology that comprises the VPN infrastructure.</td>
</tr>
<tr>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Eventia Reporter Administration Guide</td>
<td>Explains how to monitor and audit traffic, and generate detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for all events logged by Check Point Security Gateways, SecureClient and IPS.</td>
</tr>
<tr>
<td>SecurePlatform/SecurePlatform Pro Administration Guide</td>
<td>Explains how to install and configure SecurePlatform. This guide will also teach you how to manage your SecurePlatform machine and explains Dynamic Routing (Unicast and Multicast) protocols.</td>
</tr>
<tr>
<td>Provider-1/SiteManager-1 Administration Guide</td>
<td>Explains the Provider-1 security management solution. This guide provides details about a three-tier, multi-policy management architecture and a host of Network Operating Center oriented features that automate time-consuming repetitive tasks common in Network Operating Center environments.</td>
</tr>
</tbody>
</table>
More Information

- For additional technical information about Check Point products, consult Check Point’s SecureKnowledge at http://support.checkpoint.com.
- To view the latest version of this document in the Check Point User Center, go to: http://support.checkpoint.com.
Feedback

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

cp_techpub_feedback@checkpoint.com
Chapter 1
Security Management Server and Firewall Commands

In This Chapter

comp_init_policy  page 21
cp_admin_convert  page 22
cpca_client  page 23
cp_conf  page 26
cpconfig  page 29
cpinfo  page 30
cplic  page 31
cp_merge  page 44
cppkg  page 48
cpridrestart  page 53
cpridstart  page 54
cpridstop  page 55
cprinstall  page 56
cpstart  page 64
cpstat  page 65
cpstop  page 68
cpwdb_admin  page 69
dbedit  page 74
dbver page 78
dynamic_objects page 81
fw page 82
fwm page 126
GeneratorApp page 138
inet_alert page 139
ldapcmd page 142
ldapcompare page 143
ldapconvert page 144
ldapmodify page 148
ldapsearch page 150
log_export page 152
queryDB_util page 156
rs_db_tool page 158
sam_alert page 159
svr_webupload_config page 161
**comp_init_policy**

**Description**

Use the `comp_init_policy` command to generate and load, or to remove, the Initial Policy.

The Initial Policy offers protection to the gateway before the administrator has installed a Policy on the gateway.

**Usage**

```
$FWDIR/bin/comp_init_policy [-u | -g]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u</td>
<td>Removes the current Initial Policy, and ensures that it will not be generated in future when cpconfig is run.</td>
</tr>
<tr>
<td>-g</td>
<td>Can be used if there is no Initial Policy. If there is, make sure that after removing the policy, you delete the <code>$FWDIR\state\local\FW1\</code> folder. Generates the Initial Policy and ensures that it will be loaded the next time a policy is fetched (at cpstart, or at next boot, or via the <code>fw fetch localhost</code> command). After running this command, cpconfig will add an Initial Policy when needed. The <code>comp_init_policy -g</code> command will only work if there is no previous Policy. If you perform the following commands: <code>comp_init_policy -g + fw fetch localhost</code> <code>comp_init_policy -g + cpstart</code> <code>comp_init_policy -g + reboot</code> The original policy will still be loaded.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Automatically export administrator definitions that were created in cpconfig to SmartDashboard.</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td>cp_admin_convert</td>
</tr>
</tbody>
</table>
**cpca_client**

**Description**
This command and all its derivatives are used to execute operations on the ICA.

**Usage**
cpca_client

**In This Section**
- cpca_client create_cert  
- cpca_client revoke_cert  
- cpca_client lscert  
- cpca_client set_mgmt_tools

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port used to connect to the CA (if the CA was not run from the default port 18209)</td>
</tr>
<tr>
<td>-n &quot;CN=&lt;common name&gt;&quot;</td>
<td>Sets the CN</td>
</tr>
<tr>
<td>-f &lt;PKCS12 filename&gt;</td>
<td>Specifies the file name where the certificate and keys are saved.</td>
</tr>
</tbody>
</table>

**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

---

**Description**
Show all certificates issued by the ICA.

**Usage**

```
```

**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
- `-ser number` Filters results for this serial number
- `-dp number` Filters results from this CDP

---

**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" ... ]
```

---

24
Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>set_mgmt_tools on</td>
<td>off</td>
</tr>
<tr>
<td>-p &lt;ca_port&gt;</td>
<td>Specifies the port which is used to connect to the CA (if the appropriate service was not run from the default port 18265)</td>
</tr>
<tr>
<td>-no_ssl</td>
<td>Configures the server to use clear http rather than https</td>
</tr>
<tr>
<td>-al-u&quot;administratoruser DN&quot;</td>
<td>Sets the DNs of the administrators or user permitted to use the ICA Management tool</td>
</tr>
</tbody>
</table>

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.
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
```

In This Section

- `cp_conf sic`  page 26
- `cp_conf admin`  page 26
- `cp_conf ca`  page 27
- `cp_conf finger`  page 27
- `cp_conf lic`  page 27
- `cp_conf client`  page 27
- `cp_conf ha`  page 28
- `cp_conf snmp`  page 28
- `cp_conf auto`  page 28
- `cp_conf sxl`  page 28

**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
```
**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.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>cp_conf ha</td>
<td>Enable or disable High Availability.</td>
<td>cp_conf ha enable/disable [norestart] # Enable/Disable HA</td>
</tr>
<tr>
<td>cp_conf snmp</td>
<td>Activate or deactivate SNMP.</td>
<td>cp_conf snmp get # Get SNMP Extension status. cp_conf snmp activate/deactivate [norestart] # Deactivate SNMP Extension.</td>
</tr>
<tr>
<td>cp_conf auto</td>
<td>Determine whether or not the Security Gateway/Security Management server starts automatically after the machine restarts.</td>
<td>cp_conf auto get [fw1] [fg1] [rm] [all] # Get the auto state of products. cp_conf auto &lt;enable</td>
</tr>
<tr>
<td>cp_conf sxl</td>
<td>Enable or disable SecureXL acceleration.</td>
<td>cp_conf sxl &lt;enable</td>
</tr>
</tbody>
</table>
**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 Check Point Internet Security Products Installation and Upgrade Guide.
http://supportcontent.checkpoint.com/documentation_download?ID=8753
Description
CPinfo is a utility that collects data on a customer's machine at the time of execution. The CPinfo output file enables Check Point's support engineers to analyze customer setups from a remote location. Engineers can open the CPinfo file in demo mode, while viewing actual customer Security Policies and objects. This allows for in-depth analysis of all of customer configuration options and environment settings.

Usage
```bash
cpinfo [-v] [-l] [-n] [-o] [-r] [-t [tablename]] [-c cma ...]
```

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-z</td>
<td>Output gzipped (effective with -o option)</td>
</tr>
<tr>
<td>-r</td>
<td>Includes the registry (Windows - very large output)</td>
</tr>
<tr>
<td>-v</td>
<td>Prints version information</td>
</tr>
<tr>
<td>-l</td>
<td>Embeds log records (very large output)</td>
</tr>
<tr>
<td>-n</td>
<td>Does not resolve network addresses (faster)</td>
</tr>
<tr>
<td>-t</td>
<td>Output consists of tables only (SR only)</td>
</tr>
<tr>
<td>-c</td>
<td>Get information about the specified CMA (Provider-1)</td>
</tr>
<tr>
<td>-x</td>
<td>Get information about the specified VS (VSX)</td>
</tr>
</tbody>
</table>

Further Info.
SecureKnowledge solution sk30567

http://supportcontent.checkpoint.com/solutions?id=sk30567
**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**  

```
Usage: cplic
```

**In This Section**

- `cplic check`  page 31
- `cplic db_add`  page 32
- `cplic db_print`  page 33
- `cplic db_rm`  page 34
- `cplic del`  page 35
- `cplic del <object name>`  page 35
- `cplic get`  page 36
- `cplic put`  page 37
- `cplic put <object name> ...`  page 39
- `cplic print`  page 40
- `cplic upgrade`  page 41

---

### cplic check

**Description**  Check whether the license on the local machine will allow a given feature to be used.

**Usage**  

```
```
cplic db_add

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;product name&gt;</td>
<td>Product for which license information is requested. For example fw1, nets0</td>
</tr>
<tr>
<td>-v &lt;product version&gt;</td>
<td>Product version for which license information is requested</td>
</tr>
<tr>
<td>-c count</td>
<td>Output the number of licenses connected to this feature</td>
</tr>
<tr>
<td>-t &lt;date&gt;</td>
<td>Check license status on future date. Use the format ddmmyyyy. A feature may be valid on a given date on one license, but invalid in another</td>
</tr>
<tr>
<td>-r routers</td>
<td>Check how many routers are allowed. The feature option is not needed</td>
</tr>
<tr>
<td>-S SRusers</td>
<td>Check how many SecuRemote users are allowed. The feature option is not needed</td>
</tr>
<tr>
<td>&lt;feature&gt;</td>
<td>&lt;feature&gt; for which license information is requested</td>
</tr>
</tbody>
</table>

Usage

cplic db_add < -l license-file | host expiration-date signature SKU/features >

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.
Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l license-file</td>
<td>Adds the license(s) from license-file. The following options are NOT needed:</td>
</tr>
<tr>
<td></td>
<td>Host Expiration-Date Signature SKU/feature</td>
</tr>
</tbody>
</table>

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-CB6Crtjhv-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:

<table>
<thead>
<tr>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding license to database ...</td>
</tr>
<tr>
<td>Operation Done</td>
</tr>
</tbody>
</table>

**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]
```
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>The signature string within the license.</td>
</tr>
</tbody>
</table>

**Example**

```
cplic db_rm 2f540abb-d3bcb001-7e54513e-kfyigpw
```

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-F &lt;output file&gt;</td>
<td>Send the output to &lt;output file&gt; instead of the screen.</td>
</tr>
<tr>
<td>&lt;signature&gt;</td>
<td>The signature string within the license.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object name</td>
<td>The name of the Check Point Security Gateway object, as defined in SmartDashboard.</td>
</tr>
</tbody>
</table>
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**

```bash
cplic get <ipaddr | hostname | -all> [-v41]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr</td>
<td>The IP address of the Check Point Security Gateway from which licenses are to be retrieved.</td>
</tr>
</tbody>
</table>
### 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>

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The name of the Check Point Security Gateway object (as defined in SmartDashboard) from which licenses are to be retrieved.</td>
</tr>
<tr>
<td>-all</td>
<td>Retrieve licenses from all Check Point gateways in the managed network.</td>
</tr>
<tr>
<td>-v41</td>
<td>Retrieve version 4.1 licenses from the NF Check Point gateway. Used to upgrade version 4.1 licenses.</td>
</tr>
</tbody>
</table>

**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.
### Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-overwrite (or -o)</td>
<td>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.</td>
</tr>
<tr>
<td>-check-only (or -c)</td>
<td>Verify the license. Checks if the IP of the license matches the machine, and if the signature is valid</td>
</tr>
<tr>
<td>select (or -s)</td>
<td>Select only the Local licenses whose IP address matches the IP address of the machine.</td>
</tr>
<tr>
<td>-F outputfile</td>
<td>Outputs the result of the command to the designated file rather than to the screen.</td>
</tr>
<tr>
<td>-Preboot (or -P)</td>
<td>Use this option after upgrading and before rebooting the machine. Use of this option will prevent certain error messages.</td>
</tr>
<tr>
<td>-kernel-only (or -k)</td>
<td>Push the current valid licenses to the kernel. For Support use only.</td>
</tr>
<tr>
<td>-l license-file</td>
<td>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</td>
</tr>
</tbody>
</table>

### 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.
  - **Solaris** - 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-zipoVNSnm-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:
```

<table>
<thead>
<tr>
<th>Host</th>
<th>Expiration</th>
<th>SKU</th>
</tr>
</thead>
<tbody>
<tr>
<td>215.153.142.130</td>
<td>26Dec2001</td>
<td>CPMP-EVAL-1-3DES-NG CK0123456789ab</td>
</tr>
</tbody>
</table>

**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 >
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>The name of the Check Point Security Gateway object, as defined in SmartDashboard.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-noheader (or -n)</td>
<td>Print licenses with no header.</td>
</tr>
<tr>
<td>-x</td>
<td>Print licenses with their signature</td>
</tr>
<tr>
<td>-type (or -t)</td>
<td>Prints licenses showing their type: Central or Local.</td>
</tr>
<tr>
<td>-F &lt;outputfile&gt;</td>
<td>Divert the output to outputfile.</td>
</tr>
<tr>
<td>-preatures (or -p)</td>
<td>Print licenses resolved to primitive features.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l inputfile</td>
<td>Upgrades the licenses in the license repository and Check Point gateways to match the licenses in &lt;inputfile&gt;</td>
</tr>
</tbody>
</table>

**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:

```bash
count:root(su) [-] # cplic get -all
golda:
Retrieved 1 licenses.
Detached 0 licenses.
Removed 0 licenses.
```

• To see all the licenses in the repository, run the command:

```bash
cplic db_print -all -a
```

```bash
count:root(su) [-] # cplic db_print -all -a
Retrieving license information from database ...
The following licenses appear in the database:
```

<table>
<thead>
<tr>
<th>Host</th>
<th>Expiration</th>
<th>Features</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.8.11</td>
<td>Never</td>
<td>CPFW-FIG-25-41</td>
<td>CK-49C3A3CC7</td>
</tr>
<tr>
<td>121 golda</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.5.11</td>
<td>26Nov2002</td>
<td>CPSUITE-EVAL-3DES-NG</td>
<td>CK-123456789</td>
</tr>
</tbody>
</table>

• In the User Center (http://www.checkpoint.com/usercenter), 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 in step 1, 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 *Security Management Server Administration Guide*.
**cp_merge**

**Description**

The cp_merge utility has two main functionalities:

- Export and import of policy packages
- Merge of objects from a given file into the Security Management server database

**Usage**

```
cp_merge help
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Displays the usage for cp_merge.</td>
</tr>
</tbody>
</table>

**In This Section**

- `cp_merge delete_policy`  page 44
- `cp_merge export_policy`  page 45
- `cp_merge import_policy and cp_merge restore_policy`  page 46
- `cp_merge list_policy`  page 47

**cp_merge delete_policy**

**Description**

Provides the options of deleting an existing policy package. Note that the default policy can be deleted by delete action.

**Usage**

```
cp_merge delete_policy [-s <db server>] [-u <user> | -c <certificate file>] [-p <password>] -n <package name>
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s &lt;db server&gt;</td>
<td>Specify the database server IP Address or DNS name.</td>
</tr>
<tr>
<td>-u &lt;user&gt;</td>
<td>The administrator’s name.</td>
</tr>
<tr>
<td>-c &lt;certificate file&gt;</td>
<td>The path to the certificate file.</td>
</tr>
<tr>
<td>-p &lt;password&gt;</td>
<td>The administrator’s password.</td>
</tr>
<tr>
<td>-n &lt;package name&gt;</td>
<td>The policy package to export.</td>
</tr>
</tbody>
</table>

**Comments**

Further considerations:

1. Either use certificate file or user and password
2. Optional

Example
Delete the policy package called standard.
```
cp_merge delete_policy -n Standard
```

**cp_merge export_policy**

**Description**
Provides the options of leaving the policy package in the active repository, or deleting it as part of the export process. The default policy cannot be deleted during the export action.

**Usage**
```
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s &lt;db server&gt;</td>
<td>Specify the database server IP Address or DNS name.</td>
</tr>
<tr>
<td>-u &lt;user&gt;</td>
<td>The database administrator's name.</td>
</tr>
<tr>
<td>-c &lt;certificate file&gt;</td>
<td>The path to the certificate file.</td>
</tr>
<tr>
<td>-p &lt;password&gt;</td>
<td>The administrator's password.</td>
</tr>
<tr>
<td>-n &lt;policy package name&gt;</td>
<td>The policy package to export.</td>
</tr>
<tr>
<td>-l &lt;policy name&gt;</td>
<td>Export the policy package which encloses the policy name.</td>
</tr>
<tr>
<td>-d &lt;output directory&gt;</td>
<td>Specify the output directory.</td>
</tr>
<tr>
<td>-f &lt;outputfile&gt;</td>
<td>Specify the output file name (where the default file name is &lt;policy name&gt;.pol).</td>
</tr>
<tr>
<td>-r</td>
<td>Remove the original policy from the repository.</td>
</tr>
</tbody>
</table>

**Comments**

Further considerations:

1. Either use certificate file or user and password
2. Optional
3. If both -n and -l are omitted all policy packages are exported.
4. If both -n and -l are present -l is ignored.
Example

Export policy package Standard to file

```bash
```

**cp_merge import_policy and cp_merge restore_policy**

**Description**
Provides the options to overwrite an existing policy package with the same name, or preventing overwriting when the same policy name already exists

**Usage**

```bash
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s &lt;db server&gt;</td>
<td>Specify the database server IP address or DNS name.</td>
</tr>
<tr>
<td>-u &lt;user&gt;</td>
<td>The administrator's name.</td>
</tr>
<tr>
<td>-c &lt;certificate file&gt;</td>
<td>The path to the certificate file.</td>
</tr>
<tr>
<td>-p &lt;password&gt;</td>
<td>The administrator's password.</td>
</tr>
<tr>
<td>-n &lt;policy package name&gt;</td>
<td>Rename the policy package to &lt;policy package name&gt; when importing.</td>
</tr>
<tr>
<td>-d &lt;input directory&gt;</td>
<td>Specify the input directory.</td>
</tr>
<tr>
<td>-f &lt;inputfile&gt;</td>
<td>Specify the input file name.</td>
</tr>
<tr>
<td>-v</td>
<td>Override an existing policy if found.</td>
</tr>
</tbody>
</table>

**Comments**

Further considerations

1. Either use certificate file or user and password
2. Optional

The `cp_merge restore_policy` works only locally on the Security Management server and it will not work from remote machines.

**Caution:** A Security policy from `<policy>.W` file can be restored using this utility; however, important information may be lost when the policy is translated into `.W` format. This restoration should be used only if there is no other backup of the policy.
Example  
Import the policy package saved in file Standard.pol into the repository and rename it to StandardCopy.
```
cp_merge import_policy -f Standard.pol -n StandardCopy
```  

**cp_merge list_policy**

**Usage**  
```
cp_merge list_policy [-s <db server>] [-u <user> | -c <certificate file>] [-p <password>]
```  

**Syntax**  
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s &lt;db server&gt;</td>
<td>Specify the database server IP Address or DNS name.²</td>
</tr>
<tr>
<td>-u &lt;user&gt;</td>
<td>The administrator’s name.¹²</td>
</tr>
<tr>
<td>-c &lt;certificate file&gt;</td>
<td>The path to the certificate file.¹²</td>
</tr>
<tr>
<td>-p &lt;password&gt;</td>
<td>The administrator’s password.¹²</td>
</tr>
</tbody>
</table>

**Comments**  
Further considerations:
1. Either use certificate file or user and password
2. Optional

**Example**  
List all policy packages which reside in the specified repository:
```
cp_merge list -s localhost
```
cppkg

cppkg

Description  Manage the product repository. It is always executed on the Security Management server.

In This Section

cppkg add  page 48
cppkg delete  page 50
cppkg get  page 50
cppkg getroot  page 50
cppkg print  page 51
cppkg setroot  page 51

cppkg add

Description  Add a product package to the product repository. Only SmartUpdate packages can be added to the product repository.

Products can be added to the Repository as described in the following procedures, by importing a file downloaded from the Download Center web site at http://www.checkpoint.com/techsupport/downloads/downloads.html. The package file can be added to the Repository directly from the CD or from a local or network drive.

Usage  cppkg add <package-full-path | CD drive>
cppkg add does not overwrite existing packages. To overwrite existing packages, you must first delete existing packages.

### Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>package-full-path</td>
<td>If the package to be added to the repository is on a local disk or network drive, type the full path to the package.</td>
</tr>
</tbody>
</table>
| CD drive                  | If the package to be added to the repository is on a CD: For Windows machines type the CD drive letter, e.g. d:
For UNIX machines, type the CD root path, e.g. /caruso/image/CPsuite-R70 You will be asked to specify the product and appropriate Operating System (OS). |

### Comments

cppkg add does not overwrite existing packages. To overwrite existing packages, you must first delete existing packages.

### Example

```
[d:\winnt\fw1\ng\bin]cppkg add l:\CPsuite-R70\ 
Enter package name: 
----------------------
(1) SVNfoundation
(2) firewall
(3) floodgate
(4) rtm
(e) Exit
Enter you choice : 1
Enter package OS :
----------------------
(1) win32
(2) solaris
(3) linux
(4) ipso
(e) Exit
Enter your choice : 1
You choose to add ‘SVNfoundation’ for ‘win32’ OS. Is this correct? [y/n] : y
Adding package from CD ...
Package added to repository.
```
cppkg delete

**Description**  
Delete a product package from the repository. To delete a product package you must specify a number of options. To see the format of the options and to view the contents of the product repository, use the `cppkg print` command.

**Usage**  
`cppkg delete [<vendor> <product> <version> <os> [sp]]`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vendor</td>
<td>Package vendor (e.g. checkpoint).</td>
</tr>
<tr>
<td>product</td>
<td>Package name.</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>os</td>
<td>Package Operating System. Options are: win32, solaris, ipso, linux.</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version. This parameter is optional.</td>
</tr>
</tbody>
</table>

**Comments**  
It is not possible to undo the cppkg del command.

cppkg get

**Description**  
Synchronizes the Package Repository database with the content of the actual package repository under "$SUROOT".

**Usage**  
`cppkg get`

cppkg getroot

**Description**  
Find out the location of the product repository. The default product repository location on Windows machines is C:\SUroot. On UNIX it is /var/SUroot

**Usage**  
`cppkg getroot`

**Example**  
```
# cppkg getroot
Current repository root is set to : /var/suroot/
```
cppkg print

Description List the contents of the product repository.
Use cppkg print to see the product and OS strings required to install
a product package using the cprinstall command, or to delete a
package using the cppkg delete command.

Usage cppkg print

cppkg setroot

Description Create a new repository root directory location, and to move existing
product packages into the new repository.

The default product repository location is created when the Security
Management server is installed. On Windows machines the default
location is C:\SUroot and on UNIX it is /var/SUroot. Use this
command to change the default location.

When changing repository root directory:
• The contents of the old repository is copied into the new
repository.
• The $SUROOT environment variable gets the value of the new root
path.
• A product package in the new location will be overwritten by a
package in the old location, if the packages are the same (that is,
they have the same ID strings).

The repository root directory should have at least 200 Mbyte of free
disk space.

Usage cppkg setroot <repository-root-directory-full-path>

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>repository-root-directory-full-path</td>
<td>The desired location for the product repository.</td>
</tr>
</tbody>
</table>

Comments It is important to reboot the Security Management server after
performing this command, in order to set the new $SUROOT
environment variable.
cppkg setroot /var/new_suroot Repository root is set to: /var/new_suroot/

Note: When changing repository root directory:

1. Old repository content will be copied into the new repository.

2. A package in the new location will be overwritten by a package in the old location, if the packages have the same name.

Change the current repository root? [y/n]: y

The new repository directory does not exist. Create it? [y/n]: y

Repository root was set to: /var/new_suroot

Notice: To complete the setting of your directory, reboot the machine!
cpridrestart

**Description**

Stops and starts the Check Point Remote Installation Daemon (cprid). This is the daemon that is used for remote upgrade and installation of products. In Windows it is a service.
cpridstart

**cpridstart**

**Description**  
Start the Check Point Remote Installation Daemon (cprid). This is the service that allows for the remote upgrade and installation of products. In Windows it is a service.

**Usage**  
cpridstart
cpridstop

**Description**
Stop the Check Point Remote installation Daemon (cprid). This is the service that allows for the remote upgrade and installation of products. In Windows it is a service.

**Usage**
cpridstop
cprinstall

Description
Use cprinstall commands to perform remote installation of product packages, and associated operations.

On the Security Management server, cprinstall commands require licenses for SmartUpdate.

On the remote Check Point gateways the following are required:
• Trust must be established between the Security Management server and the Check Point gateway.
• cpd must run.
• cprid remote installation daemon must run.

In This Section

- cprinstall boot page 56
- cprinstall cpstart page 57
- cprinstall cpstop page 57
- cprinstall get page 58
- cprinstall install page 58
- cprinstall uninstall page 58
- cprinstall verify page 60
- cprinstall snapshot page 61
- cprinstall show page 62
- cprinstall revert page 63
- cprinstall transfer page 63

**cprinstall boot**

Description
Boot the remote computer.

Usage
```
cprinstall boot <Object name>
```

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
</tbody>
</table>
### cprinstall cpstart

**Description**
Enable `cpstart` to be run remotely.
All products on the Check Point Security Gateway must be of the same version.

**Usage**
cprinstall cpstart <object name>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
</tbody>
</table>

### cprinstall cpstop

**Description**
Enables `cpstop` to be run remotely.
All products on the Check Point Security Gateway must be of the same version.

**Usage**
cprinstall cpstop <-proc | -nopolicy> <object name>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
<tr>
<td>-proc</td>
<td>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.</td>
</tr>
<tr>
<td>-nopolicy</td>
<td></td>
</tr>
</tbody>
</table>
**cprinstall get**

**Description**
Obtain details of the products and the Operating System installed on the specified Check Point gateway, and to update the database.

**Usage**
cprinstall get <Object name>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>The name of the Check Point Security Gateway object defined in SmartDashboard.</td>
</tr>
</tbody>
</table>

**Example**
cprinstall get gw1
Checking cpnid connection...  
Verified  
Operation completed successfully  
Updating machine information...  
Update successfully completed  
'Get Gateway Data' completed successfully  
Operating system          Major Version | Minor Version
-------------------------------|----------------|
SecurePlatform               R70                  R70
Vendor | Product | Major Version | Minor Version
-----------------------------------|----------------|
Check Point | VPN-1 Power/UTM | R70 | R70 |
Check Point | SecurePlatform | R70 | R70 |
Check Point | SmartPortal | R70 | R70 |

**cprinstall install**

**Description**
Install Check Point products on remote Check Point gateways. To install a product package you must specify a number of options. Use the cppkg print command and copy the required options.

**Usage**
cprinstall install [-boot] <Object name> <vendor> <product> <version> [sp]
Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-boot</td>
<td>Boot the remote computer after installing the package. Only boot after ALL products have the same version. Boot will be cancelled in certain scenarios. See the Release Notes for details.</td>
</tr>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor (e.g. checkpoint)</td>
</tr>
<tr>
<td>product</td>
<td>Package name</td>
</tr>
<tr>
<td>version</td>
<td>Package version</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version</td>
</tr>
</tbody>
</table>

Comments

Before transferring any files, this command runs the cprinstall verify command to verify that the Operating System is appropriate and that the product is compatible with previously installed products.

Example

```
# cprinstall install -boot fred checkpoint firewall R70

Installing firewall R70 on fred...
Info : Testing Check Point Gateway
Info : Test completed successfully.
Info : Transferring Package to Check Point Gateway
Info : Extracting package on Check Point Gateway
Info : Installing package on Check Point Gateway
Info : Product was successfully applied.
Info : Rebooting the Check Point Gateway
Info : Checking boot status
Info : Reboot completed successfully.
Info : Checking Check Point Gateway
Info : Operation completed successfully.
```
cprinstall uninstall

**Description**  Uninstall products on remote Check Point gateways. To uninstall a product package you must specify a number of options. Use the cppkg print command and copy the required options.

**Usage**  
cprinstall uninstall [-boot] <Object name> <vendor> <product> <version> [sp]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-boot</td>
<td>Boot the remote computer after installing the package. Only boot after ALL products have the same version. Boot will be cancelled in certain scenarios. See the Release Notes for details.</td>
</tr>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor (e.g. checkpoint)</td>
</tr>
<tr>
<td>product</td>
<td>Package name</td>
</tr>
<tr>
<td>version</td>
<td>Package version</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version.</td>
</tr>
</tbody>
</table>

**Comments**  
*Before* uninstalling any files, this command runs the cprinstall verify command to verify that the Operating System is appropriate and that the product is installed.

*After* uninstalling, retrieve the Check Point Security Gateway data by running cprinstall get.

**Example**

```bash
# cprinstall uninstall fred checkpoint firewall R70

Uninstalling firewall R70 from fred...
Info : Removing package from Check Point Gateway
Info : Product was successfully applied.
Operation Success. Please get network object data to complete the operation.
```
cprinstall verify

**Description**
Verify:
- If a specific product can be installed on the remote Check Point gateway.
- That the Operating System and currently installed products are appropriate for the package.
- That there is enough disk space to install the product.
- That there is a CPRID connection.

**Usage**
cprinstall verify <Object name> <vendor> <product> <version> [sp]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor (e.g. checkpoint).</td>
</tr>
<tr>
<td>product</td>
<td>Package name Options are: SVNfoundation, firewall, floodgate.</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version. This parameter is optional.</td>
</tr>
</tbody>
</table>

**Example**
The following examples show a successful and a failed verify operation:

**Verify succeeds:**
cprinstall verify harlin checkpoint SVNfoundation R70

Verifying installation of SVNfoundation R70 on harlin...
Info : Testing Check Point Gateway.
Info : Test completed successfully.
Info : Installation Verified, The product can be installed.
cprinstall snapshot

Verify fails:

cprinstall verify harlin checkpoint SVNfoundation R70

Verifying installation of SVNfoundation R70 on harlin...
Info: Testing Check Point Gateway
Info: SVN Foundation R70 is already installed on 192.168.5.134
Operation Success. Product cannot be installed, did not pass dependency check.

**cprinstall snapshot**

**Description**: Creates a snapshot `<filename>` on the Check Point Security Gateway.

**Usage**

cprinstall snapshot <object name> <filename>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
<tr>
<td>filename</td>
<td>Name of the snapshot file.</td>
</tr>
</tbody>
</table>

**Comments**

Supported on SecurePlatform only.

**cprinstall show**

**Description**: Displays all snapshot (backup) files on the Check Point Security Gateway.

**Usage**

cprinstall show <object name>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
</tbody>
</table>

**Comments**

Supported on SecurePlatform only.

**Example**

# cprinstall show GW1
SU_backup.tgz
cprinstall revert

Description
Restores the Check Point Security Gateway from a snapshot.

Usage
cprinstall revert <object name> <filename>

Syntax
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
<tr>
<td>filename</td>
<td>Name of the snapshot file.</td>
</tr>
</tbody>
</table>

Comments
Supported on SecurePlatform only.

cprinstall transfer

Description
Transfers a package from the repository to a Check Point Security Gateway without installing the package.

Usage
cprinstall transfer <object name> <vendor> <product> <version> <sp>

Syntax
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object name</td>
<td>Object name of the Check Point Security Gateway defined in SmartDashboard.</td>
</tr>
<tr>
<td>vendor</td>
<td>Package vendor (e.g. checkpoint).</td>
</tr>
<tr>
<td>product</td>
<td>Package name</td>
</tr>
<tr>
<td>version</td>
<td>Package version.</td>
</tr>
<tr>
<td>sp</td>
<td>Package minor version. This parameter is optional.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Start all Check Point processes and applications running on a machine.</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td><code>cpstart</code></td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>This command cannot be used to start <code>cprid</code>. <code>cprid</code> is invoked when the machine is booted and it runs independently.</td>
</tr>
</tbody>
</table>
**cpstat**

display 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h host</td>
<td>A resolvable hostname, a dot-notation address (for example:192.168.33.23), or a DAIP object name. The default is localhost.</td>
</tr>
<tr>
<td>-p port</td>
<td>Port number of the AMON server. The default is the standard AMON port (18192)</td>
</tr>
<tr>
<td>-s</td>
<td>Secure Internal Communication (SIC) name of the AMON server.</td>
</tr>
<tr>
<td>-f flavor</td>
<td>The flavor of the output (as it appears in the configuration file). The default is the first flavor found in the configuration file.</td>
</tr>
<tr>
<td>-o</td>
<td>Polling interval (seconds) specifies the pace of the results. The default is 0, meaning the results are shown only once.</td>
</tr>
<tr>
<td>-c</td>
<td>Specifies how many times the results are shown. The default is 0, meaning the results are repeatedly shown.</td>
</tr>
</tbody>
</table>
The following flavors can be added to the application flags:

- vpn — "default", "product", "IKE", "ipsec", "traffic", "compression", "accelerator", "nic", "statistics", "watermarks", "all"
- fg — "all"
- ha — "default", "all"

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-e</td>
<td>Specifies the interval (seconds) over which ‘statistical’ olds are computed. Ignored for regular olds.</td>
</tr>
<tr>
<td>-d</td>
<td>Debug mode.</td>
</tr>
</tbody>
</table>
| application_flag | One of the following:  
  - fw — Firewall component of the Security Gateway  
  - vpn — VPN component of the Security Gateway  
  - fg — QoS (formerly FloodGate-1)  
  - ha — ClusterXL (High Availability)  
  - os — OS Status  
  - mg — for the Security Management server  
  - persistency - for historical status values  
  - polsrv  
  - uas  
  - svr  
  - cpsemd  
  - cpsead  
  - asm  
  - ls  
  - ca |
• 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

```bash
> 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**|
```
**cpstop**

**Description**
Terminate all Check Point processes and applications, running on a machine.

**Usage**
cpstop

cpstop -fwflag [-proc | -default]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-fwflag -proc</td>
<td>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.</td>
</tr>
<tr>
<td>-fwflag -default</td>
<td>Kills Check Point daemons and Security servers. The active Security Policy running in the kernel is replaced with the default filter.</td>
</tr>
</tbody>
</table>

**Comments**
This command cannot be used to terminate cprid. cprid is invoked when the machine is booted and it runs independently.
**cpwd_admin**

**Description**

`cpwd` (also known as WatchDog) is a process that invokes and monitors critical processes such as Check Point daemons on the local machine, and attempts to restart them if they fail. Among the processes monitored by Watchdog are `cpd`, `fwd`, `fwm`.

`fwd` does not work in a Security Management Only machine. To work with `fwd` in a Security Management Only machine add `-n` (for example, `fwd -n`).

`cpwd` writes monitoring information to the `$CPDIR/log/cpwd.elg` log file. In addition, monitoring information is written to the console on UNIX platforms, and to the Windows Event Viewer.

The `cpwd_admin` utility is used to show the status of processes, and to configure `cpwd`.

**Usage**

```
cpwd_admin
```

In This Section

- `cpwd_admin start`  
- `cpwd_admin stop`  
- `cpwd_admin list`  
- `cpwd_admin exist`  
- `cpwd_admin kill`  
- `cpwd_admin config`  

**cpwd_admin start**

**Description**

Start a new process by `cpwd`.

**Usage**

```
cpwd_admin start -name <process name> -path "<full path>" -command "<executable name>"
```
cpwd_admin stop

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-name &lt;process name&gt;</td>
<td>A name for the process to be watched by WatchDog.</td>
</tr>
<tr>
<td>-path &quot;full path&quot;</td>
<td>The full path to the executable including the executable name</td>
</tr>
<tr>
<td>-command &quot;executable name &amp; arguments&quot;</td>
<td>The name of the executable file.</td>
</tr>
</tbody>
</table>

Example

To start and monitor the fwm process.

```
cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"
```
**cpwd_admin list**

**Description**
Print a status of the selected processes being monitored by cpwd.

**Usage**
cpwd_admin list

**Output**
The status report output includes the following information:
- **APP** — Application. The name of the process.
- **PID** — Process Identification Number.
- **STAT** — Whether the process Exists (E) or has been Terminated (T).
- **#START** — How many times the process has been started since cpwd took control of the process.
- **START TIME** — The last time the process was run.
- **COMMAND** — The command that cpwd used to start the process.

For example:

<table>
<thead>
<tr>
<th>APP</th>
<th>PID</th>
<th>STAT</th>
<th>#START</th>
<th>START TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPD</td>
<td>463</td>
<td>E</td>
<td>1</td>
<td>[20:56:10]</td>
<td>cpd</td>
</tr>
<tr>
<td>FWD</td>
<td>440</td>
<td>E</td>
<td>1</td>
<td>[20:56:24]</td>
<td>fwd</td>
</tr>
<tr>
<td>FWM</td>
<td>467</td>
<td>E</td>
<td>1</td>
<td>[20:56:25]</td>
<td>fwm</td>
</tr>
</tbody>
</table>

**cpwd_admin exist**

**Description**
Check whether cpwd is alive.

**Usage**
cpwd_admin exist

**cpwd_admin kill**

**Description**
Kill cpwd.

**Usage**
cpwd_admin kill

**cpwd_admin config**

**Description**
Set cpwd configuration parameters. When parameters are changed, these changes will not take affect until cpwd has been stopped and restarted.

**Usage**
cpwd_admin config -p
cpwd_admin config

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config -p</td>
<td>Shows the cpwd parameters added using the config -a option.</td>
</tr>
<tr>
<td>config -a</td>
<td>Add one or more monitoring parameters to the cpwd configuration.</td>
</tr>
<tr>
<td>config -d</td>
<td>Delete one or more parameters from the cpwd configuration</td>
</tr>
<tr>
<td>config -r</td>
<td>Restore the default cpwd parameters.</td>
</tr>
</tbody>
</table>

Where the values are as follows:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout (any value in seconds)</td>
<td>If rerun_mode=1, how much time passes from process failure to rerun. The default is 60 seconds.</td>
</tr>
<tr>
<td>no_limit (any value in seconds)</td>
<td>Maximum number of times that cpwd will try to restart a process. The default is 5.</td>
</tr>
<tr>
<td>zero_timeout (any value in seconds)</td>
<td>After failing no_limit times to restart a process, cpwd will wait zero_timeout seconds before retrying. The default is 7200 seconds. Should be greater than timeout.</td>
</tr>
</tbody>
</table>
| sleep_mode      | • 1 - wait timeout  
                  • 0 - ignore timeout. Rerun the process immediately |
Example
The following example shows two configuration parameters being changed:
timeout to 120 seconds, and no_limit to 10.

# C:\>cpwd_admin config -p
WD doesn't have configuration parameters

C:\>cpwd_admin config -a timeout=120 no_limit=12

C:\>cpwd_admin config -p
WD Configuration parameters are:
timeout : 120
no_limit : 12

cpwd_admin config -a and cpwd_admin config -d have no effect if cpwd is running. They will affect cpwd the next time it is run.
dbedit

**Description**
Edit the objects file on the Security Management server. Editing the objects.C file on the gateway is not required or desirable, since it will be overwritten the next time a Policy is installed.

**Usage**

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s server</td>
<td>The Security Management server on which the objects_5_0.C file to be edited is located. If this is not specified in the command line, then the user will be prompted for it. If the server is not localhost, the user will be required to authenticate.</td>
</tr>
<tr>
<td>-u user</td>
<td>-c certificate</td>
</tr>
<tr>
<td>-p password</td>
<td>The user’s password (the password used for the SmartConsole).</td>
</tr>
<tr>
<td>-f filename</td>
<td>The name of the file containing the commands. If filename is not given, then the user will be prompted for commands.</td>
</tr>
<tr>
<td>-r db-open-reason</td>
<td>A non-mandatory flag used to open the database with a string that states the reason. This reason will be attached to audit logs on database operations.</td>
</tr>
<tr>
<td>-help</td>
<td>Print usage and short explanation.</td>
</tr>
</tbody>
</table>
**dbedit commands:**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>create</td>
<td>Create an object with its default values. The create command may use an extended (or “owned”) object. Changes are committed to the database only by an update or quit command.</td>
</tr>
<tr>
<td>modify</td>
<td>Modify fields of an object which is: • stored in the database (the command will lock the object in such case). • newly created by dbedit. Extended Formats for owned objects can be used: For example, [field_name] = Field_A:Field_B</td>
</tr>
<tr>
<td>update</td>
<td>Update the database with the object. This command will check the object validity and will issue an error message if appropriate.</td>
</tr>
<tr>
<td>delete</td>
<td>Delete an object from the database and from the client implicit database.</td>
</tr>
<tr>
<td>adddelement</td>
<td>Add an element (of type string) to a multiple field.</td>
</tr>
</tbody>
</table>
Example

Replace the owned object with a new null object, where NULL is a reserved word specifying a null object:

```plaintext
modify network_objects my_obj firewall_setting NULL
```

Example

Extended Format

`firewall_properties` owns the object `floodgate_preferences`.

`floodgate_preferences` has a Boolean attribute `turn_on_logging`, which will be set to true.

```plaintext
modify properties firewall_properties
floodgate_preferences:turn_on_logging true
```

Comments is a field of the owned object contained in the ordered container. The 0 value indicates the first element in the container (zero based index).

```plaintext
modify network_objects my_networkObj interfaces:0:comments
my_comment
```
Replace the owned object with a new one with its default values.

```
modify network_objects my_net_obj interfaces:0:security
interface_security
```
dbver

**Description**
The `dbver` utility is used to *export* and *import* different revisions of the database. The properties of the revisions (last time created, administrator responsible for, etc) can be reviewed. The utility can be found in `$FWDIR/bin`.

**Usage**

- `export <version_numbers> <delete | keep>`
- `import <exported_version_in_server>`
- `create <version_name> <version_comment>`
- `delete <version_numbers>`
- `print <version_file_path>`
- `print_all`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>version_name</code></td>
<td>the name of the revision</td>
</tr>
<tr>
<td><code>version_comment</code></td>
<td>append a comment to the revision</td>
</tr>
</tbody>
</table>

---

**dbver create**

**Description**
Create a revision from the current state of `$fwdir/conf`, including current objects, rule bases, etc.

**Usage**
`create <version_name> <version_comment>`

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>version_name</code></td>
<td>the name of the revision</td>
</tr>
<tr>
<td><code>version_comment</code></td>
<td>append a comment to the revision</td>
</tr>
</tbody>
</table>
**dbver export**

**Description**  
Archive the revision as an archive file in the revisions repository: $fwdir/conf/db_versions/export.

**Usage**  
export <version_numbers> <delete | keep>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>update [table_name]</td>
<td>Update the database with the object. This command will check the object</td>
</tr>
<tr>
<td></td>
<td>validity and will issue an error message if appropriate.</td>
</tr>
<tr>
<td>delete [table_name]</td>
<td>Delete an object from the database and from the client implicit database.</td>
</tr>
<tr>
<td>addelement [table_name]</td>
<td>Add an element (of type string) to a multiple field.</td>
</tr>
<tr>
<td></td>
<td>[object_name] [field_name] [value]</td>
</tr>
<tr>
<td>version_numbers</td>
<td>the file name of the exported version</td>
</tr>
<tr>
<td>delete</td>
<td>keep</td>
</tr>
<tr>
<td></td>
<td>- keep maintains the revision in the revisions repository.</td>
</tr>
</tbody>
</table>

**dbver import**

**Description**  
Add an exported revision to the repository a version from $fwdir/conf/db_versions/export. Give filename of revision as input.

**Usage**  
import <exported_version_in_server>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exported_version_in_server</td>
<td>The file name of the exported version.</td>
</tr>
</tbody>
</table>
dbver print

**dbver print**

**Description**
Print the properties of the revision.

**Usage**
print <version_file_path>

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version_file_path</td>
<td>The full name and path on the local machine of the revision.</td>
</tr>
</tbody>
</table>

**Output**

```
dbver> print c:\rwright_2002-04-01_160810.tar.gz
Version Id: 1
Version Date: Mon Apr  1 16:08:10 2009
Version Name: save
Created by Administrator: jbrown
Major Version: R70
Minor Version: R70
```

**dbver print_all**

**Description**
Print the properties of all revisions to be found on the server side: $fwdir/conf/db_versions

**Usage**
print_all
**dynamic_objects**

**Description**

dynamic_objects specifies an IP address to which the dynamic object will be resolved on this machine. This command cannot be executed when the Check Point gateway is running.

**Usage**
dynamic_objects -o <object_name> [-r [fromIP toIP] ...] [-a] [-d] [-l] [-n <object_name>] [-c]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-o &lt;object_name&gt;</td>
<td>The name of the object, as defined in SmartDashboard.</td>
</tr>
<tr>
<td>-r [fromIP toIP] ...</td>
<td>address ranges — one or more “from IP address to IP address” pairs</td>
</tr>
<tr>
<td>-a [fromIP toIP] ...</td>
<td>add ranges to object</td>
</tr>
<tr>
<td>-d [fromIP toIP] ...</td>
<td>delete range from object</td>
</tr>
<tr>
<td>-l</td>
<td>list dynamic objects</td>
</tr>
<tr>
<td>-n object_name</td>
<td>create new object (if Security Gateway is not running)</td>
</tr>
<tr>
<td>-c</td>
<td>compare the objects in the dynamic objects file and in objects.C.</td>
</tr>
<tr>
<td>-do object_name</td>
<td>delete object</td>
</tr>
</tbody>
</table>

**Example**

Create a new dynamic object named “bigserver” and add to it the IP address range 190.160.1.1-190.160.1.40: dynamic_objects -n bigaserver -r 190.160.1.1 190.160.1.40 -a
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

In This Section

fw -i  page 83
fw ctl  page 83
fw ctl affinity  page 87
fw ctl debug  page 85
fw ctl engine  page 90
fw ctl multik stat  page 91
fw ctl sdstat  page 92
fw fetch  page 93
fw fetchlogs  page 95
fw hastat  page 96
fw isp_link  page 96
fw kill  page 97
fw lea_notify  page 97
fw lichosts  page 98
fw log  page 98
fw logswitch  page 102
fw mergefiles  page 104
fw monitor  page 105
fw lslogs  page 113
fw putkey  page 115
fw repairlog  page 116
fw sam  page 117
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.
fw ctl

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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| <Install|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.  
• Install — tells the operating system to start passing packets to the Security Gateway. The command `fw ctl install` runs automatically when `cpstart` is performed.  
**Note** - If you run `fw ctl uninstall` followed by `fw ctl install`, the Security Policy is not restored. |
| debug        | Generate debug messages to a buffer. See “fw ctl debug” on page 85.                                                                                     |
| kdebug       | Reads the debug buffer and obtains the debug messages. If there is no debug buffer, the command will fail.  
• [-f] read the buffer every second and print the messages, until Ctrl-C is pressed. Otherwise, read the current buffer contents and end.  
• [-t/-T] print the time field (seconds/microseconds)  
• [-p] to print specific fields: all|proc|pid|date|mid|type|freq|topic|time|ticks|tid|text|err|host|vsid|cpu  
• [-m] - number of cyclic files, [-s] - size of each field.                                                                                                                                 |
|
**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
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| pstat    | Displays Security Gateway internal statistics:  
- h — Generates additional hmem details.  
- k — Generates additional kmem details.  
- s — Generates additional smem details.  
- n — Generates NDIS information (Windows only).  
- l — Generates general Security Gateway statistics. |
| iflist   | Displays the IP interfaces known to the kernel, by name and internal number |
| arp      | Displays ARP proxy table.  
- n — Do not perform name resolution. |
| block    | on — Blocks all traffic.  
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. |
## Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-buf [buffer size]</code></td>
<td>Allocates a buffer of size kilobytes (default 128) and starts collecting messages there. If the <code>-buf</code> argument is not set, the debug messages are printed to the console.</td>
</tr>
<tr>
<td><code>-m &lt;module&gt;</code></td>
<td>Specify the Security Gateway module you wish to debug. The default module is <code>fw</code>. For example: <code>fw ctl debug -m VPN all</code></td>
</tr>
</tbody>
</table>
| `[+ | -] <options|all|0>` | Sets or resets debug flags for the requested gateway.  
  - If `+` is used, the specified flags are set, and the rest remain as they were.  
  - If `-` is used, the specified flags are reset, and the rest remain as they were.  
  - 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)  
  For example: `fw ctl debug -d error,failed,^packet`  
  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)  
  For example: `fw ctl debug -s error` |
| `-x` | Shuts down the debug. |
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 Firewall Administration Guide.
http://supportcontent.checkpoint.com/documentation_download?ID=8738
/fwctl 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 Performance Pack Administration Guide
http://supportcontent.checkpoint.com/documentation_download?ID=8739

or edit the fwaffinity.conf configuration file (see the Firewall Administration Guide.

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:
fw ctl affinity

<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 Firewall Administration Guide.

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:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;pid&gt;</td>
<td>Sets affinity for a particular process, where &lt;pid&gt; is the process ID#.</td>
</tr>
<tr>
<td>-n &lt;cpdname&gt;</td>
<td>Sets affinity for a Check Point daemon, where &lt;cpdname&gt; is the Check Point daemon name (for example: fwd).</td>
</tr>
<tr>
<td>-k &lt;instance&gt;</td>
<td>Sets affinity for a kernel instance, where &lt;instance&gt; is the instance’s number.</td>
</tr>
<tr>
<td>-i &lt;interfacename&gt;</td>
<td>Sets affinity for an interface, where &lt;interfacename&gt; is the interface name (for example: eth0).</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-p &lt;pid&gt;</code></td>
<td>Displays the affinity of a particular process, where <code>&lt;pid&gt;</code> is the process ID#.</td>
</tr>
<tr>
<td><code>-n &lt;cpdname&gt;</code></td>
<td>Displays the affinity of a Check Point daemon, where <code>&lt;cpdname&gt;</code> is the Check Point daemon name (for example: <code>fwd</code>).</td>
</tr>
<tr>
<td><code>-k &lt;instance&gt;</code></td>
<td>Displays the affinity of a kernel instance, where <code>&lt;instance&gt;</code> is the instance’s number.</td>
</tr>
<tr>
<td><code>-i &lt;interfacename&gt;</code></td>
<td>Displays the affinity of an interface, where <code>&lt;interfacename&gt;</code> is the interface name (for example: <code>eth0</code>).</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>All: includes items without specific affinities.</td>
</tr>
<tr>
<td><code>-r</code></td>
<td>Reverse: lists each processing core and the items that have it as their affinity.</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Verbose: list includes additional information.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| on       | Compile the engine if necessary, and activate it. 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.  

After turning the engine ON, the engine recompiles and reactivates itself every policy installation regardless of the values of inspect2c_compile and inspect2c_activate. |
**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.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Deactivates the engine if active. Subsequent policy installation on the gateway do NOT auto-activate the engine unless the command is used again.</td>
</tr>
<tr>
<td>stat</td>
<td>Print the status of the engine. For example: “During compilation”, “Before auto-activation”, “Deactivated”.</td>
</tr>
</tbody>
</table>
| setdefault | Restore control to database settings. Security Management server settings are ignored. At the next policy installation, return the control of the engine to the values of the following gateway database attributes:  
  - 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.  
  - 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. Use GuiDBEdit to change the values of the attributes. |
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fw ctl zdebug &gt;&amp; outputfile</td>
<td>Turn on debug mode and specify an output file.</td>
</tr>
<tr>
<td>fw ctl sdstat start</td>
<td>Activate the IPS counters</td>
</tr>
<tr>
<td>fw ctl sdstat stop</td>
<td>Print a report and stop the counters.</td>
</tr>
</tbody>
</table>

**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`

<table>
<thead>
<tr>
<th>Example Debug Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sdstat_get_stats_all_instances</code>: Smart Defense report objects are not initialized, hence no report can be done.</td>
<td>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.</td>
</tr>
<tr>
<td><code>FW-1 - sdstats_print_report: Failed to calculate Smart Defense (total_smart_defense is 0)</code></td>
<td>The measurement process failed and the total time units for IPS is zero.</td>
</tr>
</tbody>
</table>

**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] ...
```
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n</td>
<td>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.</td>
</tr>
<tr>
<td>-f &lt;filename&gt;</td>
<td>Fetch the Security Policy from the Security Management server listed in &lt;filename&gt;. If filename is not specified, the list in conf/masters is used.</td>
</tr>
<tr>
<td>-c</td>
<td>Cluster mode, get policy from one of the cluster members, from the Check Point High Availability (CPHA) kernel list</td>
</tr>
<tr>
<td>-i</td>
<td>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.</td>
</tr>
<tr>
<td>master1</td>
<td>Execute command on the designated master. The name of the Security Management server from which to fetch the Policy. You may specify a list of one or more Security Management servers, such as master1 master2 which will be searched in the order listed. If no targets is not specified, or if targets is inaccessible, the Policy is fetched from localhost.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f filename</td>
<td>The Log Files to be transferred. The file name can include wildcards. In Solaris, any file containing wildcards should be enclosed in quotes. The default parameter is *.log. Related pointer files will automatically be fetched.</td>
</tr>
<tr>
<td>module</td>
<td>The name of the remote machine from where you transfer the Log Files.</td>
</tr>
</tbody>
</table>

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.
fw hastat

After the file has been fetched, the Log File is renamed:
module3_2001-12-31_123414.log


fw hastat

Description The fw hastat command displays information about High Availability machines and their states.

Usage fw hastat [<target>]

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;target&gt;</td>
<td>A list of machines whose status will be displayed. If target is not specified, the status of the local machine will be displayed.</td>
</tr>
</tbody>
</table>

fw isp_link

Description Takes down (or up) a redundant ISP link.

Usage fw isp_link [target] link-name {up|down}

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The name of the Check Point gateway.</td>
</tr>
<tr>
<td>link-name</td>
<td>The name of the ISP link as defined in the ISP-redundancy tab.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t sig_no</td>
<td>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. If no signal is specified, signal 15 (sigterm or the terminate command) is sent.</td>
</tr>
<tr>
<td>proc-name</td>
<td>Prompt the kernel to shut down specified firewall daemon processes.</td>
</tr>
</tbody>
</table>

**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.COLLOGS 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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-x</td>
<td>Use hexadecimal format.</td>
</tr>
<tr>
<td>-l</td>
<td>Use long format.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-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.  
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.  
`-t` must come with a `-f` flag. These flags are relevant only for active files. |
<p>| <code>-n</code>      | Do not perform DNS resolution of the IP addresses in the Log file (the default behavior). This option significantly speeds up the processing.          |
| <code>-l</code>      | 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). |
| <code>-o</code>      | Show detailed log chains (all the log segments a log record consists of)                                                                    |
| <code>-c action</code> | Display only events whose action is action, that is, accept, drop, reject, authorize, deauthorize, encrypt and decrypt. Control actions are always displayed. |
| <code>-h host</code> | Display only log whose origin is the specified IP address or name.                                                                           |</p>
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s starttime</td>
<td>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.</td>
</tr>
<tr>
<td>-e endtime</td>
<td>Display only events that were logged before the specified time (see format below). endtime may be a date, a time, or both.</td>
</tr>
<tr>
<td>-b starttime endtime</td>
<td>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.</td>
</tr>
<tr>
<td>-u</td>
<td>Unification scheme file name.</td>
</tr>
<tr>
<td>-m unification_mode</td>
<td>This flag specifies the unification mode.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• raw - output all records, with no unification.</td>
</tr>
</tbody>
</table>
Chapter 1  Security Management Server and Firewall Commands  101

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;

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Output account log records only.</td>
</tr>
<tr>
<td>-k alert_name</td>
<td>Display only events that match a specific alert type. The default is all, for any alert type.</td>
</tr>
<tr>
<td>-g</td>
<td>Do not use a delimited style. The default is:</td>
</tr>
<tr>
<td>logfile</td>
<td>Use logfile instead of the default Log file. The default Log File is $FWDIR/log/fw.log.</td>
</tr>
</tbody>
</table>
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 113 and “fw fetchlogs” on page 95.

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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-audit</td>
<td>Does logswitch for the Security Management server audit file. This is relevant for local activation.</td>
</tr>
<tr>
<td>filename</td>
<td>The name of the file to which the log is saved. If no name is specified, a default name is provided.</td>
</tr>
<tr>
<td>-h hostname</td>
<td>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.</td>
</tr>
<tr>
<td>+</td>
<td>Switch a remote log and copy it to the local machine</td>
</tr>
<tr>
<td>-</td>
<td>Switch a remote log and move it to the local machine thereby deleting the log from the remote machine.</td>
</tr>
</tbody>
</table>

### 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.

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.

Compress ion
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
fw monitor

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>Sort merged file by log records time field.</td>
</tr>
<tr>
<td>-t time_conversion_file</td>
<td>Fix different GMT zone log records time in the event that the log files originated from Log Servers in different time zone. The time_conversion_file format is as follows: ip-address signed_date_time_in_seconds ip-address signed_date_time_in_seconds . . log_file_name_n</td>
</tr>
<tr>
<td>output_file</td>
<td>Full pathname of the output Log File.</td>
</tr>
</tbody>
</table>

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
fw monitor

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.

- 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

### Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u</td>
<td>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.</td>
</tr>
<tr>
<td>-s</td>
<td></td>
</tr>
<tr>
<td>-i</td>
<td>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 <code>fw monitor</code> process and want to be sure that all data is written to a file.</td>
</tr>
<tr>
<td>[-d] [-D]</td>
<td>Debugging <code>fw monitor</code>: The -d option is used to start <code>fw monitor</code> in debug mode. This will give you an insight into <code>fw monitor</code>'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.</td>
</tr>
<tr>
<td>&lt;-e expr&gt;+</td>
<td>-f &lt;filter-file&gt;-</td>
</tr>
</tbody>
</table>
### Argument Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-l len</code></td>
<td><strong>Limiting the packet length:</strong> fw monitor allows you to limit the packet data which will be read from the kernel with <code>-l</code>. 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 size 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.</td>
</tr>
<tr>
<td><code>-m mask</code></td>
<td><strong>Setting capture masks:</strong> 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.</td>
</tr>
<tr>
<td><code>-x offset[,len]</code></td>
<td><strong>Printing packet/payload data:</strong> In addition to the IP and Transport header fw monitor can also print the packets’ raw data using the <code>-x</code> option. Optionally it is also possible to send all data that is written only to the screen the data written.</td>
</tr>
</tbody>
</table>
## Command Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-o <file>`        | **Write output to file:** Save the raw packet data to a file in a standard (RFC 1761) format. The file can be examined using tools like snoop, tcpdump or Ethereal.  
  **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. |
| `<[-pi pos] [-pl pos] [-po pos] [-pO pos] [-p] all>` | **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. |
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 multiple 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 CPEtheral and can be displayed by it.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td><strong>Use absolute chain positions</strong>: If you use <code>fw monitor</code> to output the capture into a file (option <code>-o</code>), one of the fields written down to the capture file is the chain position of the <code>fw monitor</code> chain module. Together with a simultaneous execution of <code>fw ctl chain</code> you can determine where the packet was captured. Especially when using <code>-p all</code> you will find the same packet captured multiples times at different chain positions. The option <code>-a</code> changes the chain id from an relative value (which only makes sense with the matching <code>fw ctl chain</code> output) to an absolute value. These absolute values are known to CPEtheral and can be displayed by it.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-ci count] [-co count]</td>
<td><strong>Capture a specific number of packets:</strong> <code>fw monitor</code> 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 <code>fw monitor</code> 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.</td>
</tr>
<tr>
<td>[-vs vsid or vsname]</td>
<td><strong>Capture on a specific Virtual Router or Virtual Machine:</strong> 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 <code>fw monitor</code> on FireWall-1 VSX for more information.</td>
</tr>
<tr>
<td>-h</td>
<td>Displays the usage.</td>
</tr>
</tbody>
</table>

**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.
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.


**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 [\[-f file name\] \[\ldots\]] [\[-e\] [\[-s name \mid size \mid stime \mid etime\]] [\[-r\] [\[machine\]]
```
### Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-f filename</code></td>
<td>The list of files to be displayed. The file name can include wildcards. In Unix, any file containing wildcards should be enclosed in quotes. The default parameter is <code>*.log</code>.</td>
</tr>
</tbody>
</table>
| `-e` | Display an extended file list. It includes the following data:  
- **Size** - The size of the file and its related pointer files together.  
- **Creation Time** - The time the Log File was created.  
- **Closing Time** - The time the Log File was closed.  
- **Log File Name** - The file name. |
| `-s` | Specify the sort order of the Log Files using one of the following sort options:  
- **name** - The file name.  
- **size** - The file size.  
- **stime** - The time the Log File was created.  
- **etime** - The time the Log File was closed.  
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
```

<table>
<thead>
<tr>
<th>Size</th>
<th>Creation Time</th>
<th>Closing Time</th>
<th>Log file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>16KB</td>
<td>10Jan2002 18:36:05</td>
<td>--</td>
<td>fw.log</td>
</tr>
</tbody>
</table>
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

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-opsec</td>
<td>Only control connections are enabled.</td>
</tr>
<tr>
<td>-no_opsec</td>
<td>Only OPSEC control connections are enabled.</td>
</tr>
<tr>
<td>-ssl</td>
<td>The key is used for an SSL connection.</td>
</tr>
<tr>
<td>-no_ssl</td>
<td>The key is not used for an SSL connection.</td>
</tr>
<tr>
<td>-k num</td>
<td>The length of the first S/Key password chain for fwal 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.</td>
</tr>
</tbody>
</table>
**fw repairlog**

**Arguments**

- **-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: “./fwd: Authentication with hostname for command sync failed”

**Comments**

This command is never used in a script.

**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-u</code></td>
<td>Indicates that the unification chains in the Log file should be rebuilt.</td>
</tr>
<tr>
<td><code>logfile</code></td>
<td>The name of the Log file to repair.</td>
</tr>
</tbody>
</table>
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][-1 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v</td>
<td>Verbose mode. Writes one message ot) to stderr for each Security Gateway machine on which the command is enforced.</td>
</tr>
<tr>
<td>-s sam_server</td>
<td>The IP address (in dot format) or the resolvable name of the FireWalled host that will enforce the command. The default is localhost.</td>
</tr>
<tr>
<td>-S server_sic_name</td>
<td>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.</td>
</tr>
<tr>
<td>-f &lt;fw host&gt;</td>
<td>Specify the host, the Security Gateway machine on which to enforce the action. host can be one of the following (default is All):</td>
</tr>
<tr>
<td></td>
<td>• localhost—Specify the computer running the SAM server to enforce the action on it.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Gateways—Action enforced on FireWalls defined as gateways and managed by Security Management server where the SAM server runs.</td>
</tr>
<tr>
<td></td>
<td>• All—Enforced on FireWalls managed by Smart- Center server where SAM server runs.</td>
</tr>
</tbody>
</table>
-D
Cancel all inhibit (-i, -j,-I,-J) and notify (-n) commands. 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.

-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.
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>
```

### 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

<table>
<thead>
<tr>
<th>Criteria Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>src &lt;ip&gt;</td>
<td>Match the source IP address of the connection.</td>
</tr>
<tr>
<td>dst &lt;ip&gt;</td>
<td>Match the destination IP address of the connection.</td>
</tr>
<tr>
<td>any &lt;ip&gt;</td>
<td>Match either the source IP address or the destination IP address of the connection.</td>
</tr>
<tr>
<td>subsrc &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match the source IP address of the connections according to the netmask.</td>
</tr>
<tr>
<td>subst &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match the destination IP address of the connections according to the netmask.</td>
</tr>
<tr>
<td>subany &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match either the source IP address or destination IP address of connections according to the netmask.</td>
</tr>
<tr>
<td>srv &lt;src ip&gt; &lt;dst ip&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match the specific source IP address, destination IP address, service and protocol.</td>
</tr>
<tr>
<td>subsrv &lt;src ip&gt; &lt;netmask&gt; &lt;dst ip&gt; &lt;netmask&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match the specific source IP address, destination IP address, service and protocol. Source and destination IP addresses are assigned according to the netmask.</td>
</tr>
<tr>
<td>subsrsvs &lt;src ip&gt; &lt;src netmask&gt; &lt;dest ip&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match the specific source IP address, source netmask, destination netmask, service and protocol.</td>
</tr>
<tr>
<td>subsrd &lt;src ip&gt; &lt;dest ip&gt; &lt;dest netmask&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match specific source IP address, destination IP, destination netmask, service and protocol.</td>
</tr>
<tr>
<td>dstsrv &lt;dst ip&gt; &lt;service&gt; &lt;protocol&gt;</td>
<td>Match specific destination IP address, service and protocol.</td>
</tr>
</tbody>
</table>
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 louvre is the source or destination address:

fw sam -M -nij any louvre

This command cancels the command in the first example:

fw sam -C -i src louvre

<table>
<thead>
<tr>
<th>Criteria Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>substsrv &lt;dst ip&gt;</td>
<td>Match specific destination IP address, service and protocol. Destination IP address is assigned according to the netmask.</td>
</tr>
<tr>
<td>&lt;netmask&gt; &lt;service&gt;</td>
<td></td>
</tr>
<tr>
<td>&lt;protocol&gt;</td>
<td></td>
</tr>
<tr>
<td>srcpr &lt;ip&gt; &lt;protocol&gt;</td>
<td>Match the source IP address and protocol.</td>
</tr>
<tr>
<td>dstpr &lt;ip&gt; &lt;protocol&gt;</td>
<td>Match the destination IP address and protocol.</td>
</tr>
<tr>
<td>subsrcpr &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match the source IP address and protocol of connections. Source IP address is assigned according to the netmask.</td>
</tr>
<tr>
<td>&lt;protocol&gt;</td>
<td></td>
</tr>
<tr>
<td>substpr &lt;ip&gt; &lt;netmask&gt;</td>
<td>Match the destination IP address and protocol of connections. Destination IP address is assigned according to the netmask.</td>
</tr>
<tr>
<td>&lt;protocol&gt;</td>
<td></td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-all</td>
<td>The command is to be executed on all targets specified in the default system configuration file (<code>$FWDIR/conf/sys.conf</code>).</td>
</tr>
<tr>
<td>-conf conffile</td>
<td>The command is to be executed on the targets specified in conffile.</td>
</tr>
<tr>
<td>-s</td>
<td>Summary of the number of entries in each table: host name, table name, table ID, and its number of entries</td>
</tr>
<tr>
<td>-m number</td>
<td>For each table, display only its first number of elements (default is 16 entries at most).</td>
</tr>
<tr>
<td>-u</td>
<td>Do not limit the number of entries displayed for each table.</td>
</tr>
<tr>
<td>-t tname</td>
<td>Display only tname table.</td>
</tr>
<tr>
<td>-x tname</td>
<td>Delete all entries in all tables</td>
</tr>
<tr>
<td>-d</td>
<td>Debug mode</td>
</tr>
<tr>
<td>targets</td>
<td>The command is executed on the designated targets.</td>
</tr>
</tbody>
</table>

**Example**

To display only the `arp_table` table,
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t &lt;table&gt;</td>
<td>Specifies a table for the command.</td>
</tr>
<tr>
<td>-s</td>
<td>Displays a short summary of the table(s) information.</td>
</tr>
<tr>
<td>-y</td>
<td>Specifies to not prompt a user before executing any commands.</td>
</tr>
<tr>
<td>-f</td>
<td>Displays a formatted version of the table content. Every table may have its own specific format style.</td>
</tr>
<tr>
<td>-o &lt;filename&gt;</td>
<td>Dumps CL formatted output to filename, which can later be read by fw log or any other entity that can read FW log formats.</td>
</tr>
<tr>
<td>-c</td>
<td>Displays formatted table information in common format.</td>
</tr>
<tr>
<td>-r</td>
<td>Resolves IP addresses in formatted output.</td>
</tr>
<tr>
<td>-x, -a, -e</td>
<td>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 (&lt;entry&gt;).</td>
</tr>
</tbody>
</table>

**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. |
fw ver

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:
<0000000001,000000002,000000003,000000004,000000005,>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:
<0000000000000001,000000002>
fw tab -t <table-name> -x -e “0,1” or
fw tab -t <table-name> -x -e “0,1;2”
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-k</td>
<td>Print the version name and build number of the Kernel module.</td>
</tr>
<tr>
<td>-f &lt;filename&gt;</td>
<td>Print the version name and build number to the specified file.</td>
</tr>
</tbody>
</table>
fwm

**Description**
Perform management operations on the Security Gateway. It controls `fwd` and all Check Point daemons.

**Usage**
fwm

In This Section

- `fwm dbimport`
- `fwm expdate`
- `fwm dbexport`
- `fwm dbload`
- `fw hastat`
- `fwm ikecrypt`
- `fwm load`
- `fwm lock_admin`
- `fwm logexport`
- `fwm sic_reset`
- `fwm unload <targets>`
- `fwm ver`
- `fwm verify <policy-name>`

**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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m</td>
<td>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.</td>
</tr>
<tr>
<td>-s</td>
<td>Suppress the warning messages issued when an existing user's values are changed by values in the import file.</td>
</tr>
<tr>
<td>-v</td>
<td>verbose mode</td>
</tr>
<tr>
<td>-r</td>
<td>fwm dbimport will delete all existing users in the database.</td>
</tr>
<tr>
<td>-k errors</td>
<td>Continue processing until nerror errors are encountered. The line count in the error messages starts from 1 including the attributes line and counting empty or commented out lines.</td>
</tr>
<tr>
<td>-f file</td>
<td>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.</td>
</tr>
<tr>
<td>-d delim</td>
<td>Specifies a delimiter different from the default value (;).</td>
</tr>
</tbody>
</table>

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
“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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-g group</td>
<td>Specifies a group (group) to be exported. The users in the group are not exported.</td>
</tr>
<tr>
<td>-u user</td>
<td>Specifies that only one user (user) is to be exported.</td>
</tr>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>-a {attrib1, attrib2, ...}</td>
<td>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.</td>
</tr>
<tr>
<td>-f file</td>
<td>file specifies the name of the output file. The default output file is $FWDIR/conf/user_def_file.</td>
</tr>
<tr>
<td>-l</td>
<td>Create an LDIF format file for importation by an LDAP server.</td>
</tr>
<tr>
<td>-p</td>
<td>The profile name.</td>
</tr>
<tr>
<td>-s</td>
<td>The branch under which the users are to be added.</td>
</tr>
<tr>
<td>-k</td>
<td>This is the Account Unit's IKE shared secret (IKE Key in the Encryption tab of the Account Unit Properties Window)</td>
</tr>
</tbody>
</table>

## Comments

Note:

- 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 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.

**Usage**

fwm ikecrypt shared-secret user-password

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-all</td>
<td>Execute command on all targets specified in the default system configuration file ($FWDIR/conf/sys.conf). This file must be manually created.</td>
</tr>
<tr>
<td>-conf conffile</td>
<td>Only OPSEC control connections are enabled.</td>
</tr>
<tr>
<td>targets</td>
<td>Execute command on the designated targets.</td>
</tr>
</tbody>
</table>

**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.

---

**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` 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-S</td>
<td>The targets are UTM-1 Edge gateways.</td>
</tr>
<tr>
<td>-p</td>
<td>Specifies the product name if applicable.</td>
</tr>
<tr>
<td>rulebase</td>
<td>A Rule Base created by the GUI. Specify the name of the rulebase, such as Standard (case sensitive).</td>
</tr>
<tr>
<td>-v version number</td>
<td>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.</td>
</tr>
<tr>
<td>targets</td>
<td>Execute command on the designated target.</td>
</tr>
</tbody>
</table>

**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]

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v v</td>
<td>View the names of all locked administrators</td>
</tr>
<tr>
<td>-u administrator</td>
<td>Unlock a single administrator</td>
</tr>
<tr>
<td>-ua</td>
<td>Unlock all locked administrators</td>
</tr>
</tbody>
</table>

### fwm logexport

**Description**
fwm logexport exports the Log file to an ASCII file.

**Usage**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d delimiter</td>
<td>Set the output delimiter. The default is a semicolon (;)</td>
</tr>
<tr>
<td>-i filename</td>
<td>The name of the input Log file. The default is the active Log file, fw.log</td>
</tr>
<tr>
<td>-o outputfile</td>
<td>The name of the output file. The default is printing to the screen.</td>
</tr>
<tr>
<td>-n</td>
<td>Do not perform DNS resolution of the IP addresses in the Log file (this option significantly speeds the processing).</td>
</tr>
<tr>
<td>-p</td>
<td>Do not perform service resolution. A service port number is displayed.</td>
</tr>
</tbody>
</table>
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.
fwm sic_reset

- 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sic_reset</td>
<td>Resets the internal CA SIC certificates and deletes the Internal CA.</td>
</tr>
</tbody>
</table>
### fwm unload <targets>

**Description**
Uninstall the currently loaded Inspection Code from selected targets.

**Usage**
fwm unload <targets>[-all | -conf conffile]

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targets</td>
<td>Execute command on the designated targets.</td>
</tr>
<tr>
<td>-all</td>
<td>Execute command on all targets specified in the default system configuration file ($FWDIR/conf/sys.conf). This file must be manually created.</td>
</tr>
<tr>
<td>conf conffile</td>
<td>Execute command on targets specified in the conffile.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;policy-name&gt;</td>
<td>The name of an available policy package.</td>
</tr>
</tbody>
</table>
**GeneratorApp**

**Description**
Generate a report for Eventia Reporter. Both command line parameters are required.

**Usage**
GeneratorApp [Directory/"" ] {ReportID}

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>The result directory (that is, the location at which the result is placed).</td>
</tr>
</tbody>
</table>

**Example**
For automatic directory computation use "". In such a case, the directory should be as follows:

<Result location>/<Report Name>/<Generation Date and Time>
**inet_alert**

**Description**
Notify a company's Internet Service Provider (ISP) when the company's corporate network is under attack. The `inet_alert` utility forwards log messages generated by the alert daemon to an external Management Station, typically located at the ISP site. The ISP can then analyze the alert and decide how to react.

`inet_alert` uses the ELA Protocol to send the alert. The Management Station receiving the alert must be running the ELA Proxy.

If communication with the ELA Proxy is to be authenticated or encrypted, a key exchange must be performed between the Management Station running the ELA Proxy and the Security Gateway generating the alert.

To use this utility, enter it into a script. From Global Properties > Logs and alert > alert commands > early versions compatibility > run 4.x alert script, and enter the name of the script.

**Usage**
```
inet_alert -s ipaddr [-o] [-a auth_type] [-p port] [-f token value] [-m alerttype]
```

**Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-s ipaddr</code></td>
<td>The IP address (in dot format) of the ELA Proxy to be contacted.</td>
</tr>
<tr>
<td><code>-o</code></td>
<td>Print the alert log received by <code>inet_alert</code> to stdout. Use this option when <code>inet_alert</code> is part of a pipe.</td>
</tr>
<tr>
<td><code>-a auth_type</code></td>
<td>The type of connection to the ELA Proxy. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• <code>ssl_opsec</code>. Means the connection is authenticated and encrypted, (Default)</td>
</tr>
<tr>
<td></td>
<td>• <code>auth_opsec</code>. Means the connection is authenticated.</td>
</tr>
<tr>
<td></td>
<td>• <code>clear</code>. Means the connection is neither authenticated nor encrypted.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Meaning</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-p port</td>
<td>The ELA Proxy's port number. Default is 18187.</td>
</tr>
<tr>
<td>-f token value</td>
<td>A field to be added to the log, represented by a token-value pair as follows:  &lt;br&gt;      &lt;br&gt;     • token is the name of the field to be added to the log. token may not contain spaces.  &lt;br&gt;     • value is the field’s value. value may not contain spaces.  &lt;br&gt;      This option may be used multiple times to add multiple token-value pairs to the log.  &lt;br&gt;      If token is a reserved log field name, the specified field’s value will appear in the corresponding column in SmartView Tracker. Otherwise, the token-value pair will be displayed in the Info. column in SmartView Tracker.</td>
</tr>
<tr>
<td>-m alertty</td>
<td>The alert to be triggered at the ISP site. This alert overrides the alert specified in the log message generated by the alert daemon.  &lt;br&gt;      The response to the alert is handled according to the actions specified in the ISP’s Security Policy:  &lt;br&gt;      The following alerts execute the OS commands defined in the corresponding fields of the Log and Alert tab of the Properties Setup window in Global Properties:  &lt;br&gt;      • alert. Popup alert command.  &lt;br&gt;      • mail. Mail alert command.  &lt;br&gt;      • snmptrap. SNMP trap alert command.  &lt;br&gt;      • spoofalert. Anti-spoof alert command.  &lt;br&gt;      The following NetQuota and ServerQuota alerts execute the OS commands specified in:  &lt;br&gt;      $FWDIR/conf/objects.C:  &lt;br&gt;      value=clientquotaalert.  &lt;br&gt;      Parameter=clientquotaalertcmd</td>
</tr>
</tbody>
</table>
Return Value

<table>
<thead>
<tr>
<th>exit status</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Execution was successful.</td>
</tr>
<tr>
<td>102</td>
<td>Undetermined error.</td>
</tr>
<tr>
<td>103</td>
<td>Unable to allocate memory.</td>
</tr>
<tr>
<td>104</td>
<td>Unable to obtain log information from stdin.</td>
</tr>
<tr>
<td>106</td>
<td>Invalid command line arguments.</td>
</tr>
<tr>
<td>107</td>
<td>Failed to invoke the OPSEC API.</td>
</tr>
</tbody>
</table>

Example

inet_alert -s 10.0.2.4 -a clear -f product cads -m alert

This command specifies that in the event of an attack, inet_alert should take the following actions:

- Establish a clear connection with the ELA Proxy located at IP address 10.0.2.4.
- Send a log message to the specified ELA Proxy. The product field of this log message should be set to "cads". This means that "cads" will be displayed in the product column of SmartView Tracker.
- Trigger the OS command specified in the Popup Alert Command field of the Log and Alert tab of the Properties Setup window in the SmartDashboard.
ldapcmd

Description
ldapcmd is used to manage processes running on the Security Gateway collectively or individually. It includes:

Cache
Cache operations, such as emptying the cache, as well as providing debug information.

Statistics
lookup statistics such as, all user search, pending lookups (when two or more lookups are identical) and total lookup time (the total search time for a specific lookup)
cache statistics such as hits and misses

Logging
view the alert and warning log regarding debug

Usage
ldapcmd -p process_name | all command [-d debug_level] [command_arg]

where command is:
• cacheclear (either all or UserCacheObject or TemplateCacheObject or TemplateExtGrpCacheObject)
• cachetrace (either all or UserCacheObject or TemplateCacheObject or TemplateExtGrpCacheObject)
• stat [either print_interval (reset interval time in secs) or 0 (stop statistics)]
• log (either on or off)

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>run a specified process or run all processes</td>
</tr>
<tr>
<td>command</td>
<td>specify a command</td>
</tr>
<tr>
<td>log</td>
<td>specify whether or not to create LDAP logs</td>
</tr>
</tbody>
</table>
**ldapcompare**

**Description**

ldapcompare is used to perform compare queries that prints a message whether the result returned a match or not. ldapcompare opens a connection to an LDAP directory server, binds, and performs the comparison specified on the command line or from a specified file.

**Usage**

```bash
ldapcompare -d [options] dn attribute value
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>options</td>
<td>See below.</td>
</tr>
<tr>
<td>dn</td>
<td>The DN object.</td>
</tr>
<tr>
<td>attribute</td>
<td>The attribute of the DN object.</td>
</tr>
<tr>
<td>value</td>
<td>The value of the attribute of the DN object.</td>
</tr>
</tbody>
</table>

The ldapcompare options are as follows:

- `-u` - Include user-friendly entry names in the output.
- `-d <level>` - Set LDAP debugging level to “level”.
- `-F sep` - Print “sep” instead of “=” between attribute names and values.
- `-f <file>` - Perform sequence of compares listed in “file”.
- `-D <binddn>` - Bind DN.
- `-w <passwd>` - Bind password (for simple authentication).
- `-h <host>` - LDAP server.
- `-p <port>` - Port on the LDAP server.
- `-T <timeout>` - Client side timeout for all operations (in milliseconds).
- `-l <time limit>` - Server Side time limit (in seconds) for compare.
- `-z <size limit>` - Server Side size limit (in entries) for compare.
**Idapconvert**

**Description**
Idapconvert is a utility program to port from Member mode to MemberOf mode. This is done by searching all specified group/template entries and fetching their Member attribute values.

Each value is the DN of a member entry. The entry identified by this DN will be added the MemberOf attribute value of the group/template DN at hand. In addition, those Member attribute values will be deleted from the group/template unless Both mode is specified.

While running the program, a log file, named `ldapconvert.log`, is generated in the current directory, logging all modifications done and errors encountered.

**Usage**
```
Idapconvert -d -h <host> -p <port> -D user_DN -w <secret> [-g group_DN | -f <file>] -m mem_attr -o memberof_attr -c memberobjectclass[extra options]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>-h &lt;host&gt;</td>
<td>LDAP server IP address.</td>
</tr>
<tr>
<td>-p &lt;port&gt;</td>
<td>LDAP server port number.</td>
</tr>
<tr>
<td>-D user_DN</td>
<td>LDAP bind DN.</td>
</tr>
<tr>
<td>-w &lt;secret&gt;</td>
<td>LDAP bind password.</td>
</tr>
<tr>
<td>-g group_DN</td>
<td>Group or template DN to perform the conversion on. May appear multiple times for multiple entries.</td>
</tr>
<tr>
<td>-f &lt;file&gt;</td>
<td>File containing a list of group DNs each separated by a new line.</td>
</tr>
<tr>
<td>-m mem_attr</td>
<td>LDAP attribute name when fetching and (possibly) deleting a Member attribute value.</td>
</tr>
</tbody>
</table>
The `ldapconvert` extra options are as follows:

- `-M - Maximum number of member LDAP updated simultaneously (default is 20).
- `-B - Convert to Both mode
- `-p <port> - LDAP port (default is 389).
- `-T <timeout> - Client side timeout for LDAP operations, in milliseconds: default is “never”.
- `-l <time limit> - Server side time limit for LDAP operations, in seconds: default is “never”.
- `-s - Server side size limit for LDAP operations (in entries) (default is “none”).
- `-z - Use SSL.

**Comments**

It is recommended to backup the LDAP server before running the conversion program in case unrecoverable errors are encountered.

There are two `GroupMembership` modes: template-to-groups and user-to-groups. It is imperative to keep these modes consistent. For instance, if you apply conversion on LDAP users to include ‘MemberOf’ attributes for their groups, then this conversion should also be applied on LDAP defined templates for their groups.

**Why does a command run with the option `─M` fail?**

The program terminates with an error message stating the connection terminated unexpectedly.

This means that the LDAP server could not handle so many LDAP requests simultaneously and closed the connection. The solution is to run the program again with a lower value for the `─M` option (the default value should be adequate but could also cause a connection failure in
ldapconvert

extreme situation). Continue to reduce the value until the program exits normally. Each time you run the program with the same set of groups the program will pick up where it left off.

Example

A group is defined with the DN: \texttt{cn=cpGroup,ou=groups, ou=cp, c=il}
and the following attributes:

\begin{verbatim}
... 
  cn=cpGroup
  uniquemember="cn=member1,ou=people, ou=cp,c=il"
  uniquemember="cn=member2, ou=people, ou=cp,c=il"
...
\end{verbatim}

For the 2 member entries:

\begin{verbatim}
... 
  cn=member1
  objectclass=fw1Person
...
\end{verbatim}

and:

\begin{verbatim}
... 
  cn=member2
  objectclass=fw1Person
...
\end{verbatim}

Run 	exttt{ldapconvert} with the following arguments:

\texttt{ldapconvert -g cn=cpGroup,ou=groups, ou=cp, c=il -h myhost -d cn=admin -w secret -m uniquemember -o memberof -c fw1Person}

The result for the group DN will be as follows:

\begin{verbatim}
... 
  cn=cpGroup
...
\end{verbatim}

The result for the 2 member entries will be as follows:

\begin{verbatim}
... 
  cn=member1
  objectclass=fw1Person
  memberof="cn=cpGroup,ou=groups, ou=cp, c=il"
...
\end{verbatim}

and

\begin{verbatim}
... 
  cn=member2
  objectclass=fw1Person
  memberof="cn=cpGroup,ou=groups, ou=cp, c=il"
...
\end{verbatim}
Running the same command with the -B options, will produce the same result but the group entry will not be modified.

If there exists another member attribute value for the same group entry:

```text
uniquemember="cn=template1,ou=people, ou=cp,c=il"
```

and the template is:

```text
cn=member1
objectclass=fw1Template
```

after running the same command line the template entry will stay intact because the command line specified the option -c fw1Person but the object class of template1 is fw1Template.
ldapmodify

Description
ldapmodify imports users to an LDAP server. The input file must be in the LDIF format.

Usage
ldapmodify -a -c -d -h <host> -p <port> -D <LDAPadminDN> -p <LDAPadminPassword> -f <exportfilename>.ldif -d

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Add users.</td>
</tr>
<tr>
<td>-c</td>
<td>Continue on errors.</td>
</tr>
<tr>
<td>-h &lt;host&gt;</td>
<td>LDAP server IP address.</td>
</tr>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>-p &lt;port&gt;</td>
<td>LDAP server port number.</td>
</tr>
<tr>
<td>-D &lt;LDAPadminDN&gt;</td>
<td>LDAP Administrator DN.</td>
</tr>
<tr>
<td>-p &lt;LDAPadminPassword&gt;</td>
<td>LDAP Administrator password.</td>
</tr>
<tr>
<td>-f &lt;exportfilename&gt;.ldif</td>
<td>Specifies the name of the input file. This file must be in the LDIF format.</td>
</tr>
</tbody>
</table>

Comments
You can import the Security Management User Database to an LDAP server by first generating an LDIF file using fwm dbexport, and then using ldapmodify.

Before importing, prepare the LDAP directory as follows:
• Make sure the root branch is defined as an allowed branch on your LDAP server.
• Restart the LDAP server.
• Create the branch into which the users will be imported, either by using Create Tree Object in the Account Management Client or with the ldapmodify command:

```bash
ldapmodify -a -h <host> -p <port> -D <LDAPadminDN> -w -p <LDAPadminPassword>
dn: o=myOrg,c=US
objectclass: organization
o:myOrg
```

Example
Importing Users using ldapmodify:
1. Export the users using `fwm dbexport` using `hello1234` as the pre-shared secret.

```
fwm dbexport -l -f ./o_file.ldif -s "o=bigcorp,c=uk" -k hello1234
```

2. Create the "o=bigcorp,c=uk" branch.

3. Import the users:

```
ldapmodify -a -c -h <host> -p <port> -D bindDN -w bindPas -f ./o_file.ldif
```

4. Define an Account Unit with these parameters.
ldapsearch

Description
ldapsearch queries an LDAP directory and returns the results.

Usage
ldapsearch [options] filter [attributes] -d

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>options</td>
<td>See the options attributes below.</td>
</tr>
<tr>
<td>filter</td>
<td>RFC-1558 compliant LDAP search filter. For example, objectclass=fw1host.</td>
</tr>
<tr>
<td>attributes</td>
<td>The list of attributes to be retrieved. If no attributes are given, all attributes are retrieved.</td>
</tr>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
</tbody>
</table>

The following are the attributes for options:
- -A - Retrieve attribute names only (without values).
- -B - Do not suppress printing of non-ASCII values.
- -D bindDN - The DN to be used for binding to the LDAP server.
- -F separator - Print separator between attribute name and value instead of “=”.
- -h host - The LDAP server identified by IP address or resolvable name.
- -l timelimit - The server side time limit for search, in seconds.
- -p portnum - The port number. The default is standard LDAP port 389.
- -S attribute - Sort the results by the values of attribute.
- -s scope - One of the following: “base”, “one”, “sub”.
- -b - Base distinguished name (DN) for search.
- -t - Write values to files in /tmp. Each attribute-value pair is written to a separate file, named: /tmp/ldapsearch-<attribute>-<value>. For example, for the fw1color attribute, the file written is named /tmp/ldapsearch-fw1color-a00188.
- -T timeout - Client-side timeout (in milliseconds) for all operations.
- -u - Show “user friendly” entry names in the output. For example, show “cn=Babs Jensen, users, omi” instead of “cn=Babs Jensen, cn=users, cn=omi”.
- -w password - The password.
-Z - Encrypt using SSL.
-z sizelimit -Server-side size limit for search, in entries.

Example
ldapsearch -p 18185 -b cn=omi objectclass=fw1host objectclass

This means that the LDAP directory will be queried for fw1host objects using port number 18185 with DN common name “omi”. For each object found, the value of its objectclass attribute will be printed.
**log_export**

**Description**

`log_export` is a utility that allows you to transfer Log data to an external database. This utility behaves as a LEA client. LEA (Log Export API) enables Security Gateway Log data to be exported to third-party applications. `log_export` receives the Logs from the Security Management server via LEA so it can be run from any host that has a SIC connection with the Security Management server and is defined as an OPSEC host. To run `log_export`, you need a basic understanding and a working knowledge of:

- Oracle database administration
- LEA

**Usage**


**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f conf_file</td>
<td>The Configuration File from which <code>log_export</code> reads the Log file parameters. If <code>conf_file</code> is not specified, the default Configuration File <code>log_export.conf</code>, located in the current working directory.</td>
</tr>
<tr>
<td>-l &lt;lea_server_ip_address&gt;</td>
<td>The IP address of the LEA server.</td>
</tr>
<tr>
<td>-g log_file_name,log_file_name,...</td>
<td>A comma separated list of log file names from where the logs will be taken.</td>
</tr>
<tr>
<td>-t &lt;database_table_name&gt;</td>
<td>The name of the table in the database to which the logs will be added.</td>
</tr>
<tr>
<td>-p &lt;database_password&gt;</td>
<td>The database login password. If you do not want to specify the password in the Configuration File for security reasons, you can enter the password using the command line where it will not be saved anywhere.</td>
</tr>
<tr>
<td>-h</td>
<td>Display <code>log_export</code> usage.</td>
</tr>
<tr>
<td>-d</td>
<td>Display debugging information.</td>
</tr>
</tbody>
</table>
Further Info.  
For more information about LEA, see *Check Point LEA (Log Export API) Specification*

Comments  
Only Oracle database is currently supported.

Before you can run `log_export`, the Oracle client must be installed and configured. Make sure that:

- the `ORACLE_HOME` environment variable is set correctly.
- `$ORACLE_HOME/lib` is located in the `PATH` environment variable on the Windows platform or `LD_LIBRARY_PATH` on Solaris and Linux platforms.
- If `log_export` is running from another machine, you must install and configure at least Eventia Reporter.

**The `log_export` Configuration File**

`log_export` has a Configuration File. The Configuration File is a Check Point Set file and should be configured according to Set file conventions. The Configuration File contains the default parameters for `log_export`. `log_export` reads all parameters from the Configuration File that is specified in the command line.

**Modifying the Configuration File**

`log_export` parameters are defined in the Configuration File. To change the parameters, you can either modify the Configuration File or use the command line. Any parameter entered using the command line will override the parameters in the Configuration File.

Modify the Configuration File according to the following parameters:

- `db_connection_string` - The string that defines the Oracle database server. For example, the name of the server.
- `db_table_name` - The name of the table in the database to which the logs will be added.
- `create_db_table` - Following are the available options:
  - 1 - create a new table in the database
  - 0 - use the existing table.
  If there is an existing table, the logs will be added to that table. This requires that the existing table have the same format as the logs you are adding. If you enter 0 and there is no existing table, you will get an error message. The default is 1.
- `db_user_name` - The database login user name.
- `db_password` - The database login password.
- `log_server_ip_address` - The IP address of the LEA server.
• log_server_port - Port number of the LEA server. The default LEA port is 18184.

• log_file_name - A list of log file names from where the logs will be taken.

• log_fields - The name of the Log file as known by LEA.

• db_field_name - The Log field name as represented in the database table.

• db_field_type - The Log field type in the database table. This parameter can be one of the following:
  • STRING
  • NUMBER
  • DATE

• db_field_size - The size of the field in the database table. This parameter is required only if the db_field_type is either STRING or NUMBER.
Example

**Configuration File Example**

```plaintext
:db_table_name (fw_log)
:db_connection_string (database_service_name)
:db_user_name (scott)
:db_password (tiger)
:log_server_ip_address (127.0.0.1)
:log_server_port (18184)
:create_db_table (1)
:log_file_name (fw.log)
:log_fields (
  :{time
    :db_field_name (log_time)
    :db_field_type (DATE)
  }
  :{product
    :db_field_name (product)
    :db_field_type (STRING)
    :db_field_size (25)
  }
  :{i/f_name
    :db_field_name (interface)
    :db_field_type (STRING)
    :db_field_size (100)
  }
  :{orig
    :db_field_name (origin)
    :db_field_type (STRING)
    :db_field_size (16)
  }
  :{action
    :db_field_name (action)
    :db_field_type (STRING)
    :db_field_size (16)
  }
  :{service
    :db_field_name (service)
    :db_field_type (STRING)
    :db_field_size (40)
  }
)
queryDB_util

Description
queryDB_util enables searching the object database according to search parameters.

Usage
queryDB_util [-t <table_name>] [-o <object_name>] [-a]
[-mu <modified_by>] [-mh <modified_from>]
[-ma <modified_after>] [-mb <modified_before>] [-p|m|u|h|t|f]
[-f filename] [-h] [-q]

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t &lt;table_name&gt;</td>
<td>The name of the table.</td>
</tr>
<tr>
<td>-o &lt;object_name&gt;</td>
<td>The name of the object.</td>
</tr>
<tr>
<td>[-a]</td>
<td>All objects.</td>
</tr>
<tr>
<td>-mu &lt;modified_by&gt;</td>
<td>The name of the administrator who last modified the object.</td>
</tr>
<tr>
<td>-mh &lt;modified_from&gt;</td>
<td>The host from which the object was last modified.</td>
</tr>
<tr>
<td>-ma &lt;modified_after&gt;</td>
<td>The date after which the object was modified &lt;[hh:mm:ss][ddmmmyyyy]&gt;. Either or both options may be used. Omitting hh:mm:ss defaults to today at midnight, omitting ddmmmyyyy defaults to today's date on the client.</td>
</tr>
<tr>
<td>-mb &lt;modified_before&gt;</td>
<td>The date before which the object was modified &lt;[hh:mm:ss][ddmmmyyyy]&gt;. Either or both options may be used. Omitting hh:mm:ss defaults to today at midnight, omitting ddmmmyyyy defaults to today's date on the client.</td>
</tr>
<tr>
<td>-plmluhlhtlf</td>
<td>Short print options:</td>
</tr>
<tr>
<td></td>
<td>• c -creation details</td>
</tr>
<tr>
<td></td>
<td>• m -last_modification details</td>
</tr>
<tr>
<td></td>
<td>• u - administrator name</td>
</tr>
<tr>
<td></td>
<td>(create/modify)</td>
</tr>
<tr>
<td></td>
<td>• h -host name (create/modify)</td>
</tr>
<tr>
<td></td>
<td>• t -time (create/modify)</td>
</tr>
<tr>
<td></td>
<td>• f -field details</td>
</tr>
</tbody>
</table>
### Example

Print modification details of all objects modified by administrator “aa”

```plaintext
query> -a -mu Bob -pm
Object Name:my_object
Last Modified by:Bob
Last Modified from:london
Last Modification time:Mon Jun 19 11:44:27 2000

Object Name:internal_ca
Last Modified by:Bob
Last Modified from:london
Last Modification time:Tue Jun 20 11:32:58 2000

A total of 2 objects match the query.
```
**rs_db_tool**

**Description**

rs_db_tool is used to manage DAIP gateways in a DAIP database.

**Usage**

```
rs_db_tool [-d]  <-operation <add <-name object_name> <-ip module_ip> <-TTL Time-To-Live> >
rs_db_tool [-d]  <-operation fetch <-name object_name> >
rs_db_tool [-d]  <-operation <delete <-name object_name> >
rs_db_tool [-d]  <-operation <list> >
rs_db_tool [-d]  <-operation <sync> >
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>debug file</td>
</tr>
<tr>
<td>-operation add</td>
<td>Add entry to database.</td>
</tr>
<tr>
<td>&lt;-name object_name&gt;</td>
<td>Enter the name of the gateway object.</td>
</tr>
<tr>
<td>&lt;-ip module_ip&gt;</td>
<td>Enter the IP Address of the gateway</td>
</tr>
<tr>
<td>&lt;-TTL Time-To-Live&gt;</td>
<td>The relative time interval (in seconds) during which the entry is valid. A value of zero specifies “unlimited”.</td>
</tr>
<tr>
<td>-operation fetch</td>
<td>Get entry from database.</td>
</tr>
<tr>
<td>-operation delete</td>
<td>Delete entry from database.</td>
</tr>
<tr>
<td>-operation list</td>
<td>List all the database entries.</td>
</tr>
<tr>
<td>-operation sync</td>
<td>Synchronize the database.</td>
</tr>
</tbody>
</table>
### Description

This tool executes FW-1 SAM (Suspicious Activity Monitoring) actions according to information received through Standard input. This tool is for executing FW-1 SAM actions with the FW-1 User Defined alerts mechanism.

### Usage

```
```

### Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-o</code></td>
<td>Prints the input of this tool to the standard output (for pipes).</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Turns on verbose mode (of the <code>fw sam</code> command).</td>
</tr>
<tr>
<td><code>-s sam_server</code></td>
<td>The sam server to be contacted. Localhost is the default.</td>
</tr>
<tr>
<td><code>-t timeout</code></td>
<td>The time period, in seconds, for which the action will be enforced. The default is forever.</td>
</tr>
<tr>
<td><code>-f fw_host</code></td>
<td>Identifies the FireWalls to run the operation on. Default is “all FireWalls.”</td>
</tr>
<tr>
<td><code>-C</code></td>
<td>Cancels the specified operation.</td>
</tr>
<tr>
<td><code>-n</code></td>
<td>Notify every time a connection that matches the specified criteria passes the FireWall.</td>
</tr>
<tr>
<td><code>-i</code></td>
<td>Inhibit connections that match the specified criteria.</td>
</tr>
<tr>
<td><code>-I</code></td>
<td>Inhibit connections that match the specified criteria and close all existing connections that match the criteria.</td>
</tr>
<tr>
<td><code>-src</code></td>
<td>Match the source address of connections.</td>
</tr>
</tbody>
</table>
**Argument** | **Description**  
--- | ---  
-dst | Match the destination address of connections.  
-any | Match either the source or destination address of the connection.  
-srv | Match specific source, destination, protocol and service.
svr_webupload_config

This utility is used to configure the Eventia Reporter web upload script. For the complete upload procedure and additional information refer to the section “How to upload reports to a web server” in the Eventia Reporter Administration Guide.


Usage

svr_webupload_config [-i perl_int_loc]
[-p rep_dir_root]

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>Specifies the Perl interpreter location.</td>
</tr>
<tr>
<td>-p</td>
<td>Specifies the path for the reports virtual directory.</td>
</tr>
</tbody>
</table>
Chapter 2

VPN Commands

**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.

In This Chapter

- `vpn accel`  page 164
- `vpn compreset`  page 165
- `vpn compstat`  page 166
- `vpn crl_zap`  page 166
- `vpn crlview`  page 166
- `vpn debug`  page 167
- `vpn drv`  page 169
- `vpn export_p12`  page 169
- `vpn macutil`  page 170
- `vpn nssm_toplogy`  page 170
- `vpn overlap_encdom`  page 171
Perform operations on VPN accelerator cards (encryption only cards, not the full SecureXL cards) and VPNx. VPNx is a software module that takes advantage of multiple CPUs to accelerate VPN operations. 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autostart on/off</td>
<td>Automatically starts/stops the vpnx accelerator software</td>
</tr>
<tr>
<td>on/off</td>
<td>Enable/disable accelerator card or vpnx accelerator module</td>
</tr>
<tr>
<td>stat [-l]</td>
<td>Reports the status of the accelerator card in long format</td>
</tr>
</tbody>
</table>

**Example**

- `vpn accel -d vpnx stat`

**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
```
**Example**

```
vpn accel -d vpnx stat -l
```

**Output**

```
VPN-1: VPNx started
Number of initialization errors: 0
Number of processing errors: 0

Number of packets and bytes since last activation

<table>
<thead>
<tr>
<th></th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP decrypted</td>
<td>52</td>
<td>7072</td>
</tr>
<tr>
<td>ESP encrypted</td>
<td>52</td>
<td>7072</td>
</tr>
<tr>
<td>ESP total</td>
<td>104</td>
<td>14144</td>
</tr>
<tr>
<td>Total</td>
<td>104</td>
<td>14144</td>
</tr>
</tbody>
</table>

Average rates for the last 42.343 seconds

<table>
<thead>
<tr>
<th></th>
<th>Packets/sec</th>
<th>Kbit/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP decrypted</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>ESP encrypted</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>ESP total</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>0.00</td>
</tr>
</tbody>
</table>
```

---

**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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| -obj -cert | • -obj refers to the name of the CA network object  
| | • -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

---

Chapter 2  VPN Commands  167
## VPN Debug

**Syntax**

```plaintext
vpn debug on DEBUG_TOPIC=level |off timeon<SECONDS>|timeoff

vpn debug ikeon | ikeoff timeon|timeoff

vpn debug trunc
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Turns on high level VPN debugging.</td>
</tr>
<tr>
<td>on topic=level</td>
<td>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</td>
</tr>
<tr>
<td>off</td>
<td>Turns off all VPN debugging.</td>
</tr>
<tr>
<td>timeon/timeoff</td>
<td>Number of seconds to run the debug command</td>
</tr>
<tr>
<td>ikeon</td>
<td>Turns on IKE packet logging to: $FWDIR/log/IKE.elg</td>
</tr>
<tr>
<td>ikeoff</td>
<td>Turns off IKE logging</td>
</tr>
<tr>
<td>trunc</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Return Value**

0 = success, failure is some other value, typically -1 or 1.

**Example**

```plaintext
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.
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on/off</td>
<td>Starts/stops the VPN kernel</td>
</tr>
<tr>
<td>stat</td>
<td>Returns the status of the VPN kernel, whether the kernel is on or off</td>
</tr>
</tbody>
</table>

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_p12 -obj <network object> -cert <certificate object> -file <filename> -passwd <password>

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-obj</td>
<td>Name of the gateway network object</td>
</tr>
<tr>
<td>-cert</td>
<td>Name of the certificate</td>
</tr>
<tr>
<td>-file</td>
<td>What the file with the p12 should be called</td>
</tr>
<tr>
<td>-passwd</td>
<td>Password required to open the encrypted p12 file</td>
</tr>
</tbody>
</table>

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  
```bash
vpn macutil <username>
```

Example  
```bash
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  
```bash
vpn nssm_toplogy -url <"url"> -dn <"dn"> -name <"name"> -pass <"password"> [-action <bypass|drop>] [-print_xml]
```

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-url</td>
<td>URL of the Nokia NSSM server</td>
</tr>
<tr>
<td>-dn</td>
<td>Distinguished name of the NSSM server needed to establish an SSL connection</td>
</tr>
<tr>
<td>-name</td>
<td>Valid Login name for NSSM server</td>
</tr>
<tr>
<td>-pass</td>
<td>Valid password for NSSM server</td>
</tr>
<tr>
<td>-action</td>
<td>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</td>
</tr>
<tr>
<td>-print_xml</td>
<td>The topology is in XLM format. This flag writes that topology to a file in XLM format.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communities</td>
<td>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.</td>
</tr>
<tr>
<td>Traditional</td>
<td>Default flag. All pairs of objects with overlapping VPN domains are displayed.</td>
</tr>
</tbody>
</table>

**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
- 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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d</td>
<td>Debug flag</td>
</tr>
<tr>
<td>-dir</td>
<td>Output directory for file</td>
</tr>
<tr>
<td>-name</td>
<td>Nickname of site which appears in remote client</td>
</tr>
<tr>
<td>-profile</td>
<td>Name of the sofware profile for which the topology is created</td>
</tr>
<tr>
<td>-filename</td>
<td>Name of the output file</td>
</tr>
</tbody>
</table>
**vpn tu**

**Description**
Launch the TunnelUtil tool which is used to control VPN tunnels.

**Usage**
`vpn tu`

`vpn tunnelutil`

**Example**
`vpn tu`

**Output**

<table>
<thead>
<tr>
<th>Select Option</th>
<th>Table Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>List all IKE SAs</td>
</tr>
<tr>
<td>(2)</td>
<td>List all IPsec SAs</td>
</tr>
<tr>
<td>(3)</td>
<td>List all IKE SAs for a given peer</td>
</tr>
<tr>
<td>(4)</td>
<td>List all IPsec SAs for a given peer</td>
</tr>
<tr>
<td>(5)</td>
<td>Delete all IPsec SAs for a given peer</td>
</tr>
<tr>
<td>(6)</td>
<td>Delete all IPsec+IKE SAs for a given peer</td>
</tr>
<tr>
<td>(7)</td>
<td>Delete all IPsec SAs for ALL peers</td>
</tr>
<tr>
<td>(8)</td>
<td>Delete all IPsec+IKE SAs for ALL peers</td>
</tr>
<tr>
<td>(A)</td>
<td>Abort</td>
</tr>
</tbody>
</table>

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>`
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ver</strong></td>
<td>Displays the version name and version build number</td>
</tr>
<tr>
<td><strong>-k</strong></td>
<td>Displays the version name and build number and the kernel build number</td>
</tr>
<tr>
<td><strong>-f</strong></td>
<td>Prints the version number and build number to a text file.</td>
</tr>
</tbody>
</table>
Chapter 3

SmartView Monitor Commands

**RTM**

**Description**
This command and all its derivatives are used to execute SmartView Monitor operations.

In This Chapter

- `rtm debug` page 176
- `rtm drv` page 176
- `rtm monitor <module_name><interface_name>` or `rtm monitor <module_name>-filter` page 176
- `rtm monitor <module_name>-v<virtual_link_name>` page 180
- `rtm rtmd` page 181
- `rtm stat` page 181
- `rtm ver` page 181
- `rtmstart` page 182
- `rtmstop` page 182
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Start debug mode</td>
</tr>
<tr>
<td>off</td>
<td>Stop debug mode</td>
</tr>
<tr>
<td>OPSEC_DEBUG_LEVEL</td>
<td>Turn on OPSEC debug printouts</td>
</tr>
<tr>
<td>TDERROR_RTM_ALL</td>
<td>Turn on SmartView Monitor debug printouts</td>
</tr>
</tbody>
</table>

rtm drv

Description
Start, stop or check the status of the SmartView Monitor kernel driver.

Usage
rtm drv <on | off | stat>

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Start the SmartView Monitor kernel driver</td>
</tr>
<tr>
<td>off</td>
<td>Stop the SmartView Monitor kernel driver</td>
</tr>
<tr>
<td>stat</td>
<td>SmartView Monitor kernel driver status</td>
</tr>
</tbody>
</table>

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]
rtm monitor <module_name> <interface_name> or rtm monitor <module_name>-filter

or

rtm monitor <module_name>-filter["complex filter"] [options] -g<grouping>[entity-1...entity-n]

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>&lt;aggregate</td>
</tr>
<tr>
<td>-w</td>
<td>&lt;bandwidth</td>
</tr>
<tr>
<td>-t</td>
<td>&lt;wire</td>
</tr>
<tr>
<td>-i</td>
<td>&lt;number of seconds&gt;</td>
</tr>
<tr>
<td>@@</td>
<td>specifies subrule (for example, ‘rule@@subrule’)</td>
</tr>
<tr>
<td>default values</td>
<td>'-y bytes -a aggregate -w bandwidth -i2</td>
</tr>
<tr>
<td>grouping types</td>
<td>svc</td>
</tr>
<tr>
<td>module-name</td>
<td>The name of the SmartView Monitor module.</td>
</tr>
<tr>
<td>interface-name</td>
<td>The name of the monitored interface.</td>
</tr>
<tr>
<td>-d</td>
<td>Specifies one of the following monitor directions:</td>
</tr>
<tr>
<td></td>
<td>- inbound</td>
</tr>
<tr>
<td></td>
<td>- outbound</td>
</tr>
<tr>
<td></td>
<td>- eitherbound</td>
</tr>
<tr>
<td>inbound</td>
<td>Monitors the inbound direction.</td>
</tr>
<tr>
<td>outbound</td>
<td>Monitors the outbound direction.</td>
</tr>
<tr>
<td>eitherbound</td>
<td>Monitors both directions.</td>
</tr>
<tr>
<td>-y</td>
<td>Specifies one of the following measurement units:</td>
</tr>
<tr>
<td></td>
<td>- bytes</td>
</tr>
<tr>
<td></td>
<td>- pkts</td>
</tr>
<tr>
<td></td>
<td>- line</td>
</tr>
<tr>
<td>c</td>
<td>Indicates the number of new connections opened per second.</td>
</tr>
<tr>
<td>C</td>
<td>Average concurrent connections</td>
</tr>
</tbody>
</table>
```
rtm monitor <module_name><interface_name> or rtm monitor <module_name>-filter
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Aggregate - displays a specific type of connections as an aggregate. Individual - displays a specific type of connections as an individual. The default is eitherbound.</td>
</tr>
<tr>
<td>-g</td>
<td>Specifies one of the following grouping options for monitored traffic: svc src dst ip fgrule topsvc topsrc topdst topfwm topfgrule</td>
</tr>
<tr>
<td>svc</td>
<td>Monitors according to a service.</td>
</tr>
<tr>
<td>src</td>
<td>Monitors according to a network object (source only).</td>
</tr>
<tr>
<td>dst</td>
<td>Monitors according to a network object (destination only).</td>
</tr>
<tr>
<td>ip</td>
<td>Monitors according to a network object (source and destination).</td>
</tr>
<tr>
<td>fgrule</td>
<td>Monitors according to a QoS Policy rule.</td>
</tr>
<tr>
<td>topsvc</td>
<td>Monitors the traffic of the top 50 services.</td>
</tr>
<tr>
<td>topsrc</td>
<td>Monitors the traffic of the top 50 sources.</td>
</tr>
<tr>
<td>topdst</td>
<td>Monitors the traffic of the top 50 destinations.</td>
</tr>
</tbody>
</table>
rtm monitor <module_name><interface_name> or rtm monitor <module_name>-filter

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>topdst</td>
<td>Monitors traffic to and from the top 50 IP addresses (source of destination).</td>
</tr>
<tr>
<td>topfwn</td>
<td>Monitors according to the top 50 Firewall rules.</td>
</tr>
<tr>
<td>topfgrule</td>
<td>Monitors according to the top 50 QoS Policy rules.</td>
</tr>
<tr>
<td>-p</td>
<td>Specifies whether or not thousands will be separated by commas.</td>
</tr>
<tr>
<td>-filter</td>
<td>[&quot;&lt;complex filter&gt;&quot;] Only monitors traffic that matches the complex -filter boolean expression.</td>
</tr>
</tbody>
</table>

**Example**

The following command line displays monitoring data in bytes-per-sec for the top 50 services passed on any interface in both directions:

```bash
rtm monitor localhost -filter -g topsvc
```

The following command will display monitoring data in Concurrent-Connections for the top 50 sources passed on interface eth0, inbound (that is, not telnet of http).

```bash
rtm monitor localhost -filter "[and[[interface O [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.

```bash
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module-name</td>
<td>The name of the SmartView Monitor module.</td>
</tr>
<tr>
<td>-virtual-link-name</td>
<td>The name of the monitored Virtual Link.</td>
</tr>
<tr>
<td>-d</td>
<td>Specifies one of the following monitoring directions:</td>
</tr>
<tr>
<td></td>
<td>- a2b</td>
</tr>
<tr>
<td></td>
<td>- b2a</td>
</tr>
<tr>
<td></td>
<td>- a2b_b2a</td>
</tr>
<tr>
<td>a2b</td>
<td>Monitors End Point A to End Point B.</td>
</tr>
<tr>
<td>b2a</td>
<td>Monitors End Point B to End Point A.</td>
</tr>
<tr>
<td>a2b_b2a</td>
<td>Monitors both directions.</td>
</tr>
<tr>
<td>-y</td>
<td>Specifies one of the following measurement units. It is only required when the -w value is bandwidth.</td>
</tr>
<tr>
<td></td>
<td>- bytes</td>
</tr>
<tr>
<td></td>
<td>- pkts</td>
</tr>
<tr>
<td>-w</td>
<td>Specifies the displayed data type.</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Displays the effective bandwidth.</td>
</tr>
<tr>
<td>loss</td>
<td>Displays the difference between the transmission rate and the receiving rate.</td>
</tr>
<tr>
<td>rtt</td>
<td>Displays the time required to make the round trip between the two End Points.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Help</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose</td>
</tr>
<tr>
<td>vl</td>
<td>Current virtual links</td>
</tr>
<tr>
<td>view</td>
<td>Current views</td>
</tr>
</tbody>
</table>

rtm ver

Description
Display the SmartView Monitor version.

Usage
rtm ver [-k]
**rtmstart**

**Description**
Load the SmartView Monitor kernel module and starts the SmartView Monitor daemon.

**Usage**
rtmstart

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-k</td>
<td>-k</td>
<td>Displays the SmartView Monitor kernel version.</td>
</tr>
</tbody>
</table>

**rtmstop**

**Description**
Kill the SmartView Monitor daemon and unloads the SmartView Monitor kernel module.

**Usage**
rtmstop

182
Chapter 4

SecureClient Commands

**SCC**

**Description**

VPN commands executed on SecureClient are used to generate status information, stop and start services, or connect to defined sites using specific user profiles. Typically, a SecureClient does not need to open a command prompt and use these commands, but the site administrator may wish to include them in a script which is then transferred to remote users. In this way, the SecureClient CLI exposes SecureClient operations (such as Connect/Disconnect) to external third party applications via scripting.

The general format for SecureClient commands is:

```
C:\> scc <command> [optional arguments]
```

Some of the commands have keyboard shortcuts. Some of the commands require you to be in command line mode. Use the `setmode` command for switching to command line mode. Once in CLI mode, the system tray SecureClient icon is disabled.

**Return Value**

All the scc commands return 0 on success and (-1) on error. Any textual output goes to stdout on success (for example: `'scc numprofiles'`), and any error string goes to stderr.

In This Chapter

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>scc connect</td>
<td>184</td>
</tr>
<tr>
<td>scc connectnowait</td>
<td>184</td>
</tr>
<tr>
<td>scc disconnect</td>
<td>185</td>
</tr>
</tbody>
</table>
scc connect

    scc erasecreds   page 185
    scc listprofiles page 185
    scc numprofiles  page 186
    scc restartsc    page 186
    scc passcert     page 186
    scc setmode <mode> page 186
    scc setpolicy    page 187
    scc sp           page 187
    scc startsc      page 187
    scc status       page 187
    scc stopsc       page 187
    scc suppressdialogs page 188
    scc userpass     page 188
    scc ver          page 188

scc connect

Description
Connect to the site using the specified profile, and waits for the connection to be established. In other words, the OS does not put this command into the background and executes the next command in the queue.

Usage
connect [-p] <profilename>

Syntax

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>Displays connection progress</td>
</tr>
</tbody>
</table>

Comments
Shortcut: scc c
You must be in CLI mode to run this command.

scc connectnowait

Description
Connect asynchronously to the site using the specified profile. This means, the OS moves onto the next command in the queue and this command is run in the background.
**scc disconnect**

Description: Disconnect from the site using a specific profile.

Usage: `scc disconnect -p <profilename>`

Comments:
- Shortcut: `scc d`
- You must be in CLI mode to run this command.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>Displays disconnect progress</td>
</tr>
</tbody>
</table>

**scc erasescreds**

Description: Unset authorization credentials

Usage: `scc erasescreds`

Comments:
- Shortcut: `scc ep`
- You need to be in CLI mode to run this command.

**scc listprofiles**

Description: List all profiles

Usage: `scc listprofiles`

Comments:
- Shortcut: `scc lp`
- You must be in CLI mode to run this command.
**scc numprofiles**

**Description** Display the number of profiles.

**Usage**

```
scc numprofiles
```

**Comments**

Shortcut: `scc np`

You need to be in CLI mode to run this command.

**scc restartsc**

**Description** Restart SecureClient services.

**Usage**

```
scc restartsc
```

**Comments**

You need administrator privileges to run this command.

**scc passcert**

**Description** Set the user’s authentication credentials when authentication is performed using certificates.

**Usage**

```
scc passcert <certificate> <password>
```

**Comments**

Shortcut: `scc pc`

You need to be in CLI mode to run this command.

**scc setmode <mode>**

**Description** Switch the SecuRemote/SecureClient mode

**Usage**

```
scc setmode [-cli | -con]
```

**Syntax**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-cli</td>
<td>command line interface mode</td>
</tr>
<tr>
<td>-con</td>
<td>connect mode</td>
</tr>
</tbody>
</table>

**Comments**

You need administrator privileges to run this command.
### scc setpolicy

**Description**  
Enable or disable the current default security policy.

**Usage**  
scc setpolicy [on|off]

**Comments**  
Shortcut: `scc sp`  
You need administrator privileges to run this command.

### scc sp

**Description**  
Display the current default security policy.

**Usage**  
scc sp

**Comments**  
You need to be in CLI mode to run this command.

### scc startsc

**Description**  
Start SecureClient services.

**Usage**  
scc startsc

**Comments**  
You need administrator privileges to run this command.

### scc status

**Description**  
Display the connection status.

**Usage**  
scc status

**Comments**  
Shortcut: `scc s`

### scc stopsc

**Description**  
Stop SecureClient services.

**Usage**  
scc stopsc

**Comments**  
You need administrator privileges to run this command.
scc suppressdialogs

Description: Enable or suppress dialog popups. By default, suppressdialogs is off.
Usage: scc suppressdialogs [on|off]
Comments: When using suppressdialogs on, only popups requesting authentication credentials appear.
Shortcut: scc sd
You need to be in CLI mode to run this command.

scc userpass

Description: Sets the user’s authentication credentials -- username, and password.
Usage: scc userpass <username> <password>
Comments: Shortcut scc up
You need to be in CLI mode to run this command.

scc ver

Description: Displays the current SecureClient version.
Usage: scc ver
In This Chapter

cphaconf  page 190
cphaprob  page 191
cphastart  page 192
cphastop  page 193
**cphaconf**

**Description**  The cphaconf command configures ClusterXL.

*Warning* - 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_ccp option, as described below.

**Usage**

```bash
  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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cphaconf set_ccp</td>
<td>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. Note, the same value (either broadcast or multicast) should be set on all cluster members.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cphaprob -d &lt;device&gt; -t &lt;timeout(sec)&gt; -s &lt;ok</td>
<td>init</td>
</tr>
<tr>
<td>cphaprob -f &lt;file&gt; register</td>
<td>Register all the user defined critical devices listed in &lt;file&gt;.</td>
</tr>
<tr>
<td>cphaprob -d &lt;device&gt; [-p] unregister</td>
<td>Unregister a user defined &lt;device&gt; as a critical process. This means that this device is no longer considered critical.</td>
</tr>
<tr>
<td>cphaprob -a unregister</td>
<td>Unregister all the user defined &lt;device&gt;.</td>
</tr>
<tr>
<td>cphaprob -d &lt;device&gt; -s &lt;ok</td>
<td>init</td>
</tr>
<tr>
<td>cphaprob [-i[a]] [-e] list</td>
<td>View the list of critical devices on a cluster member, and of all the other machines in the cluster.</td>
</tr>
<tr>
<td>cphaprob state</td>
<td>View the status of a cluster member, and of all the other members of the cluster.</td>
</tr>
<tr>
<td>cphaprob [-a] if</td>
<td>View the state of the cluster member interfaces and the virtual cluster interfaces.</td>
</tr>
</tbody>
</table>
**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.
## Debugging SmartConsole Clients

You can run any SmartConsole client in debug mode and save the debug information in a text file.

**Usage:** `<client.exe> -d -o <Debug-Output-File-Name.txt>`

**Syntax:**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;client.exe&gt;</code></td>
<td>The SmartConsole client executable file. For example, <code>fwpolicy.exe</code></td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Enter the debug mode. If <code>-o</code> is omitted, debug information is saved into a file with the default name: <code>&lt;ROLE_STR&gt;_debug_output.txt</code>.</td>
</tr>
<tr>
<td><code>-o</code></td>
<td>This optional parameter, followed by a file name indicates in which text file debug information should be saved.</td>
</tr>
</tbody>
</table>
Chapter 7

CLI for Other Products

This guide documents Command Line Interface (CLI) commands for Check Point Products and features. The commands are documented by product. CLI commands for some products are documented in other guides:

CLI Commands in Other Guides

- For CoreXL commands, see the Firewall Administration Guide. http://supportcontent.checkpoint.com/documentation_download?ID=8738
- For Provider-1/SiteManager-1 commands, see the Provider-1/SiteManager-1 Administration Guide. http://supportcontent.checkpoint.com/documentation_download?ID=8741
- For QoS commands, see the QoS Administration Guide. http://supportcontent.checkpoint.com/documentation_download?ID=8742