Important Information

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

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=22917
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R76 home page (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 February 2013</td>
<td>Updated SKUs for Expansion Cards (&quot;Deciding if Multi-queue is needed&quot; on page 28)</td>
</tr>
<tr>
<td>7 February 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Performance Tuning R76 Administration Guide).
## Contents

### Important Information
- Performance Pack................................................................. 6
  - Introduction to Performance Pack........................................... 6
  - Supported Features.............................................................. 6
  - Preparing the Performance Pack............................................ 7
  - Installing during a SecurePlatform Gateway Installation............ 7
  - Installing on SecurePlatform Gateway.................................... 7
  - Installing on Installed SecurePlatform Gateway with HFA............ 7
  - Upgrading with SmartUpdate................................................ 8
  - Upgrading with the Command Line........................................ 8

### Command Line
- fwaccel ................................................................. 8
- fwaccel6 ............................................................... 9
- fwaccel stats and fwaccel6 stats.......................................... 11
- cpconfig .............................................................. 13
- sim affinity................................................................ 13
- proc entries................................................................ 14

### Performance Tuning and Measurement
- Setting the Maximum Concurrent Connections.......................... 14
- Increasing the Number of Concurrent Connections..................... 14
- SecureXL Templates ......................................................... 14
- SecureXL NAT templates .................................................. 15
- Delayed Notification .......................................................... 15
- Connection Templates ....................................................... 15
- Delayed Synchronization .................................................... 16
- Multi-Core Systems .......................................................... 16
- Performance Measurement.................................................... 17

### CoreXL Administration
- Supported Platforms and Unsupported Features........................ 18
- Default Configuration ......................................................... 19
- CoreXL for IPv6 ............................................................. 19
- Configuring IPv4 and IPv6 Firewall Instances............................ 19
- Performance Tuning ............................................................ 21
  - Processing Core Allocation.................................................. 21
  - Allocating Processing Cores............................................... 21
- Configuring CoreXL ......................................................... 24
- Command Line Reference..................................................... 24
  - Affinity Settings ................................................................ 24
  - fwaffinity.conf .................................................................. 24
  - fwaffinity_apply ............................................................... 25
  - fw ctl affinity .................................................................. 25
  - fw ctl multitk stat ............................................................ 27

### Multi-queue
- Introduction to Multi-Queue ................................................. 28
  - Multi-queue Requirements and Limitations............................. 28
  - Deciding if Multi-queue is needed........................................ 28
- Basic Multi-queue Configuration............................................. 31
- Multi-queue Administration.................................................... 32
- Glossary of Terms ............................................................... 33
- Advanced Multi-queue settings............................................. 33
  - The Sim Affinity Command.................................................. 35
  - Overriding rx queue and interface limitations....................... 35
Special Scenarios and Configurations ................................................................. 36
Troubleshooting ................................................................................................. 37
Index .................................................................................................................... 39
Chapter 1

Performance Pack

In This Chapter

Introduction to Performance Pack 6
Command Line 8
Performance Tuning and Measurement 14

Introduction to Performance Pack


Performance Pack is supported on:

- **SecurePlatform**
  - To install SecureXL, run: `sysconfig`
  - To enable SecureXL, run: `cpconfig`

- **Gaia**
  - On Gaia, Performance Pack is automatically installed when you run the *First Time Wizard*.
  - To enable SecureXL, run: `cpconfig`

**Supported Features**

These security functions are enhanced by Performance Pack:

- Access control
- Encryption
- NAT
- Accounting and logging
- Connection/session rate
- General security checks
- IPS features
- CIFs resources
- ClusterXL High Availability and Load Sharing
- TCP Sequence Verification
- Dynamic VPN
- Anti Spoofing verifications
- Passive streaming
- Drop rate
Preparing the Performance Pack

For optimal performance, configure the BIOS and NICs for Performance Pack.

BIOS Settings

- If your BIOS supports CPU clock setting, make sure that the BIOS is set to the actual CPU speed.
- If you are running Performance Pack on a machine with Intel Xeon CPUs, it is recommended to disable Hyper-Threading.

Network Interface Cards

- If you are using a motherboard with multiple PCI or PCI-X buses, make sure that each Network Interface Card is installed in a slot connected to a different bus.
- If you are using more than two Network Interface Cards in a system with only two 64bit/66Mhz PCI buses, make sure that the least-used cards are installed in slots connected to the same bus.

For an updated list of certified Network Interface Cards, see Certified Network Interfaces (http://www.checkpoint.com/services/techsupport/hcl/nic/).

Note - Performance Pack is automatically disabled on PPTP and PPPoE interfaces

Installing during a SecurePlatform Gateway Installation

During the Check Point SecurePlatform installation process, select the following products from the list of products to install:

- Security Gateway
- Performance Pack

Installing on SecurePlatform Gateway

Performance Pack can be installed on a Security Gateway on SecurePlatform.

1. Type sysconfig to enter the configuration menu.
2. Select Products Installation.
3. Follow the instructions until reaching the product selection screen.
5. Follow the instructions until finish.
6. Exit the configuration menu.
7. Reboot the gateway.

Installing on Installed SecurePlatform Gateway with HFA

If the SecurePlatform Security Gateway has a customer release, minor release, hotfix, or hotfix accumulator (HFA) installed on top of the main gateway version, use these steps.

1. Type sysconfig to enter the configuration menu.
2. Select Products Installation.
3. Follow the instructions until reaching the product selection screen.
5. Follow the instructions until finish.
6. Select Products Configuration.
7. Disable Check Point SecureXL.
8. Exit the configuration menu.
9. Reboot the gateway.
10. Upgrade the Performance Pack using SmartUpdate or from command line.

**Upgrading with SmartUpdate**

We recommend that you use SmartUpdate to upgrade Performance Pack.

**To upgrade with SmartUpdate:**
1. Select SmartUpdate from Check Point SmartConsole.
2. From the Packages menu, select Add > From File…
3. Select the HFA package and wait until the uploading finished.
4. From the Package Repository, select the Performance Pack package and drag it to the appropriate gateway.
5. Follow the instructions until finished.

**Upgrading with the Command Line**

If SmartUpdate is not an option, you can update with the command line.

1. Change to the directory where the upgrade file (.tgz) is located.
2. Run: `tar –xzvf <filename>`
3. Change to the CPppak directory.
4. Run: `tar –xzvf <sim filename>`
5. Run the sim executable.

**Command Line**

**fwaccel**

**Description**

Lets you dynamically enable or disable acceleration for IPv4 traffic while a Security Gateway is running. The fwaccel6 has the same functionality for IPv6 traffic. The default setting is determined by the setting configured with cpconfig. This setting reverts to the default after reboot.

Works with the IPv4 kernel.

**Syntax**

`fwaccel [on|off|stat|stats|conns|templates]`
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Starts acceleration</td>
</tr>
<tr>
<td>off</td>
<td>Stops acceleration</td>
</tr>
<tr>
<td>stat</td>
<td>Shows the acceleration device status and the status of the Connection Templates on the local Security Gateway.</td>
</tr>
<tr>
<td>stats</td>
<td>Shows acceleration statistics.</td>
</tr>
<tr>
<td>stats -s</td>
<td>Shows more summarized statistics.</td>
</tr>
<tr>
<td>stats -d</td>
<td>Shows dropped packet statistics.</td>
</tr>
<tr>
<td>conns</td>
<td>Shows all connections.</td>
</tr>
<tr>
<td>conns -s</td>
<td>Shows the number of connections defined in the accelerator.</td>
</tr>
<tr>
<td>conns -m max_entries</td>
<td>Limits the number of connections displayed by the conns command to the number entered in the variable <code>max_entries</code>.</td>
</tr>
<tr>
<td>templates</td>
<td>Shows all connection templates.</td>
</tr>
<tr>
<td>templates -m max_entries</td>
<td>Limits the number of templates displayed by the templates command to the number entered in the variable <code>max_entries</code>.</td>
</tr>
<tr>
<td>templates -s</td>
<td>Shows the number of templates currently defined in the accelerator.</td>
</tr>
</tbody>
</table>

**fwaccel6**

**Description**

Lets you enable or disable acceleration dynamically while a Security Gateway is running. The default setting is determined by the setting configured using `cpconfig`. This setting goes back to the default after reboot.

Works with the IPv6 kernel.

**Syntax**

```
fwaccel6 [on|off|stat|stats|conns|templates]
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Starts IPv6 acceleration.</td>
</tr>
<tr>
<td>off</td>
<td>Stops IPv6 acceleration.</td>
</tr>
<tr>
<td>stat</td>
<td>Shows the acceleration device status and the status of the Connection Templates on the local Security Gateway.</td>
</tr>
<tr>
<td>stats</td>
<td>Shows summary acceleration statistics.</td>
</tr>
<tr>
<td>stats -s</td>
<td>Shows detailed summarized statistics.</td>
</tr>
<tr>
<td>conns</td>
<td>Shows all IPv6 connections.</td>
</tr>
<tr>
<td>conns -s</td>
<td>Shows the number of IPv6 connections currently defined in the accelerator.</td>
</tr>
<tr>
<td>conns -m &lt;max_entries&gt;</td>
<td>Lowers the number of IPv6 connections shown by the conns command to the number entered in the variable max_entries.</td>
</tr>
<tr>
<td>templates</td>
<td>Shows all IPv6 connection templates.</td>
</tr>
<tr>
<td>templates -m max_entries</td>
<td>Lowers the number of templates shown by the templates command to the number entered in the variable max_entries.</td>
</tr>
<tr>
<td>templates -s</td>
<td>Shows the number of templates currently defined for the accelerator.</td>
</tr>
</tbody>
</table>

### Example: fwaccel6 stat

**Description**
The `fwaccel6 stat` command displays the acceleration device status and the status of the Connection Templates on the local Security Gateway.

**Example**
```
fwaccel6 stat -all
```

**Output**
```
Accelerator Status : on
Accept Templates : enabled
Accelerator Features : Accounting, NAT, Routing, HasClock, Templates, Synchronous, IdleDetection, Sequencing, TcpStateDetect, AutoExpire, DelayedNotif, TcpStateDetectV2, CPLS, WireMode, DropTemplates
```

### Example: fwaccel6 templates

**Description**
The `fwaccel6 templates` command displays all the connection templates

**Example**
```
fwaccel6 templates
```

**Output**
```
Source SPort Destination DPort PR Flags LCT DLY C2S i/f S2C i/f
---------------------------------------
-----
9999:b:0:0:0:0:0:10 * 9999:b:0:0:0:0:0:20 10000 17 ....... 15 0
Lan5/Lan1 Lan1/Lan5
```
Example: fwaccel6 stats

**Description**
The `fwaccel6 stats` command displays acceleration statistics.

**Example**
`fwaccel6 stats`

**Output**
```
Name    Value    Name    Value
-------------------------
conns created 11    conns deleted 7    
temporary conns 0    templates 1
nat conns 0    accel packets 2
accel bytes 96    F2F packets 39
ESP enc pkts 0    ESP enc err 0
ESP dec pkts 0    ESP dec err 0
ESP other err 0    espudp enc pkts 0
espudp enc err 0    espudp dec pkts 0
delay espudp dec err 0    espudp other err 0
AH enc pkts 0    AH enc err 0
AH dec pkts 0    AH dec err 0
AH other err 0    memory used 0
free memory 0    acct update interval 3600
current total conns 4    TCP violations 0
conns from templates 0    TCP conns 0
delayed TCP conns 0    non TCP conns 4
delayed nonTCP conns 0    F2F conns 3
F2F bytes 2848    crypt conn 0
enc bytes 0    dec bytes 0
partial conn 0    anticipated conn 0
dropped packets 0    dropped bytes 0
nat templates 0    port alloc templates 0
conn from nat tmpl 0    port alloc conn 0
port alloc f2f 0
```

**fwaccel stats and fwaccel6 stats**
The `fwaccel stats` and `fwaccel6 stats` commands show performance statistics. This information can help you understand traffic behavior and help investigate performance issues.

<table>
<thead>
<tr>
<th>Statistic parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>conns created</td>
<td>Number of created connections</td>
</tr>
<tr>
<td>conns deleted</td>
<td>Number of deleted connections</td>
</tr>
<tr>
<td>temporary conns</td>
<td>Number of temporary connections</td>
</tr>
<tr>
<td>templates</td>
<td>Number of templates currently handled</td>
</tr>
<tr>
<td>nat conns</td>
<td>Number of NAT connections</td>
</tr>
<tr>
<td>accel packets</td>
<td>Number of accelerated packets</td>
</tr>
<tr>
<td>accel bytes</td>
<td>Number of accelerated traffic bytes</td>
</tr>
<tr>
<td>F2F packets</td>
<td>Number of packets handled by the VPN kernel in slow-path</td>
</tr>
<tr>
<td>ESP enc pkts</td>
<td>Number of ESP encrypted packets</td>
</tr>
<tr>
<td>ESP enc err</td>
<td>Number of ESP encrypted errors</td>
</tr>
<tr>
<td>Statistic parameter</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ESP dec pkts</td>
<td>Number of ESP decrypted packets</td>
</tr>
<tr>
<td>ESP dec err</td>
<td>Number of ESP decrypted errors</td>
</tr>
<tr>
<td>ESP other err</td>
<td>Number of ESP other general errors</td>
</tr>
<tr>
<td>espudp enc pkts</td>
<td>Not in use</td>
</tr>
<tr>
<td>espudp enc err</td>
<td>Not in use</td>
</tr>
<tr>
<td>espudp dec pkts</td>
<td>Not in use</td>
</tr>
<tr>
<td>espudp dec err</td>
<td>Not in use</td>
</tr>
<tr>
<td>espudp other err</td>
<td>Not in use</td>
</tr>
<tr>
<td>AH enc pkts</td>
<td>Not in use</td>
</tr>
<tr>
<td>AH enc err</td>
<td>Not in use</td>
</tr>
<tr>
<td>AH dec pkts</td>
<td>Not in use</td>
</tr>
<tr>
<td>AH dec err</td>
<td>Not in use</td>
</tr>
<tr>
<td>AH other err</td>
<td>Not in use</td>
</tr>
<tr>
<td>memory used</td>
<td>Not in use</td>
</tr>
<tr>
<td>free memory</td>
<td>Not in use</td>
</tr>
<tr>
<td>acct update interval</td>
<td>Accounting update interval in seconds</td>
</tr>
<tr>
<td>current total conns</td>
<td>Number of connections currently handled</td>
</tr>
<tr>
<td>TCP violations</td>
<td>Number of packets which are in violation of the TCP state</td>
</tr>
<tr>
<td>conns from templates</td>
<td>Number of connections created from templates</td>
</tr>
<tr>
<td>TCP conns</td>
<td>Number of TCP connections currently handled</td>
</tr>
<tr>
<td>delayed TCP conns</td>
<td>Number of delayed TCP connections currently handled</td>
</tr>
<tr>
<td>non TCP conns</td>
<td>Number of non TCP connections currently handled</td>
</tr>
<tr>
<td>delayed nonTCP conns</td>
<td>Number of delayed non TCP connections currently handled</td>
</tr>
<tr>
<td>F2F conns</td>
<td>Number of connections currently handled by the VPN kernel in slow-path</td>
</tr>
<tr>
<td>F2F bytes</td>
<td>Number of traffic bytes handled by the VPN kernel in slow-path</td>
</tr>
<tr>
<td>crypt conns</td>
<td>Number of encrypted connections currently handled</td>
</tr>
<tr>
<td>enc bytes</td>
<td>Number of encrypted traffic bytes</td>
</tr>
<tr>
<td>dec bytes</td>
<td>Number of decrypted traffic bytes</td>
</tr>
<tr>
<td>Statistic parameter</td>
<td>Explanation</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>partial conns</td>
<td>Number of partial connections currently handled</td>
</tr>
<tr>
<td>anticipated conns</td>
<td>Number of anticipated connections currently handled</td>
</tr>
<tr>
<td>dropped packets</td>
<td>Number of dropped packets</td>
</tr>
<tr>
<td>dropped bytes</td>
<td>Number of dropped traffic bytes</td>
</tr>
<tr>
<td>nat templates</td>
<td>Not in use</td>
</tr>
<tr>
<td>port alloc templates</td>
<td>Not in use</td>
</tr>
<tr>
<td>conns from nat tmpl</td>
<td>Not in use</td>
</tr>
<tr>
<td>port alloc conns</td>
<td>Not in use</td>
</tr>
<tr>
<td>port alloc f2f</td>
<td>Not in use</td>
</tr>
<tr>
<td>PXL templates</td>
<td>Number of PXL templates</td>
</tr>
<tr>
<td>PXL conns</td>
<td>Number of PXL connections</td>
</tr>
<tr>
<td>PXL packets</td>
<td>Number of PXL packets</td>
</tr>
<tr>
<td>PXL bytes</td>
<td>Number of PXL traffic bytes</td>
</tr>
<tr>
<td>PXL async packets</td>
<td>Number of PXL packets handled asynchronously</td>
</tr>
</tbody>
</table>

**cpconfig**

Check Point products are configured using the **cpconfig** utility. This utility shows the configuration options of the installed configuration and products. You can use **cpconfig** to enable or disable Performance Pack. When you select an acceleration setting, the setting remains configured until you change it.

For an alternative method to enable or disable acceleration, see **fwaccel** (on page 8).

Run: **cpconfig**

A menu shows **Enable/Disable Check Point SecureXL**.

**sim affinity**

**Description**  
The **sim affinity** utility controls various Performance Pack driver features and applies only for SecurePlatform.

Affinity is a general term for binding Network Interface Card (NIC) interrupts to processors. By default, SecurePlatform does not set Affinity to the NIC interrupts. Therefore, each NIC is handled by all processors. For optimal network performance, make sure each NIC is individually bound to one processor.

**Syntax**

```
sim affinity [-a|-s|-l]
```
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td><strong>Automatic Mode</strong> — (default) Affinity is determined by analysis of the load on each NIC. If a NIC is not activated, Affinity is not set. NIC load is analyzed every 60 seconds.</td>
</tr>
<tr>
<td>-s</td>
<td><strong>Manual Mode</strong> — Configure Affinity settings for each interface: the processor numbers (separated by space) that handle this interface, or all. In Manual Mode, periodic NIC analysis is disabled.</td>
</tr>
<tr>
<td>-l</td>
<td>See Affinity settings.</td>
</tr>
</tbody>
</table>

### proc entries

**Description**
Performance Pack supports proc entries. These read-only entries show data about Performance Pack. The proc entries are in `/proc/ppk`.

**Syntax**
`cat /proc/ppk/[conf|ifs|statistics|drop statistics]`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf</td>
<td>Shows Performance Pack configuration.</td>
</tr>
<tr>
<td>ifs</td>
<td>Shows the interfaces to which Performance Pack is attached.</td>
</tr>
<tr>
<td>statistics</td>
<td>Shows general Performance Pack statistics.</td>
</tr>
<tr>
<td>drop statistics</td>
<td>Shows Performance Pack dropped packet statistics.</td>
</tr>
</tbody>
</table>

### Performance Tuning and Measurement

#### Setting the Maximum Concurrent Connections

To set the desired number of maximum concurrent connections:

1. Open SmartDashboard's Gateway Object Properties window.
2. Open the Capacity Optimization tab. Make sure that Calculate connections hash table size and memory pool is set to Automatically.
3. Set the desired amount of concurrent connections in the Maximum Concurrent Connections field.

#### Increasing the Number of Concurrent Connections

You can increase the actual number of concurrent connections by reducing the timeout of TCP and UDP sessions:

- TCP end timeout determines the amount of time a TCP connection will stay in the Firewall connection table after a TCP session has ended.
- UDP virtual session timeout determines the amount of time a UDP connection will stay in the Firewall connection table after the last UDP packet was seen by the gateway.

By reducing the above values, the capacity of actual TCP and UDP connections is increased.

#### SecureXL Templates

Verify that templates are not disabled using the `fwaccel stat` command.

For further information regarding SecureXL Templates, see sk32578 (http://supportcontent.checkpoint.com/solutions?id=sk32578).
SecureXL NAT templates

Using SecureXL Templates for NAT traffic lets you achieve a high session rate for NAT traffic. SecureXL NAT Templates are supported in cluster in High Availability, VRRP, and Load Sharing modes.

For more, see: sk71200 (http://supportcontent.checkpoint.com/solutions?id=sk71200).

Delayed Notification

In the ClusterXL configuration, the Delayed Notification feature is disabled by default. Enabling this feature improves performance (at the cost of connections' redundancy, which can be tuned using delayed notifications expiration timeout).

The **fwaccel stats** command indicates the number of delayed connections.

The **fwaccel templates** command indicates the delayed time for each template under the DLY entry.

Connection Templates

Connection templates are generated from active connections according to the policy rules. The connection template feature accelerates the speed at which a connection is established by matching a new connection to a set of attributes. When a new connection matches the template, connections are established without performing a rule match and therefore are accelerated. Connection templates are generated from active connections according to policy rules. Currently, connection template acceleration is performed only on connections with the same destination port.

Examples:

- A connection from 10.0.0.1/2000 to 11.0.0.1/80 — established through Firewall and then accelerated.
- A connection from 10.0.0.1/2001 to 11.0.0.1/80 — fully accelerated (including connection establishment).
- A connection from 10.0.0.1/8000 to 11.0.0.1/80 — fully accelerated (including connection establishment).

HTTP GET requests to specific server will be accelerated since the connection has the same source IP address.

Restrictions

In general, Connections Templates will be created only for plain UDP or TCP connections. The following restrictions apply for Connection Template generation:

Global restrictions:

- SYN Defender — Connection Templates for TCP connections will not be created
- VPN connections
- Complex connections (H323, FTP, SQL)
- NetQuotas
- ISN Spoofing

If the Rule Base contains a rule regarding one of the following components, the Connection Templates will be disabled for connections matching this rule, and for all of the following rules:

- Security Server connections.
- Time objects in the rules.
- Dynamic Objects and/or Domain Objects.
- Services of type "other" with a match expression.
- User/Client/Session Authentication actions.
- Services of type RPC/DCERPC/DCOM.
When installing a policy containing restricted rules, you will receive console messages indicating that Connection Templates will not be created due to the rules that have been defined. The warnings should be used as a recommendation that will assist you to fine-tune your policy in order to optimize performance.

**Testing**

To verify that connection templates are enabled, use the `fwaccel stat` command. To verify that connection templates are generated, use `fwaccel templates`. This should be done while traffic is running, in order to obtain a list of currently defined templates.

**Delayed Synchronization**

The synchronization mechanism guarantees High Availability. In a cluster configuration, if one cluster member fails, the other recognizes the connection failure and takes over, so the user does not experience any connectivity issue. However, there is an overhead per synchronized operation, which can occasionally cause a system slow-down when there are short sessions.

Delayed synchronization is a mechanism based upon the duration of the connection, with the duration itself used to determine whether or not to perform synchronization. A time range can be defined per service. The time range indicates that connections terminated before a specified expiration time will not be synchronized. As a result, synchronized traffic is reduced and overall performance increases. Delayed Synchronization is performed only for connections matching a connection template.

**Note** - Delayed synchronization is disabled if the log or account are enabled.

Currently, delayed synchronization is allowed only for services of type HTTP or None. In order to configure delayed synchronization, proceed as follows:

1. In SmartDashboard, right click on the **Service** tab.
2. Either edit an existing service or click **New** and select **TCP**. The TCP service properties window is shown.
3. After defining TCP parameters, click **Advanced** in the TCP service properties window. The Advanced TCP Service Properties window is shown.
4. Select the **HTTP** or **None** protocol from the Protocol Type list.
5. Check **Start synchronizing**.
6. Define the duration value **Seconds after connection initiation**. The duration value is specified in seconds.

**Multi-Core Systems**

Running Performance Pack on multi-core systems may require more advanced configurations to account for core affinity and IRQ behavior. For more information, see sk33250 (http://supportcontent.checkpoint.com/solutions?id=sk33250).
Performance Measurement

There are various ways to monitor and measure the performance of a Security Gateway.

TCP State and Benchmarking

Certain testing applications (SmartBits or Chariot) generate invalid TCP sequences. The Security Gateway's TCP state check detects these faulty sequences, and drops the packets. As a result, the benchmark fails. Since these TCP sequences are invalid, they may affect overall Firewall performance.

To disable this type of TCP state check, perform the following operations in SmartDashboard:

1. In the IPS tab, select Protections > By Protocol > Network Security > TCP > Sequence Verifier.
2. Select the profile assigned to your gateway and click Edit.
3. In the Action field, select Inactive.
4. Click OK to close the Protections Settings window.
5. Click OK to close the Protections Details window.
6. Click Install Policy to apply the changes.

Non-accelerated traffic analysis

Use the fwaccel stats command to verify the amount of non-accelerated traffic compared to accelerated traffic.

Use the sim dbg + f2f command to understand the possible reasons for the non-accelerated traffic.

Performance Troubleshooting

Additional CLI commands, such as ethtool, are available to monitor the performance of the gateway. For a list of these commands and explanation of their usage, see sk33781 (http://supportcontent.checkpoint.com/solutions?id=sk33781).
Chapter 2

CoreXL Administration

In This Chapter

- Supported Platforms and Unsupported Features
- Default Configuration
- CoreXL for IPv6
- Configuring IPv4 and IPv6 Firewall Instances
- Performance Tuning
- Configuring CoreXL
- Command Line Reference

CoreXL is a performance-enhancing technology for Security Gateways on multi-core processing platforms. CoreXL enhances Security Gateway performance by enabling the processing cores to concurrently perform multiple tasks.

CoreXL provides almost linear scalability of performance, according to the number of processing cores on a single machine. The increase in performance is achieved without requiring any changes to management or network topology.

CoreXL joins ClusterXL Load Sharing and SecureXL as part of Check Point's fully complementary family of traffic acceleration technologies.

In a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.

Supported Platforms and Unsupported Features

CoreXL is supported:

- SecurePlatform
- Gaia
- IPSO
- Crossbeam platforms

Unsupported Features:

CoreXL does not support Check Point Suite with these features:

- Check Point QoS (Quality of Service)
- Route-based VPN
- IPv6 on IPSO
- Overlapping NAT

To enable a non-supported feature in the Check Point Suite, disable CoreXL using cpconfig and reboot the gateway (see Configuring CoreXL (on page 24)).
Default Configuration

When you enable CoreXL, the number of kernel instances is based on the total number of CPU cores.

<table>
<thead>
<tr>
<th>Number of Cores</th>
<th>Number of Kernel Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>More than 12</td>
<td>Number of cores, minus 2</td>
</tr>
</tbody>
</table>

The default affinity setting for all interfaces is automatic when Performance Pack is installed. See Processing Core Allocation (on page 21). Traffic from all interfaces is directed to the core running the Secure Network Distributor (SND).

CoreXL for IPv6

R76 supports multiple cores for IPv6 traffic. For each firewall kernel instance that works with IPv4 traffic, there is a corresponding firewall kernel instance that also works with IPv6 traffic. Both instances run on the same core.

To check the status of CoreXL on your Security Gateway, run:
fw6 ctl multik stat.

The fw6 ctl multik stat (multi-kernel statistics) command shows IPv6 information for each kernel instance. The state and processing core number of each instance is displayed, along with:

- The number of connections currently running.
- The peak number of concurrent connections the instance has used since its inception.

Configuring IPv4 and IPv6 Firewall Instances

After IPv6 support is enabled on the gateway, you can configure the gateway's processing cores to run different combinations of IPv4 and IPv6 firewall kernel instances.

- The number of IPv4 instances range from a minimum of two to a number equal to the maximum number of cores on the gateway.
  By default, the number of IPv6 firewall instances is set to two.
- The number of IPv6 instances range from a minimum of two to a number equal to the number of IPv4 instances.
  The number of IPv6 instances cannot exceed the number of IPv4 instances.

To configure the number of IPv6 firewall instances:
1. From a command line on the gateway, run: cpconfig.
   The configuration menu shows.
2. Enter option 8: Configure Check Point CoreXL.
Configure Check Point CoreXL...

CoreXL is currently enabled with 3 firewall instances and 2 IPv6 firewall instances.

(1) Change the number of firewall instances
(2) Change the number of IPv6 firewall instances
(3) Disable Check Point CoreXL
(4) Exit

The Configuring Check Point CoreXL menu shows how many IPv4 and IPv6 firewall instances are running on the processing cores.

3. Enter option 2: Change the number of IPv6 firewall instances.
   The menu shows how many cores are available on the gateway.

4. Enter the total number of IPv6 firewall instances to run.
   You can only select a number from within the range shown.

5. Reboot the gateway.

Example:
A gateway that has four cores and is running three IPv4 instances of the firewall kernel and two IPv6 instances of the firewall kernel can be represented like this:

<table>
<thead>
<tr>
<th>Core</th>
<th>Firewall instances</th>
<th>IPv6 Firewall instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU 1</td>
<td>fw4_2</td>
<td></td>
</tr>
<tr>
<td>CPU 2</td>
<td>fw4_1</td>
<td>fw6_1</td>
</tr>
<tr>
<td>CPU 3</td>
<td>fw4_0</td>
<td>fw6_0</td>
</tr>
</tbody>
</table>

- 3 instances of IPv4   2 instances of IPv6

- The minimum allowed number of IPv4 instances is two and the maximum four
- The minimum allowed number of IPv6 instances is two and the maximum is three

To increase the number of IPv6 instances to four, you must first increase the number of IPv4 firewall instances to the maximum of four:

How many firewall instances would you like to enable (2 to 4)[3] ? 4

CoreXL was enabled successfully with 4 firewall instances.
Important: This change will take effect after reboot.

The gateway now looks like this:

<table>
<thead>
<tr>
<th>Core</th>
<th>Firewall instances</th>
<th>IPv6 Firewall instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU 0</td>
<td>fw4_3</td>
<td></td>
</tr>
<tr>
<td>CPU 1</td>
<td>fw4_2</td>
<td></td>
</tr>
<tr>
<td>CPU 2</td>
<td>fw4_1</td>
<td>fw6_1</td>
</tr>
<tr>
<td>CPU 3</td>
<td>fw4_0</td>
<td>fw6_0</td>
</tr>
</tbody>
</table>

- 4 instances of IPv4   2 instances of IPv6

Increase the number of IPv6 instances to four:
How many IPv6 firewall instances would you like to enable (2 to 4)?

CoreXL was enabled successfully with 3 IPv6 firewall instances.
Important: This change will take effect after reboot.

The gateway now looks like this:

<table>
<thead>
<tr>
<th>Core</th>
<th>Firewall instances</th>
<th>IPv6 Firewall instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU 0</td>
<td>fw4_3</td>
<td>fw6_3</td>
</tr>
<tr>
<td>CPU 1</td>
<td>fw4_2</td>
<td>fw6_2</td>
</tr>
<tr>
<td>CPU 2</td>
<td>fw4_1</td>
<td>fw6_1</td>
</tr>
<tr>
<td>CPU 3</td>
<td>fw4_0</td>
<td>fw6_0</td>
</tr>
<tr>
<td></td>
<td>4 instances of IPv4</td>
<td>4 instances of IPv6</td>
</tr>
</tbody>
</table>

Performance Tuning

The following sections are relevant only for SecurePlatform.

**Processing Core Allocation**

The CoreXL software architecture includes the Secure Network Distributor (SND). The SND is responsible for:

- Processing incoming traffic from the network interfaces
- Securely accelerating authorized packets (if Performance Pack is running)
- Distributing non-accelerated packets among kernel instances.

Traffic entering network interface cards (NICs) is directed to a processing core running the SND. The association of a particular interface with a processing core is called the interface's *affinity* with that core. This affinity causes the interface’s traffic to be directed to that core and the SND to run on that core. Setting a kernel instance or a process to run on a particular core is called the instance’s or process's *affinity* with that core.

The default affinity setting for all interfaces is Automatic. Automatic affinity means that if Performance Pack is running, the affinity for each interface is automatically reset every 60 seconds, and balanced between available cores. If Performance Pack is not running, the default affinities of all interfaces are with one available core. In both cases, any processing core running a kernel instance, or defined as the affinity for another process, is considered unavailable and will not be set as the affinity for any interface.

In some cases, which are discussed in the following sections, it may be advisable to change the distribution of kernel instances, the SND, and other processes, among the processing cores. This is done by changing the affinities of different NICs (interfaces) and/or processes. However, to ensure CoreXL’s efficiency, all interface traffic must be directed to cores not running kernel instances. Therefore, if you change affinities of interfaces or other processes, you will need to accordingly set the number of kernel instances and ensure that the instances run on other processing cores.

Under normal circumstances, it is not recommended for the SND and an instance to share a core. However, it is necessary for the SND and an instance to share a core when using a machine with exactly two cores.

**Allocating Processing Cores**

In certain cases, it may be advisable to change the distribution of kernel instances, the SND, and other processes, among the processing cores. This section discusses these cases.

Before planning core allocation, make sure you have read the Processing Core Allocation (on page 21).
Adding Processing Cores to the Hardware

Increasing the number of processing cores on the hardware platform does not automatically increase the number of kernel instances. If the number of kernel instances is not increased, CoreXL does not utilize some of the processing cores. After upgrading the hardware, increase the number of kernel instances using `cpconfig`.

Reinstalling the gateway will change the number of kernel instances if you have upgraded the hardware to an increased number of processing cores, or if the number of processing cores stays the same but the number of kernel instances was previously manually changed from the default. Use `cpconfig` to reconfigure the number of kernel instances.

In a clustered deployment, changing the number of kernel instances (such as by reinstalling CoreXL) should be treated as a version upgrade. Follow the instructions in the *R76 Installation and Upgrade Guide* ([http://supportcontent.checkpoint.com/solutions?id=sk91140](http://supportcontent.checkpoint.com/solutions?id=sk91140)), in the "Upgrading ClusterXL Deployments" chapter, and perform either a Minimal Effort Upgrade (using network downtime) or a Zero Downtime Upgrade (no downtime, but active connections may be lost), substituting the instance number change for the version upgrade in the procedure. A Full Connectivity Upgrade cannot be performed when changing the number of kernel instances in a clustered environment.

Allocating an Additional Core to the SND

In some cases, the default configuration of instances and the SND will not be optimal. If the SND is slowing the traffic, and your platform contains enough cores that you can afford to reduce the number of kernel instances, you may want to allocate an additional core to the SND. This is likely to occur especially if much of the traffic is of the type accelerated by Performance Pack; in a ClusterXL Load Sharing deployment; or if IPS features are disabled. In any of these cases, the task load of the SND may be disproportionate to that of the kernel instances.

**To check if the SND is slowing down the traffic:**

1. Identify the processing core to which the interfaces are directing traffic using `fw ctl affinity -l -r`.
2. Under heavy traffic conditions, run the `top` command on the CoreXL gateway and check the values for the different cores under the 'idle' column.

It is recommended to allocate an additional core to the SND only if all of the following conditions are met:

- Your platform has at least eight processing cores.
- The 'idle' value for the core currently running the SND is in the 0%-5% range.
- The sum of the 'idle' values for the cores running kernel instances is significantly higher than 100%.

If any of the above conditions are not met, the default configuration of one processing core allocated to the SND is sufficient, and no further configuration is necessary.

Allocating an additional processing core to the SND requires performing the following two stages in the order that they appear:

1. Reduce the number of kernel instances using `cpconfig`.
2. Set interface affinities to the remaining cores, as detailed below.
3. Reboot to implement the new configuration.

**Setting Interface Affinities**

Check which cores are running the kernel instances. See also Allocating Processing Cores (on page 21). Allocate the remaining cores to the SND by setting interface affinities to the cores. The correct method of defining interface affinities depends on whether or not Performance Pack is running, as described in the following sections.

- **When Performance Pack is Running**
  - If Performance Pack is running, interface affinities are handled by using Performance Pack's `sim affinity` command.
  - The default `sim affinity` setting is Automatic. In Performance Pack's Automatic mode, interface affinities are automatically distributed among cores that are not running kernel instances and that are not set as the affinity for any other process.
  - In most cases, you do not need to change the `sim affinity` setting.
- **Setting Interface Affinities when Performance Pack is not Running**
If Performance Pack is not running, interface affinities are loaded at boot from a configuration text file called `fwaffinity.conf`, located under: `$FWDIR/conf`. In the text file, lines beginning with the letter `i` define interface affinities.

If Performance Pack is running, interface affinities are defined by `sim affinity` settings, and lines beginning with `i` in `fwaffinity.conf` are ignored.

If you are allocating only one processing core to the SND, it is best to have that core selected automatically by leaving the default interface affinity set to automatic, and having no explicit core affinities for any interfaces. To do this, make sure `fwaffinity.conf` contains the following line:

```
  i default auto
```

In addition, make sure that `fwaffinity.conf` contains no other lines beginning with `i`, so that no explicit interface affinities are defined. All interface traffic will be directed to the remaining core.

If you are allocating two processing cores to the SND, you need to explicitly set interface affinities to the two remaining cores. If you have multiple interfaces, you need to decide which interfaces to set for each of the two cores. Try to achieve a balance of expected traffic between the cores (you can later check the balance by using the `top` command).

**To explicitly set interface affinities, when Performance Pack is not running:**

1. Set the affinity for each interface by editing `fwaffinity.conf`. The file should contain one line beginning with `i` for each interface. Each of these lines should follow the following syntax:

   ```
   i <interfacename> <cpuid>
   ```

   where `<interfacename>` is the interface name, and `<cpuid>` is the number of the processing core to be set as the affinity of that interface.

   For example, if you want the traffic from `eth0` and `eth1` to go to core #0, and the traffic from `eth2` to go to core #1, create the following lines in `fwaffinity.conf`:

   ```
   i eth0 0
   i eth1 0
   i eth2 1
   ```

   Alternatively, you can choose to explicitly define interface affinities for only one processing core, and define the other core as the default affinity for the remaining interfaces, by using the word `default` for `<interfacename>`.

   In the case described in the previous example, the lines in `fwaffinity.conf` would be:

   ```
   i eth2 1
   i default 0
   ```

2. Run `$FWDIR/scripts/fwaffinity_apply` for the `fwaffinity.conf` settings to take effect.

   The affinity of virtual interfaces can be set using their physical interface(s).

**Allocating a Core for Heavy Logging**

If the gateway is performing heavy logging, it may be advisable to allocate a processing core to the `fwd` daemon, which performs the logging. Like adding a core for the SND, this too will reduce the number of cores available for kernel instances.

**To allocate a processing core to the `fwd` daemon, you need to do two things:**

1. Reduce the number of kernel instances using `cpconfig`.
2. Set the `fwd` daemon affinity, as detailed below.

**Setting the `fwd` Daemon Affinity**

Check which processing cores are running the kernel instances and which cores are handling interface traffic using `fw ctl affinity -l -r`. Allocate the remaining core to the `fwd` daemon by setting the `fwd` daemon affinity to that core.

**Note** - Avoiding the processing core or cores that are running the SND is important only if these cores are explicitly defined as affinities of interfaces. If interface affinities are set to Automatic, any core that is not running a kernel instance can be used for the `fwd` daemon, and interface traffic will be automatically diverted to other cores.
Affinities for Check Point daemons (such as the fwd daemon), if set, are loaded at boot from the fwaffinity.conf configuration text file located at: $FWDIR/conf. Edit the file by adding the following line:

```
n fwd <cpuid>
```

where `<cpuid>` is the number of the processing core to be set as the affinity of the fwd daemon. For example, to set core #2 as the affinity of the fwd daemon, add to the file:

```
n fwd 2
```

Reboot for the fwaffinity.conf settings to take effect.

### Configuring CoreXL

**To enable/disable CoreXL:**
1. Log in to the Security Gateway.
2. Run cpconfig
3. Select Configure Check Point CoreXL.
4. Enable or disable CoreXL.
5. Reboot the Security Gateway.

**To configure the number of instances:**
1. Run cpconfig
2. Select Configure Check Point CoreXL.
3. If CoreXL is enabled, enter the number of firewall instances.
   - If CoreXL is disabled, enable CoreXL and then set the number of firewall instances.

Reboot the gateway.

**Note** - In a clustered deployment, changing the number of kernel instances should be treated as a version upgrade.

### Command Line Reference

**Affinity Settings**

Affinity settings controlled by the fwaffinity_apply script file, which executes automatically at boot. When you make a change to affinity settings, the settings will not take effect until you either reboot or manually execute the fwaffinity_apply script.

fwaffinity_apply executes affinity definitions according to the information in the fwaffinity.conf text file. To change affinity settings, edit the text file.

**Note** - If Performance Pack is running, interface affinities are only defined by Performance Pack’s sim affinity command. The fwaffinity.conf interface affinity settings are ignored.

**fwaffinity.conf**

fwaffinity.conf is located in the $FWDIR/conf directory.

**Syntax**

Each line in the text file uses the same format: `<type> <id> <cpu>`
<table>
<thead>
<tr>
<th>Data</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;type&gt;</td>
<td>i</td>
<td>interface</td>
</tr>
<tr>
<td></td>
<td>n</td>
<td>Check Point daemon</td>
</tr>
<tr>
<td></td>
<td>k</td>
<td>kernel instance</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td></td>
<td>interface name if &lt;type&gt; = i</td>
</tr>
<tr>
<td></td>
<td></td>
<td>daemon name if &lt;type&gt; = n</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance number if &lt;type&gt; = k</td>
</tr>
<tr>
<td>default</td>
<td></td>
<td>interfaces that are not specified in another line</td>
</tr>
<tr>
<td>&lt;cpuid&gt;</td>
<td>&lt;number&gt;</td>
<td>number(s) of processing core(s) to be set as the affinity</td>
</tr>
<tr>
<td>all</td>
<td></td>
<td>all processing cores are available to the interface traffic, daemon or kernel instance</td>
</tr>
<tr>
<td>ignore</td>
<td></td>
<td>no specified affinity (useful for excluding an interface from a default setting)</td>
</tr>
<tr>
<td>auto</td>
<td></td>
<td>Automatic mode See also Processing Core Allocation (on page 21).</td>
</tr>
</tbody>
</table>

Note - Interfaces that share an IRQ cannot have different cores as their affinities, including when one interface is included in the default affinity setting. Either set both interfaces to the same affinity, or use ignore for one of them. To view the IRQs of all interfaces, run: fw ctl affinity -l -v -a.

fwaffinty_apply

fwaffinty_apply is located in the $FWDIR/scripts directory. Use the following syntax to execute the command: $FWDIR/scripts/fwaffinty_apply <option>

where <option> is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-q</td>
<td>Quiet mode - print only error messages.</td>
</tr>
<tr>
<td>-t &lt;type&gt;</td>
<td>Only apply affinity for the specified type.</td>
</tr>
<tr>
<td>-f</td>
<td>Sets interface affinity even if automatic affinity is active.</td>
</tr>
</tbody>
</table>

fw ctl affinity

The fw ctl affinity command controls affinity settings. However, fw ctl affinity settings will not persist through a restart of the Security Gateway.

To set affinities, execute fw ctl affinity -s.
To list existing affinities, execute fw ctl affinity -l.

fw ctrl affinity -s

Use this command to set affinities.
fw ctl affinity -s settings are not persistent through a restart of the Security Gateway. If you want the settings to be persistent, either use sim affinity or edit the fwa/finity.conf configuration file.

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.

**Syntax**

fw ctl affinity -s <proc_selection> <cpuid>

<proc_selection> is one of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</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>

<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**

Use this command to list existing affinities. For an explanation of kernel, daemon and interface affinities, see CoreXL Administration (on page 18).

**Syntax**

fw ctl affinity -l [<proc_selection>] [<listtype>]

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>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p &lt;pid&gt;</td>
<td>Displays the affinity of a particular process, where &lt;pid&gt; is the process ID#.</td>
</tr>
<tr>
<td>-n &lt;cpdname&gt;</td>
<td>Displays the affinity of 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>Displays the affinity of a kernel instance, where &lt;instance&gt; is the instance’s number.</td>
</tr>
</tbody>
</table>
**Parameter** | **Description**
---|---
-\(i\) <interfacename> | Displays the affinity of an interface, where <interfacename> is the interface name (for example: eth0).

If <listtype> is omitted, `fw ctl affinity -l` lists items with specific affinities, and their affinities. Otherwise, <listtype> is one or more of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>All: includes items without specific affinities.</td>
</tr>
<tr>
<td>-r</td>
<td>Reverse: lists each processing core and the items that have it as their affinity.</td>
</tr>
<tr>
<td>-v</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 multik stat**

The `fw ctl multik stat` and `fw6ctl multik stat` (multi-kernel statistics) commands show information 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.
Chapter 3
Multi-queue

In This Chapter
- Introduction to Multi-Queue
- Basic Multi-queue Configuration
- Multi-queue Administration
- Glossary of Terms
- Advanced Multi-queue settings
- Special Scenarios and Configurations
- Troubleshooting

Introduction to Multi-Queue

By default, each network interface has one traffic queue that is handled by one CPU at a time. Because the SND (Secure Network distributor, the SecureXL and CoreXL dispatcher) runs on the CPUs handling the traffic queues, you cannot use more CPUs for acceleration than the number of interfaces handling traffic.

Multi-queue lets you configure more than one traffic queue for each network interface. This means more than one CPU can be used for acceleration.

Multi-queue Requirements and Limitations

- Multi-queue is not supported on single core computers.
- Network interfaces must support multi-queue
- The number of queues is limited by the number of CPUs and the type of interface driver:

<table>
<thead>
<tr>
<th>Driver type</th>
<th>Maximum recommended number of rx queues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Igb</td>
<td>4</td>
</tr>
<tr>
<td>Ixgbe</td>
<td>16</td>
</tr>
</tbody>
</table>

Deciding if Multi-queue is needed

This section will help you decide if you can benefit from configuring Multi-queue. We recommend that you do these steps before configuring Multi-queue:

- Make sure that SecureXL is enabled
- Examine the CPU roles allocation
- Examine CPU Utilization
- Decide if more CPUs can be allocated to the SND
- Make sure that network interfaces support Multi-queue

Making sure that SecureXL is enabled

1. On the Security Gateway, run: `fwaccel stat`
2. Examine the Accelerator Status value:
[Expert@gw-30123d:0]# fwaccel stat
Accelerator Status : on
Accept Templates   : enabled
Drop Templates     : disabled
NAT Templates      : disabled by user

Accelerator Features : Accounting, NAT, Cryptography, Routing,
HasClock, Templates, Synchronous,
IdleDetection,
Sequencing, TcpStateDetect, AutoExpire,
DelayedNotif, TcpStateDetectV2, CPLS, WireMode,
DropTemplates, NatTemplates, Streaming,
MultiFW, AntiSpoofing, DoS Defender,

ViolationStats,
Nac, AsychronicNotif, ERDOS

Cryptography Features : Tunnel, UDPEncapsulation, MD5, SHA1, NULL,
3DES, DES, CAST, CAST-40, AES-128, AES-256,
ESP, LinkSelection, DynamicVPN, NatTraversal,
EncRouting, AES-XCBC, SHA256

SecureXL is enabled if the value of this field is: on.

Note -
- Multi-queue is relevant only if SecureXL is enabled.
- Drop templates still show in the command output even though support for drop templates stopped in R75.40

Examining the CPU roles allocation

To see the CPU roles allocation, run: fw ctl affinity -l

This command shows the CPU affinity of the interfaces, which assigns SND CPUs. It also shows the CoreXL firewall instances CPU affinity. For example, if you run the command on a security gateway:

[Expert@gw-30123d:0]# fw ctl affinity -l
Mgmt: CPU 0
eth1-05: CPU 0
eth1-06: CPU 1
fw 0: CPU 5
fw 1: CPU 4
fw 2: CPU 3
fw_3: CPU 2

In this example:
- The SND is running on CPU 0 and CPU1
- CoreXL firewall instances are running on CPUs 2-5

If you run the command on a VSX gateway:

[Expert@gw-30123d:0]# fw ctl affinity -l
Mgmt: CPU 0
eth1-05: CPU 0
eth1-06: CPU 1
VS 0 fwk: CPU 2 3 4 5
VS_1 fwk: CPU 2 3 4 5

In this example:
- The SND is running on CPU 0-1
- CoreXL firewall instances (part of fwk processes) of all the Virtual Systems are running on CPUs 2-5.
Examining CPU Utilization

2. Press 1 to toggle the SMP view.

This shows the usage and idle percentage for each CPU. For example:

```
top - 10:02:33 up 28 days, 1:10. 1 user, load average: 1.22, 1.38, 1.40
Tasks: 137 total, 3 running, 134 sleeping, 0 stopped, 0 zombie

Cpu0 : 2.0%us, 0.0%sy, 0.0%ni, 32.7%id, 5.9%ws, 0.0%hi, 59.4%si, 0.0%st
Cpu1 : 0.0%us, 1.0%sy, 0.0%ni, 35.2%id, 0.0%ws, 0.0%hi, 63.8%si, 0.0%st
Cpu2 : 2.0%us, 2.0%sy, 0.0%ni, 65.5%id, 0.0%ws, 4.0%hi, 26.5%si, 0.0%st
Cpu3 : 1.0%us, 2.0%sy, 0.0%ni, 74.5%id, 0.0%ws, 0.0%hi, 22.5%si, 0.0%st
Cpu4 : 5.0%us, 1.0%sy, 0.0%ni, 72.6%id, 0.0%ws, 0.0%hi, 31.5%si, 0.0%st
```

In this example:
- SND CPUs (CPU0 and CPU1) are approximately 30% idle
- CoreXL firewall instances CPUs are approximately 70% idle

Deciding if more CPU can be allocated to the SND

If you have more network interfaces handling traffic than CPUs assigned to the SND (as shown in the output of the `fw ctl affinity -l` command), you can allocate more CPUs for SND.

For example, if you have the following network interfaces:
- eth1-04 – connected to an internal network
- eth1-05 – connected to an internal network
- eth1-06 – connected to the DMZ
- eth1-07 – connected to the external network

And running `fw ctl affinity -l` shows this IRQ affinity:

```
[Expert@gw-30123d:0]# fw ctl affinity -l
Mgmt: CPU 0
eth1-04: CPU 1
eth1-05: CPU 0
eth1-06: CPU 1
eth1-07: CPU 0
fw_0: CPU 5
fw_1: CPU 4
fw_2: CPU 3
fw_3: CPU 2
```

You can change the interfaces IRQ affinity to use more CPUs for the SNDs.

Making sure that the network interfaces support Multi-queue

Multi-queue is supported only on network cards that use `igb` (1Gb) or `ixgbe` (10Gb) drivers. Before upgrading these drivers, make sure that the latest version supports multi-queue.
### Multi-queue

**Gateway type** | **Expansion Card Model**
--- | ---
Security Appliance | Multi-queue is supported on these expansion cards for 4000, 12000, and 21000 appliances:
- CPAC-ACC-4-1C
- CPAC-ACC-4-1F
- CPAC-ACC-8-1C
- CPAC-ACC-2-10F
- CPAC-ACC-4-10F

IP appliance | The XMC 1Gb card is supported on:
- IP1280
- IP2450

Open server | Network cards that use `igb` (1Gb) or `ixgbe` (10Gb) drivers

- To view which driver an interface is using, run: `ethtool -i <interface name>`.
- When installing a new interface that uses the `igb` or `ixgbe` driver, run: `cpmq reconfigure` and reboot.

**Recommendation**

We recommend configuring multi-queue when:

- CPU load for SND is high (idle is less than 20%) and
- CPU load for CoreXL firewall instances are low (idle is greater than 50%)
- You cannot assign more CPUs to the SND by changing interface IRQ affinity

### Basic Multi-queue Configuration

The `cpmq` utility is used to view or change the current multi-queue configuration.

#### Configuring Multi-queue

The `cpmq set` command lets you to configure Multi-queue on supported interfaces.

To configure Multi-queue:

- On the gateway, run: `cpmq set`

  This command:
  - Shows all supported interfaces that are active
  - Lets you change the Multi-queue configuration for each interface.

  Network interfaces that are down do not show.

  **Note** -
  - Multi-queue lets you configure a maximum of two interfaces
  - You must reboot the gateway after changing the multi-queue configuration.

#### Querying the current Multi-queue configuration

The `cpmq get` command shows the Multi-queue status of supported interfaces.

To see the Multi-queue configuration:

Run: `cpmq get [-a]`

The `-a` option shows the Multi-queue configuration for all supported interfaces (both active and inactive).

For example:
[Expert@gw-30123d:0]# cpmq get -a

Active igb interfaces:
eth1-05 [On]
eth1-06 [Off]
eth1-01 [Off]
eth1-03 [Off]
eth1-04 [On]

Non active igb interfaces:
eth1-02 [Off]

Status messages

<table>
<thead>
<tr>
<th>Status</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>Multi-queue is enabled on the interface</td>
</tr>
<tr>
<td>Off</td>
<td>Multi-queue is disabled on the interface</td>
</tr>
<tr>
<td>Pending On</td>
<td>Multi-queue currently disabled. Multi-queue will be enabled on this interface only after rebooting the gateway</td>
</tr>
<tr>
<td>Pending Off</td>
<td>Multi-queue enabled. Multi-queue will be disabled on this interface only after rebooting the gateway</td>
</tr>
</tbody>
</table>

In this example:

- Two interfaces are up with Multi-queue enabled (eth1-05, eth1-04)
- Three interfaces are up with Multi-queue disabled (eth1-06, eth1-01, eth1-03)
- One interface that supports Multi-queue is down (eth1-02)

Running the command without the `-a` option shows the active interfaces only.

**Multi-queue Administration**

There are two main roles for CPUs applicable to SecureXL and CoreXL:

- SecureXL and CoreXL dispatcher CPU (the SND - Secure Network Distributor)
  You can manually configure this using the `sim affinity -s` command.
- CoreXL firewall instance CPU
  You can manually configure this using the `fw ctl affinity` command.

For best performance, the same CPU should not work in both roles. During installation, a default CPU role configuration is set. For example, on a twelve core computer, the two CPUs with the lowest CPU ID are set as SNDs and the ten CPUs with the highest CPU IDs are set as CoreXL firewall instances.

Without Multi–queue, the number of CPUs allocated to the SND is limited by the number of network interfaces handling the traffic. Since each interface has one traffic queue, each queue can be handled by only one CPU at a time. This means that the SND can use only one CPU at a time per network interface.

When most of the traffic is accelerated, the CPU load for SND can be very high while the CPU load for CoreXL firewall instances can be very low. This is an inefficient utilization of CPU capacity.

Multi–queue lets you configure more than one traffic queue for each supported network interface, so that more than one SND CPU can handle the traffic of a single network interface at a time. This balances the load efficiently between SND CPUs and CoreXL firewall instances CPUs.
Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SND</td>
<td>Secure Network Distributor. A CPU that runs SecureXL and CoreXL</td>
</tr>
<tr>
<td>rx queue</td>
<td>Receive packet queue</td>
</tr>
<tr>
<td>tx queue</td>
<td>Transmit packet queue</td>
</tr>
<tr>
<td>IRQ affinity</td>
<td>Binding an IRQ to a specific CPU or CPUs.</td>
</tr>
</tbody>
</table>

Advanced Multi-queue settings

Advanced multi-queue settings include:

- Controlling the number of queues
- IRQ Affinity
- Viewing CPU Utilization

Controlling the number of queues

Controlling the number of queues depends on the driver type:

<table>
<thead>
<tr>
<th>Driver type</th>
<th>Queues</th>
</tr>
</thead>
<tbody>
<tr>
<td>igxbe</td>
<td>When configuring Multi-queue for an ixgbe interface, an RxTx queue is created per CPU. You can control the number of active rx queues (all tx queues are active).</td>
</tr>
<tr>
<td>igb</td>
<td>When configuring Multi-queue for an igb interface, the number of tx and rx queues is calculated by the number of active rx queues.</td>
</tr>
</tbody>
</table>

- By default on a Security Gateway, the number of active rx queues is calculated by:
  \[ \text{active rx queues} = \text{Number of CPUs} - \text{number of CoreXL firewall instances} \]
- By default on a VSX gateway, the number of active rx queues is calculated by:
  \[ \text{active rx queues} = \text{the lowest CPU ID that an fwk process is assigned to} \]

To control the number of active rx queues:

Run: `cpmq set rx_num <igb/ixgbe> <number of active rx queues>`

This command overrides the default value.

To view the number of active rx queues:

Run: `cpmq get rx_num <igb/ixgbe>`

To return to the recommended number of rx queues:

On a Security Gateway, the number of active queues changes automatically when you change the number of CoreXL firewall instances (using `cpconfig`). This number of active queues does not change if you configure the number of rx queues manually.

Run: `cpmq set rx_num <igb/ixgbe> default`

IRQ Affinity

The IRQ affinity of the queues is set automatically when the operating system boots, as shown (rx_num set to 3):

- `rxtx-0 -> CPU 0`
- `rxtx-1 -> CPU 1`
- `rxtx-2 -> CPU 2`
and so on. This is also true in cases where rx and tx queues are assigned with a separated IRQ:

- rx-0 -> CPU 0
- tx-0 -> CPU 0
- rx-1 -> CPU 1
- tx-1 -> CPU 1

and so on.

- You cannot use the `sim affinity` or the `fw ctl affinity` commands to change and query the IRQ affinity for Multi-queue interfaces.
- You can reset the affinity of Multi-queue IRQs by running: `cpmq set affinity`
- You can view the affinity of Multi-queue IRQs by running: `cpmq get -v`

⚠️ **Important** - Do not change the IRQ affinity of queues manually. Changing the IRQ affinity of the queues manually can affect performance.

### Viewing CPU Utilization

1. Find the CPUs assigned to multi-queue IRQs by running: `cpmq get -v`. For example:

   ```bash
   [Expert@gw-30123d:0]# cpmq get -v
   
   Active igb interfaces:
   eth1-05 [On]
   eth1-06 [Off]
   eth1-01 [Off]
   eth1-03 [Off]
   eth1-04 [On]
   
   multi-queue affinity for igb interfaces:
   
   eth1-05:
   
   - irq | cpu | queue
   --|---|---
   178 | 0 | TxRx-0
   186 | 1 | TxRx-1
   
   eth1-04:
   
   - irq | cpu | queue
   --|---|---
   123 | 0 | TxRx-0
   131 | 1 | TxRx-1
   
   In this example:
   - Multi-queue is enabled on two igb interfaces (eth1-05 and eth1-04)
   - The number of active rx queues is configured to 2 (for igb, the number of queues is calculated by the number of active rx queues).
   - The IRQs for both interfaces are assigned to CPUs 0-1.

2. Run: `top`
3. Press 1 to toggle to the SMP view.

In the above example, CPU utilization of Multi-queue CPUs is approximately 50%, as CPU0 and CPU1 are handling the queues (as shown in step 1).

**The Sim Affinity Command**

<table>
<thead>
<tr>
<th>Description</th>
<th>A process used to automatically assign or cancel interface - CPU affinity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>sim affinity</code></td>
</tr>
<tr>
<td>Parameters</td>
<td>Parameter</td>
</tr>
<tr>
<td></td>
<td><code>-l</code></td>
</tr>
<tr>
<td></td>
<td><code>-s</code></td>
</tr>
<tr>
<td></td>
<td><code>-a</code></td>
</tr>
<tr>
<td></td>
<td><code>-h</code></td>
</tr>
<tr>
<td>Example</td>
<td><code>sim affinity -a</code></td>
</tr>
<tr>
<td>Comments</td>
<td>By default, the <code>sim affinity -a</code> process runs, assigning affinity to both multi-queue and none multi-queue enabled interfaces. Before R76, multi-queue interfaces were ignored by the <code>sim affinity</code> command. If the <code>sim affinity -a</code> process has been canceled by running <code>sim affinity -s</code>, use <code>cpqm set affinity</code> to reset the affinity of the multi-queue interface.</td>
</tr>
</tbody>
</table>

**Overriding rx queue and interface limitations**

- The number of rx queues is limited by the number of CPUs and the type of interface driver:

<table>
<thead>
<tr>
<th>Driver type</th>
<th>Maximum recommended number of rx queues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Igb</td>
<td>4</td>
</tr>
<tr>
<td>Ixgbe</td>
<td>16</td>
</tr>
</tbody>
</table>

To add more rx queues, run:

```
cpmq rx_num <igb/ixgbe> <number of active rx queues> -f
```

- Due to IRQ limitations, you can configure a maximum of two interfaces with Multi-queue. To add more interfaces, run:

```
cpmq set -f
```
Special Scenarios and Configurations

- **In Security Gateway mode**: Changing the number of CoreXL firewall instances when Multi-queue is enabled on some or all interfaces
  For best performance, the default number of active rx queues is calculated by:
  $$\text{Number of active rx queues} = \text{number of CPUs} - \text{number of CoreXL firewall instances}$$
  This configuration is set automatically when configuring Multi-queue. When changing the number of instances, the number of active rx queues will change automatically if it was not set manually.

- **In VSX mode**: changing the number of CPUs that the \texttt{fwk} processes are assigned to
  The default number of active rx queues is calculated by:
  $$\text{Number of active rx queues} = \text{the lowest CPU ID that an fwk process is assigned to}$$
  For example:

  ```
  [Expert@gw-30123d:0]# fw ctl affinity -l
  Mgmt: CPU 0
  eth1-05: CPU 0
  eth1-06: CPU 1
  VS_0 fwk: CPU 2 3 4 5
  VS_1 fwk: CPU 2 3 4 5
  ```

  In this example
  - The number of active rx queues is set to 2.
  - This configuration is set automatically when configuring Multi-queue.
  - It will not automatically update when changing the affinity of the Virtual Systems. When changing the affinity of the Virtual Systems, make sure to follow the instructions in Advanced Multi-queue settings (on page 33).

The effects of changing the status of a multi-queue enabled interface

- **Changing the status to DOWN**
  The Multi-queue configuration is saved when you change the status of an interface to down.
  Since the number of interfaces with Multi-queue enabled is limited to two, you may need to disable Multi-queue on an interface after changing its status to down to enable Multi-queue on other interfaces.
  The \texttt{cpmq set} command lets you disable Multi-queue on non-active interfaces.

- **Changing the status to UP**
  You must reset the IRQ affinity for multi-queue interfaces if
  - Multi-queue was enabled on the interface
  - You changed the status of the interface to down
  - You rebooted the gateway
  - You changed the interface status to up.
  This problem does not occur if you are running automatic sim affinity \texttt{(sim affinity -a)}. Automatic sim affinity runs by default, and has to be manually canceled using the \texttt{sim affinity -s} command.
  To set the static affinity of Multi-queue interfaces again, run: \texttt{cpmq set affinity}.

Adding a network interface

- When adding a network interface card to a gateway that uses \texttt{igb} or \texttt{ixgbe} drivers, the Multi-queue configuration can change due to interface indexing. If you add a network interface card to a gateway that uses \texttt{igb} or \texttt{ixgbe} drivers make sure to run Multi-queue configuration again or run: \texttt{cpmq reconfigure}.
  - If a reconfiguration change is required, you will be prompted to reboot the computer.

Changing the affinity of CoreXL firewall instances

- For best performance, we recommend that you do not assign both SND and a CoreXL firewall instance to the same CPU.
When changing the affinity of the CoreXL firewall instances to a CPU assigned with one of the Multi-queue queues, we recommend that you reconfigure the number of active rx queues following this rule:

Active rx queues = the lowest CPU number that a CoreXL firewall instance is assigned to

You can configure the number of active rx queues by running:

cpmq set rx_num <igb/ixgbe> <value/default>

Troubleshooting

- After reboot, the wrong interfaces are configured for Multi-queue
  This can happen after changing the physical interfaces on the gateway. To solve this issue:
  a) Run: `cpmq reconfigure`
  b) Reboot.
  Or configure Multi-queue again.

- When changing the status of interfaces, all the interface IRQs are assigned to CPU 0 or to all of the CPUs
  This can happen when an interface status is changed to UP after the automatic affinity procedure runs (the affinity procedure runs automatically during boot).
  To solve this issue, run: `cpmq set affinity`
  This problem does not occur if you are running automatic sim affinity (`sim affinity -s`). Automatic sim affinity runs by default, and has to be manually canceled using the `sim affinity -s` command.

- In VSX mode, an fwk process runs on the same CPU as some of the interface queues
  This can happen when the affinity of the Virtual System was manually changed but Multi-queue was not reconfigured accordingly.
  To solve this issue, configure the number of active rx queues manually or run: `cpmq reconfigure` and reboot.

- In Security Gateway mode – after changing the number of instances Multi-queue is disabled on all interfaces
  When changing the number of CoreXL firewall instances, the number of active rx queues automatically changes according to this rule (if not configured manually):
  Active rx queues = Number of CPUs – number of CoreXL firewall instances
  If the number of instances is equal to the number of CPUs, or if the difference between the number of CPUs and the number of CoreXL firewall instances is 1, multi-queue will be disabled. To solve this issue, configure the number of active rx queues manually by running:
  `cpmq set rx_num <igb/ixgbe> <value>`