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=16203
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the home page at the Check Point Support Center (http://supportcontent.checkpoint.com/solutions?id=sk76540).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>04 March 2013</td>
<td>SIM affinity update (&quot;sim affinity&quot; on page 12)</td>
</tr>
<tr>
<td>15 July 2012</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 Pack R75.40VS Administration Guide).
Contents

Important Information .................................................................................................................. 3
Introduction to Performance Pack ................................................................................................. 5
  Supported Features ................................................................................................................... 5
  Preparing the Performance Pack R70 Machine ..................................................................... 6
    BIOS Settings ....................................................................................................................... 6
    Network Interface Cards ..................................................................................................... 6
  Installing during a New Security Gateway Installation ......................................................... 6
  Installing on an Already Installed Security Gateway ......................................................... 6
  Installing on an Already Installed Security Gateway with HFA .......................................... 7
  Upgrading with SmartUpdate ............................................................................................... 7
  Upgrading with the Command Line ..................................................................................... 7
Command Line ............................................................................................................................. 7
  fwaccel .................................................................................................................................. 7
  fwaccel6 ............................................................................................................................... 8
    Example: fwaccel6 stat ....................................................................................................... 8
    Example: fwaccel6 templates ............................................................................................ 9
    Example: fwaccel6 stats ..................................................................................................... 9
  fwaccel stats ......................................................................................................................... 9
  cpconfig ............................................................................................................................... 12
  sim affinity ............................................................................................................................ 12
  proc entries ......................................................................................................................... 12
Performance Tuning and Measurement ......................................................................................... 13
  Setting the Maximum Concurrent Connections ............................................................... 13
  Increasing the Number of Concurrent Connections ............................................................ 13
  SecureXL Templates ............................................................................................................. 13
  Delayed Notification ............................................................................................................ 13
  Connection Templates .......................................................................................................... 13
    Restrictions ........................................................................................................................ 14
    Testing ................................................................................................................................. 14
  Delayed Synchronization ..................................................................................................... 14
  Multi-Core Systems ............................................................................................................. 15
  Performance Measurement .................................................................................................... 16
    TCP State and Benchmarking ............................................................................................ 16
    Non-accelerated traffic analysis ........................................................................................ 16
    Performance Troubleshooting ........................................................................................... 16
Index ............................................................................................................................................ 17
Chapter 1

Introduction to Performance Pack

In This Chapter

- Supported Features 5
- Preparing the Performance Pack R70 Machine 6
- Installing during a New Security Gateway Installation 6
- Installing on an Already Installed Security Gateway 6
- Installing on an Already Installed Security Gateway with HFA 7
- Upgrading with SmartUpdate 7
- Upgrading with the Command Line 7


Performance Pack is supported on SecurePlatform.

Supported security functions include:

- 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

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 R70 Machine

For optimal performance, appropriate configuration settings are recommended for the following:

• BIOS Settings
• Network Interface Cards

**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 New Security 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 an Already Installed Security Gateway

1. Type `sysconfig` to enter the configuration menu.
2. Select **Products Installation**.
3. Follow the instructions until reaching the product selection screen.
4. Select **Performance Pack**.
5. Follow the instructions until finish.
6. Exit the configuration menu.
7. Reboot the gateway.
Installing on an Already Installed Security Gateway with HFA

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. For more information, see Upgrading Performance Pack.

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

The fwaccel utility allows you to enable or disable acceleration dynamically while Security Gateway is running. The default setting is determined by the setting configured with cpconfig (see "cpconfig"). This setting reverts to the default after reboot.
fwaccel6

Description
Let 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 &lt;max_entries&gt;</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, AutoExpand, 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
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 conns 0
enc bytes 0 dec bytes 0
partial conns 0 anticipated conns 0
dropped packets 0 dropped bytes 0
nat templates 0 port alloc templates 0
conns from nat tmpl 0 port alloc conns 0
port alloc f2f 0
```

**fwaccel stats**

The `fwaccel stats` command provides performance statistics. These values can help you understand traffic behavior and help you to investigate performance issues.

**fwaccel stats Statistics**

<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>Statistic parameter</td>
<td>Explanation</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------</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>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>Statistic parameter</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------</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>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 7).

Run: **cpconfig**

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

**sim affinity**

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

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]`

**Parameters**

<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).

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.
• NAT connections.
• 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.
• Services with source port range.
• 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](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).