Performance Pack

R71

Administration Guide
Contents

Introduction to Performance Pack..........................................................4
Getting Started.........................................................................................5
  Performance Pack System and Hardware Requirements.....................5
  Preparing the Performance Pack R70 Machine.................................5
  BIOS Settings.........................................................................................5
  Network Interface Cards.......................................................................5
  Installing Performance Pack .................................................................6
  Upgrading Performance Pack .................................................................6
Command Line..........................................................................................8
  fwaccel...................................................................................................8
  Usage.....................................................................................................8
  fwaccel stats.........................................................................................9
  cpconfig..............................................................................................11
  Usage.....................................................................................................11
  sim affinity...........................................................................................11
  Usage.....................................................................................................11
  proc entries..........................................................................................12
  Usage.....................................................................................................12
Performance Tuning and Measurement.......................................................14
  Performance Tuning.............................................................................14
  Setting the Maximum Concurrent Connections...............................14
  Increasing the Number of Concurrent Connections........................14
  SecureXL Templates............................................................................14
  Delayed Notification............................................................................14
  Connection Templates........................................................................15
  Delayed Synchronization.....................................................................16
  Multi-Core Systems.............................................................................16
Performance Measurement......................................................................16
  TCP State and Benchmarking..............................................................16
  Non-accelerated traffic analysis.........................................................16
  Performance Troubleshooting..............................................................17
Chapter 1

Introduction to Performance Pack

Performance Pack is supported on SecurePlatform. Performance Pack is a software acceleration product installed as an add-on to Check Point Security Gateway. Performance Pack significantly enhances and improves the performance of Security Gateway.

Performance Pack uses Check Point's SecureXL technology and other innovative network acceleration techniques, to deliver wire-speed performance for Security Gateways. Moreover, it accelerates key security functions, thereby ensuring your organization the best security with the best performance available on an open platform.

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
Chapter 2

Getting Started

In This Chapter

- Performance Pack System and Hardware Requirements
- Preparing the Performance Pack R70 Machine

Performance Pack System and Hardware Requirements

For information on operating system and hardware requirements, as well as the recommended platform configuration, see the R71 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=10330).

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-Threaded.

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 Performance Pack

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.
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 (on page 6).

Upgrading Performance Pack

Upgrading via SmartUpdate (Recommended)

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 via the Command Line

1. Change to the directory where the HFA file (.tgz) is located.
2. Type the following command to extract the HFA file:
   ```bash
   tar –xzvf <HFA file>
   ```
3. Change to the CPppak directory.
4. Type the following command to extract the sim HFA file:
   ```bash
   tar –xzvf <sim HFA file>
   ```
5. Run the sim hot fix.
Chapter 3

Command Line

In This Chapter

fwaccel

cpconfig

sim affinity

proc entries

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.

Usage

fwaccel [on|off|stat|stats|conns|templates]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Start acceleration</td>
</tr>
<tr>
<td>off</td>
<td>Stop acceleration</td>
</tr>
<tr>
<td>stat</td>
<td>Display the acceleration device status and the status of the Connection Templates on the local Security Gateway.</td>
</tr>
<tr>
<td>stats</td>
<td>Displays acceleration statistics.</td>
</tr>
<tr>
<td>stats -s</td>
<td>Displays more summarized statistics.</td>
</tr>
<tr>
<td>stats -d</td>
<td>Displays dropped packet statistics.</td>
</tr>
<tr>
<td>conns</td>
<td>Displays all connections.</td>
</tr>
<tr>
<td>conns -s</td>
<td>Displays the number of connections currently defined in the accelerator.</td>
</tr>
<tr>
<td>conns -m &lt;max_entries&gt;</td>
<td>Limits the number of connections displayed by the conns command to the number entered in the variable max_entries.</td>
</tr>
<tr>
<td>templates</td>
<td>Display all connection templates.</td>
</tr>
</tbody>
</table>
### Parameter Explanation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>templates -d</td>
<td>Displays all drop templates; each template is assembled from four ranges indexes. In order to see mapping between range index and the range itself, use the command &quot;sim ranges -a&quot; (Output will be printed to /var/log/messages)</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 max_entries.</td>
</tr>
<tr>
<td>templates -s</td>
<td>Displays the number of templates currently defined in the accelerator.</td>
</tr>
</tbody>
</table>

## fwaccel stats

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

### Table 3-2  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>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>Statistic parameter</td>
<td>Explanation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------</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>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>
</tbody>
</table>
### cpconfig

Check Point products are configured using the `cpconfig` utility. When run, this utility displays a screen with the configuration options. The options that are displayed depend on the installed configuration and product(s). You can use `cpconfig` to enable or disable Performance Pack. Once you have selected an acceleration setting, the setting remains configured, until you choose to change it on another occasion. In other words, the settings that you define will remain even after the machine is rebooted. For an alternative method to enable or disable acceleration, see `fwaccel` (on page 8).

### Usage

Execute `cpconfig` by entering the following command:

```
cpconfig
```

An interactive menu will be displayed providing you with the option to enable or disable the acceleration by selecting `Enable/Disable Check Point SecureXL`. Select `Enable` in order to enable acceleration. Select `Disable` in order to disable acceleration.

### sim affinity

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

### Usage

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

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, which means that each NIC is handled by all processors. Optimal network performance is obtained when each NIC is individually bound to a single processor. To achieve the above, the sim utility includes an Affinity feature, which has the following operation modes:

<table>
<thead>
<tr>
<th>Table 3-3</th>
<th><strong>Table 3-3 sim Affinity operation modes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Explanation</td>
</tr>
<tr>
<td>-a</td>
<td><strong>Automatic Mode</strong> — the Affinity is determined automatically, by analyzing the load on each NIC. If the NICs are not loaded, the Affinity will not be set. This is the default Affinity operation mode, in which the Affinity is re-tuned every 60 seconds.</td>
</tr>
</tbody>
</table>
| -s        | **Manual Mode** — allows you to manually specify the Affinity settings. For each interface, you will be asked to enter one of the following:  
  • A space-separated list of the processor numbers that are to handle this interface, or  
  • The word all, to allow all processors to handle this interface.  
  When setting the Affinity manually, the periodic automatic check will be disabled. After booting, it will remain disabled and the Affinity settings entered manually will be applied. |
| -l        | View a list of the current Affinity settings. |

proc entries

Performance Pack supports SecurePlatform proc entries. These entries are used to display information about the Performance Pack.

The proc entries are read-only entries. They cannot be configured. The proc entries are located under /proc/ppk.

Usage

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

Parameters

<table>
<thead>
<tr>
<th>Table 3-4</th>
<th><strong>/proc Parameters</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Explanation</td>
</tr>
<tr>
<td>conf</td>
<td>Displays the Performance Pack Configuration.</td>
</tr>
<tr>
<td>ifs</td>
<td>Lists the interfaces to which Performance Pack is attached.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays general Performance Pack statistics.</td>
</tr>
<tr>
<td>drop statistics</td>
<td>Displays Performance Pack dropped packet statistics.</td>
</tr>
</tbody>
</table>
Chapter 4

Performance Tuning and Measurement

In This Chapter

Performance Tuning 14
Performance Measurement 16

Performance Tuning

There are various options for improving performance that can be configured on the Security Gateway.

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).

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](http://supportcontent.checkpoint.com/solutions?id=sk33781).