Check Point DDoS Protector
R75.20 Supplement
Release Notes and Getting Started Guide

7 October 2012

Classification: [Protected]
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=18981

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

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07 October 2012</td>
<td>Updated for link to latest version of documentation</td>
</tr>
<tr>
<td>5 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 Check Point DDoS Protector R75.20 Supplement Release Notes and Getting Started Guide).
Introduction

This release integrates SmartView Tracker and SmartEvent with the Check Point DDoS Protector appliance.

**SmartEvent** includes SmartEvent Intro, SmartReporter and SmartEvent Correlation for centralized reporting, real-time security event correlation, and management of security data. Security teams do not look through massive amounts of data: they focus on the threats and trends with the greatest risk potential.

**SmartView Tracker** is a Logging and Status Software Blade for real-time tracking of logged connections and administrator activity. SmartView Tracker reduces time required to troubleshoot configuration errors.

**Check Point DDoS Protector** is an appliance with advanced Denial of Service (DoS) detection and prevention. DDoS Protector technology inspects signatures and behavior before new server sessions are started.

**Supported Appliance Models**

<table>
<thead>
<tr>
<th>Series</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Point DDoS Protector x06</td>
<td>DDoS Protector 506</td>
</tr>
<tr>
<td></td>
<td>DDoS Protector 1006</td>
</tr>
<tr>
<td></td>
<td>DDoS Protector 2006</td>
</tr>
<tr>
<td></td>
<td>DDoS Protector 3006</td>
</tr>
<tr>
<td>Check Point DDoS Protector x412</td>
<td>DDoS Protector 4412</td>
</tr>
<tr>
<td></td>
<td>DDoS Protector 8412</td>
</tr>
<tr>
<td></td>
<td>DDoS Protector 12412</td>
</tr>
</tbody>
</table>

**Supported Products and Platforms**

**Supported Check Point version:**

R75.20

⚠️ **Important** - If the server has a release or hotfix after R75.20, you must revert to R75.20 before you install.

**Supported Check Point products:**

- SmartEvent server
- Log Server
- Multi-Domain Log Server
- Standalone environment of one of those servers with a Security Management server or Multi-Domain Server

**Supported operating systems:**

- SecurePlatform
- Linux
- Windows
Installation

**Important** - Before you begin installation, we recommend that you backup the Log Server, the SmartEvent server, and (if in a Multi-Domain Security Management environment) the Multi-Domain Log Server.

- Make sure to install on all these servers in your environment.
- After you install this supplement on the logging server, install the new SmartConsole.

**Downloading the Package**

Download the package for the correct platform.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Package Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurePlatform or Linux</td>
<td>fw1_wrapper_HOTFIX_FLOW_HF_BASE_319.tgz</td>
</tr>
<tr>
<td>Windows</td>
<td>fw1_wrapper_FLOW_HF_BASE_319.exe</td>
</tr>
</tbody>
</table>

**Installing with CLI**

The package is the same for Security Management server and for Multi-Domain Security Management. On Multi-Domain Security Management, you must stop the services before you install, and you must activate syslog listening after you install.

**To install with the CLI on Security Management server, SmartEvent, Log Server:**

1. Log in with administrator permissions.
2. Go to the directory of the downloaded file.
3. On Multi-Domain Security Management only, run these commands:
   - mdsenv
   - mdsstop
4. Extract the TGZ and run the installation script:
   - SecurePlatform / Linux
     a) `tar -xvfz fw1_wrapper_HOTFIX_FLOW_HF_BASE_319.tgz`
     b) `./fw1_wrapper_HOTFIX_FLOW_HF_BASE_319_983319016_1`
   - Windows
     a) Extract the files.
     b) Double-click the exe file.
     c) Continue with the installation wizard.
5. Reboot.

After you install this package on Log Servers, it starts to listen to syslog messages. On a Multi-Domain Server, manually activate syslog listening only on the Domain Management Servers that manage DDoS Protector.

**To activate Multi-Domain Security Management log server to listen to syslog messages:**

1. Open the SmartDashboard of the Domain Management Server.
2. Open the Log Server network object.
3. Open Logs > Additional Logging Configuration.
4. Select Accept Syslog messages.
5. Restart the Domain Management Server services:
   mds_stop_customer
   mds_start_customer

Installing SmartConsole

To manage Check Point DDoS Protector logs and details, install the updated SmartConsoles.

1. On the Windows GUI client, download the new SmartConsole executable.
2. Double-click the EXE file.
3. Continue with the installation wizard.
4. Start the new SmartView Tracker and SmartEvent consoles.

DDoS Protector in SmartView Tracker

In SmartView Tracker Predefined filters, open DDoS Protector. You can filter by importance or for Critical Not Prevented attacks.

In SmartView Tracker, see the Status column. Attacks with multiple sources / destinations, usually have multiple logs. That status of these attacks shows sampled, with sample IP addresses from the complete logs.

DDoS Protector in SmartEvent

In SmartEvent Predefined filters, open DDoS Protector. You can filter by importance, severity, or attack name.

Samples:
DoS/DDoS attacks often have multiple sources and multiple destinations in a short amount of time.

- Multiple Sources - See a sample of the attacking IP addresses.
- Multiple Destinations - Destination shows hosts under your protection and under attack. If there are Multiple Destinations, see a sample of the attacked IP addresses.

Use the Details tab to learn more about the attack. With this information, you can fine-tune the DDoS Protector settings. Also, use the Advisory to learn more about the attack. You can link to the Advisory from the Summary tab.

If you enable Learning Mode:

In learning mode, DDoS Protector learns your environment and traffic and then tunes its own thresholds. Be aware of this when reviewing SmartEvent data. There can be inaccurate events while learning.

Uninstalling

If the log server is on Windows, uninstall with Add/Remove Programs. Otherwise, use these steps:

To uninstall this supplement on SecurePlatform or Linux:
1. Log in with administrator permissions.
2. Stop Check Point services:
   cpstop or mdsenv and mdsstop
3. Run: /opt/CPsuite-R75.20/uninstall_fw1_wrapper_HOTFIX_FLOW_HF_BASE_319 -SU
4. Reboot.
5. Install an Event Policy from SmartEvent servers on Correlation Units.

Known Limitations

- Install with SmartUpdate is not supported.
- Before you upgrade to R75.40, you must delete all custom queries in SmartView Tracker and SmartEvent, and custom events related to **DDoS Protector** fields.