DDoS Protector Signaling
Parsing Enhancement

6.12 Hotfix

Release Notes

17 December 2014
© 2014 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.
Important Information

More Information
Visit the Check Point Support Center (http://supportcenter.checkpoint.com).

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 DDoS Protector Signaling Parsing Enhancement 6.12 Hotfix Release Notes).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 December 2014</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
DDoS Protector Signal Parsing

DDoS Protector 6.12 exposes situational signals through the attack data. When DDoS Protector detects an attack, it sends signals to a specified syslog server. The signals have the footprint data, attack events, and traffic anomaly indicators (compared to the normal traffic behavior). This Hotfix lets the log server parse the new DDoS Protector signaling syslog messages.

You can see the formatted logs only in R77.20 SmartLog. To see the attack events with signaling information, you must use the NGSE version of SmartEvent.

Installing

Install the packages of this release on R77.20 Security Management Server and log servers that get DDoS syslog messages.

IMPORTANT - Before you begin:

If you installed earlier builds of this release, uninstall them. The builds of this release are:

- `fw1` - 990154003
- `indexer` - 990154008

Save a backup (snapshot) of the Security Management Server and log servers.

To install:

1. Copy the TGZ files to the Security Management Server and log servers.
2. Extract the TGZ files:
   ```
   # tar -zxvf fw1_wrapper_HOTFIX_GOLLUM_HF_BASE_154.tgz
   # tar -zxvf indexer_HOTFIX_GOLLUM_HF_BASE_154.tgz
   ```
3. Run the installer:
   ```
   # ./fw1_wrapper_HOTFIX_GOLLUM_HF_BASE_154_990154003_1
   # ./indexer_HOTFIX_GOLLUM_HF_BASE_154_990154008_1
   
   The scripts run cpstop and cpstart.
   ```
4. Make sure that installation completes successfully with no errors.
5. Reboot the computer.

To uninstall this build or earlier builds:

1. Run the fw1 uninstaller:
   ```
   /opt/CPsuite-R77/uninstall_fw1_wrapper_HOTFIX_GOLLUM_HF_BASE_154
   ```
2. Run the indexer uninstaller:
   ```
   /opt/CPSmartLog-R77/uninstall_indexer_HOTFIX_GOLLUM_HF_BASE_154
   
   If there are issues, restore the backups and contact Check Point Technical Support.