Flow Sensor and Load Balancer Integration Guide
(for Stealthwatch System v6.9.2)
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Audience</td>
<td>4</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>4</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>4</td>
</tr>
<tr>
<td>Configuring the Load Balancer</td>
<td>5</td>
</tr>
<tr>
<td>Disabling the XFF Option for HTTP</td>
<td>5</td>
</tr>
<tr>
<td>Creating the iRule</td>
<td>6</td>
</tr>
<tr>
<td>Adding the iRule as a Virtual Server Resource</td>
<td>8</td>
</tr>
<tr>
<td>Configuring All Load Balancers in the Network</td>
<td>10</td>
</tr>
<tr>
<td>Enabling XFF Processing on the Flow Sensor</td>
<td>11</td>
</tr>
<tr>
<td>Verifying the Configuration</td>
<td>12</td>
</tr>
<tr>
<td>Verifying the Configuration in the SMC Desktop Client</td>
<td>12</td>
</tr>
<tr>
<td>Adding Columns to the Flow Table (SMC Desktop Client)</td>
<td>12</td>
</tr>
<tr>
<td>Verifying the Configuration in the SMC Web Client</td>
<td>13</td>
</tr>
</tbody>
</table>
Introduction

If a load balancer is installed in front of a resource on the network, it obscures visibility and may reduce the detection of threats in the Stealthwatch System.

Use the instructions in this guide to configure the load balancer and Flow Sensor. This configuration stitches the client side and server side flows together, so the outside host connects to the inside host, providing visibility and enhanced security on the Flow Sensor and the Stealthwatch System.

Audience

The primary audience for this guide includes administrators responsible for configuring the Stealthwatch System.

Before You Begin

Before starting the procedures in this guide, you should do the following:

- Confirm that your Stealthwatch System is communicating. Go to the SMC client interface. Check the Alarm Table to make sure there are no active Management Channel Down or Failover Channel Down alarms.
- Confirm that your Stealthwatch System appliance licenses are active.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco partner
- Contact Cisco Stealthwatch Support
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
Configuring the Load Balancer

Use the following instructions to configure the load balancer. You will disable the X-Forwarded-For (XFF) option for HTTP, create an iRule, and enable a virtual server resource. If you prefer to use an existing iRule, you can modify it using the information provided here. For successful integration, apply the instructions in this section to all load balancers in the network.

**Note:** The instructions in this guide show the configuration on an F5 Load Balancer as an example, but we believe this configuration can be used on all types of load balancers.

Disabling the XFF Option for HTTP

Use the following procedure to disable the XFF option for HTTP.

The built-in functionality to insert data in an XFF HTTP header must be disabled in the F5 Load Balancer as follows:

1. Log in to the F5 Load Balancer configuration utility.
2. Under the Main tab, click **Local Traffic**.
3. Click **Profiles > Services > HTTP**.
   If **HTTP** is not shown in the Services menu, skip to step 8.
4. Click **http**.
5. Under **Settings**, locate **Insert X-Forwarded-For**.
6. Select **Disabled** from the drop-down list (or uncheck the **Enabled** check box to clear it).
7. Click the **Update** button.
8. From the **Services** menu, click **Fast HTTP**.
   - **If Fast HTTP is not available in the Services menu**, skip the rest of this section. Proceed to [Creating the iRule](#).
9. Locate **Insert X-Forwarded-For**.
10. Select **Disabled** from the drop-down list (or uncheck the **Enabled** check box to clear it).
11. Click the **Update** button to save and exit.
12. Continue to [Creating the iRule](#).

## Creating the iRule

Use the following instructions to add an iRule for the XFF header. This procedure is used to map the Load Balancer IP and ensure that accurate port and protocol information are reported to the Flow Sensor.

**Note:** If you prefer to use an existing iRule, you can modify it using the information provided here.

To create an iRule for the XFF header in the F5 Load Balancer, complete the following steps:

1. Under the Main tab, click **Local Traffic**.
2. Click **iRules**.
3. Click the **Create** button.
4. In the **Name** field, enter **xff**.

```sql
continued...
```
5. Copy and paste the following text into the **Definition** field:

```plaintext
when CLIENT_ACCEPTED {
    if { [PROFILE::exists clientssl] } then {
        set client_protocol "https"
        set local_port 443
    } else {
        set client_protocol "http"
        set local_port 80
    }
}
when HTTP_REQUEST {
    if { [HTTP::header exists "X-Forwarded-For"] } {
        HTTP::header replace X-Forwarded-For "[HTTP::header X-Forwarded-For], [IP::client_addr]"
    } else {
        HTTP::header insert "X-Forwarded-For" [IP::client_addr]
    }
    if { [HTTP::header exists "X-Forwarded-Proto"] } {
        HTTP::header replace X-Forwarded-Proto "[HTTP::header X-Forwarded-Proto], $client_protocol"
    } else {
        HTTP::header insert "X-Forwarded-Proto" $client_protocol
    }
    if { [HTTP::header exists "X-Forwarded-Port"] } {
        HTTP::header replace X-Forwarded-Port "[HTTP::header X-Forwarded-Port], [TCP::client_port]"
    } else {
        HTTP::header insert "X-Forwarded-Port" [TCP::client_port]
    }
    if { [HTTP::header exists "X-Forwarded-Host"] } {
        HTTP::header replace X-Forwarded-Host "[HTTP::header X-Forwarded-Host], [IP::local_addr]:$local_port"
    } else {
        HTTP::header insert "X-Forwarded-Host" [IP::local_addr]:$local_port
    }
}
```

6. Click the **Finished** button to save and exit.

7. Continue to [Adding the iRule as a Virtual Server Resource](#).

**Adding the iRule as a Virtual Server Resource**

To enable a virtual server, the new XFF iRule must be added as a resource in the F5 Load Balancer. This step enables the load balancer to report the XFF Header.
1. Under the Main tab, click **Local Traffic**.
2. Click **Virtual Servers**.
3. Locate the **Service Port** column and find **Service Port 80 (HTTP)** or **443 (HTTPS)** that is handling the traffic handled by the device. Click the **Virtual Server** name.

4. Click the **Resources** tab.
5. In the iRules section, click the **Manage** button.

6. Scroll through the Available iRules to find the new XFF iRule. Click the **XFF** iRule to select it.
7. Click on the **<<** button to add the XFF iRule to the **Enabled** box.
8. Click the **Finished** button to save and exit.

**Configuring All Load Balancers in the Network**

If there are multiple load balancers chained on the network, apply the preceding instructions in this Configuring the Load Balancer section on each load balancer before proceeding to [Enabling XFF Processing on the Flow Sensor](#).

Configuring each load balancer preserves the XFF information and appends it. In this configuration, the Flow Sensor will report only the original load balancer IP in the translated host.

Configuring the Load Balancer instructions include the following:

- **Disabling the XFF Option for HTTP**
- **Creating the iRule**
- **Adding the iRule as a Virtual Server Resource**
Enabling XFF Processing on the Flow Sensor

To process the XFF header field on the Flow Sensor, complete the following steps:

1. Log in to the Flow Sensor.
2. Click Configuration.
3. Click Advanced Settings.
4. Check the Enable X-Forwarded-For Processing check box.
5. Click the Apply button.
6. Repeat these instructions on all Flow Sensors in the network that are receiving load balancer support.
7. Continue to Verifying the Configuration.
Verifying the Configuration

To verify the load balancer configuration, log in to the SMC Desktop Client or the SMC Web Client. The SMC Desktop Client provides the load balancer IP address and port, and the SMC Web Client provides the load balancer IP address.

Verifying the Configuration in the SMC Desktop Client

Use the following instructions to review the load balancer IP address and port in the SMC Desktop Client.

1. Open a web page on the server (behind the F5 Load Balancer).
2. Log in to the SMC Desktop Client.
3. Locate the Flow Sensor in the Enterprise Tree. Right-click the Flow Sensor name (or IP address).
4. Click Flows > Flow Table.
5. Review the Translated Host and Translated Port columns to confirm the F5 Load Balancer IP address and port are shown.
   - Translated Host (load balancer IP address)
   - Translated Port (load balancer port)

Adding Columns to the Flow Table (SMC Desktop Client)

If the Translated Host and Translated Port columns are not shown in the SMC Desktop Client Flow Table, complete the following steps:

1. Right-click any column.
2. Scroll through the list. Select More until you reach the T's.
3. Click Translated Host and Translated Port to add them to the Flow Table.
Verifying the Configuration in the SMC Web Client

Use the following instructions to review the load balancer IP address in the SMC Web Client. The translated port is not available in the SMC Web Client. See Verifying the Configuration in the SMC Desktop Client to verify the port.

1. Open a web page on the server (behind the F5 Load Balancer).
2. Log in to the SMC.
3. Click Analyze > Flow Search.
4. Click Search.
5. When the Flow search results display flows, click Manage Columns.
6. Click the check box to add a check mark to Peer NAT and Subject NAT.
7. Click Set.
8. Confirm the load balancer IP address is shown in the Peer NAT column or the Subject NAT column. The column is determined by the direction of flow.

<table>
<thead>
<tr>
<th>START</th>
<th>DURATION</th>
<th>SUBJECT IP ADDRESS</th>
<th>SUBJECT PORT/PROTOCOL</th>
<th>SUBJECT NAT</th>
<th>SUBJECT HOST GROUPS</th>
<th>SUBJECT BYTES</th>
<th>CONNECTION APPLICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 10, 2017 9:17:40 AM</td>
<td>2m 17s</td>
<td>192 View URL Data</td>
<td>52861/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>11.5K</td>
<td>HTTP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:17:40 AM</td>
<td>2m 19s</td>
<td>192 View URL Data</td>
<td>54733/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>9.7K</td>
<td>HTTP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:17:40 AM</td>
<td>2m 17s</td>
<td>192 View URL Data</td>
<td>60374/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>9.42K</td>
<td>SSH/SCP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:16:40 AM</td>
<td>17s</td>
<td>192 View URL Data</td>
<td>52861/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>3.83K</td>
<td>HTTP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:16:40 AM</td>
<td>19s</td>
<td>192 View URL Data</td>
<td>54733/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>3.26K</td>
<td>HTTP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:17:40 AM</td>
<td>2m 15s</td>
<td>192 View URL Data</td>
<td>46463/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>7.64K</td>
<td>SSH/SCP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:16:40 AM</td>
<td>17s</td>
<td>192 View URL Data</td>
<td>60374/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>3.14K</td>
<td>SSH/SCP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:16:40 AM</td>
<td>15s</td>
<td>192 View URL Data</td>
<td>46463/TCP</td>
<td>–</td>
<td>Catch All</td>
<td>2.63K</td>
<td>SSH/SCP (unclassified)</td>
</tr>
<tr>
<td>Aug 10, 2017 9:17:40 AM</td>
<td>1m 43s</td>
<td>192 View URL Data</td>
<td>50459/TCP</td>
<td>192</td>
<td>Catch All</td>
<td>716</td>
<td>HTTP</td>
</tr>
<tr>
<td>Aug 10, 2017 9:16:40 AM</td>
<td>20s</td>
<td>192 View URL Data</td>
<td>50459/TCP</td>
<td>192</td>
<td>Catch All</td>
<td>540</td>
<td>HTTP</td>
</tr>
</tbody>
</table>