



Cisco Secure Network Analytics

Flow Sensor and Load Balancer Integration Guide 7.5.1



Table of Contents

| | |
|-----------------------------------------------------------------|-----------|
| Introduction | 3 |
| Audience | 3 |
| Before You Begin | 3 |
| Configuring the Load Balancer | 4 |
| Disabling the XFF Option for HTTP | 4 |
| Creating the iRule | 5 |
| Adding the iRule as a Virtual Server Resource | 7 |
| Configuring All Load Balancers in the Network | 9 |
| Enabling XFF Processing on the Flow Sensor | 10 |
| Verifying the Configuration | 11 |
| Verifying the Configuration in the Manager Desktop Client | 11 |
| Adding Columns to the Flow Table (Desktop Client) | 11 |
| Verifying the Configuration in the Web App | 12 |
| Contacting Support | 13 |
| Change History | 14 |

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 Secure Network Analytics 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 Secure Network Analytics system.

Audience

The primary audience for this guide includes administrators responsible for configuring the Secure Network Analytics system.

Before You Begin

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

- Confirm that your Secure Network Analytics system is communicating. Go to the Desktop Client. Check the Alarm Table to make sure there are no active Management Channel Down or Failover Channel Down alarms.
- Confirm that your Secure Network Analytics system appliance licenses are active.

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.

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.

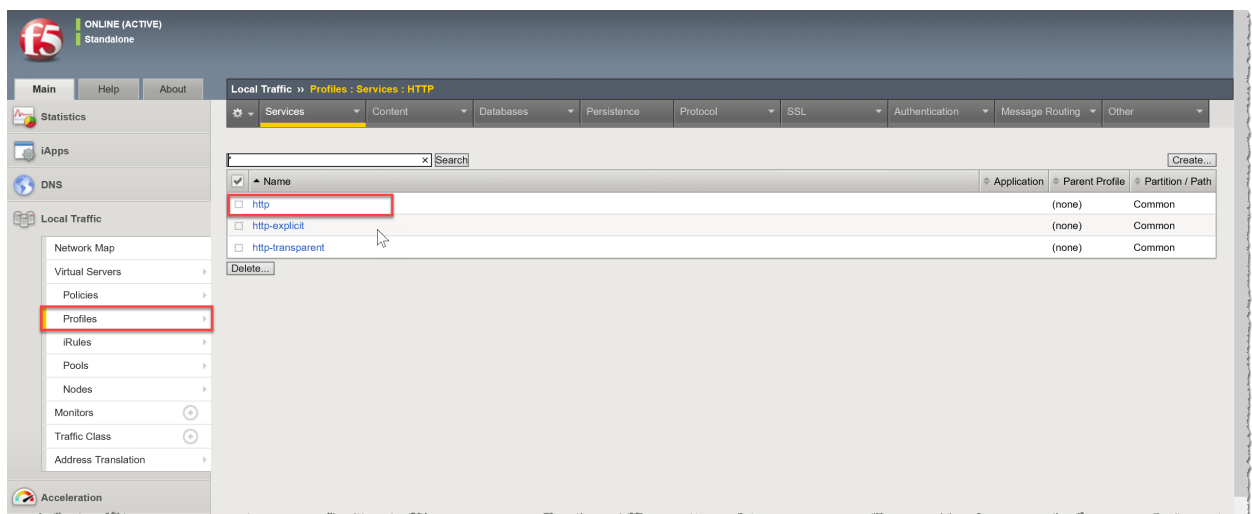
Disabling the XFF Option for HTTP

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).

| Settings | |
|--------------------------------------|---------------------------------------------|
| Basic Auth Realm | <input type="text"/> |
| Fallback Host | <input type="text"/> |
| Fallback on Error Codes | <input type="text"/> |
| Request Header Erase | <input type="text"/> |
| Request Header Insert | <input type="text"/> |
| Response Headers Allowed | <input type="text"/> |
| Request Chunking | Preserve <input type="button" value="v"/> |
| Response Chunking | Selective <input type="button" value="v"/> |
| OneConnect Transformations | <input checked="" type="checkbox"/> Enabled |
| Redirect Rewrite | None <input type="button" value="v"/> |
| Encrypt Cookies | <input type="text"/> |
| Cookie Encryption Passphrase | <input type="text"/> |
| Confirm Cookie Encryption Passphrase | <input type="text"/> |
| Insert X-Forwarded-For | Disabled <input type="button" value="v"/> |
| LWS Maximum Columns | 80 |
| LWS Separator | <input type="text"/> |

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

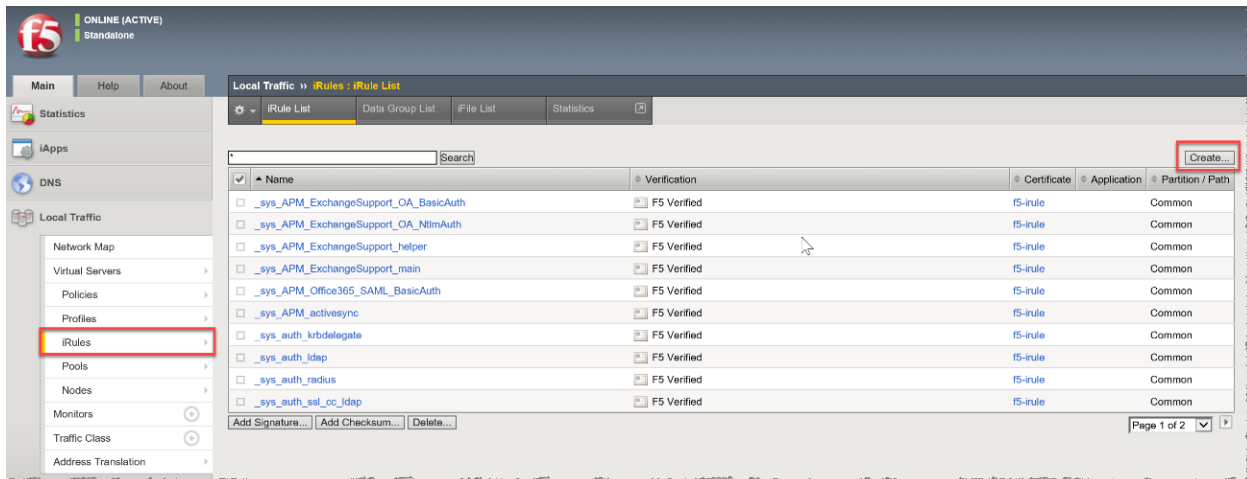
Use the following instructions to add an iRule for the XFF header. This procedure is used to map the Load Balancer IP and ensure that accurate port and protocol information are reported to the Flow Sensor.

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

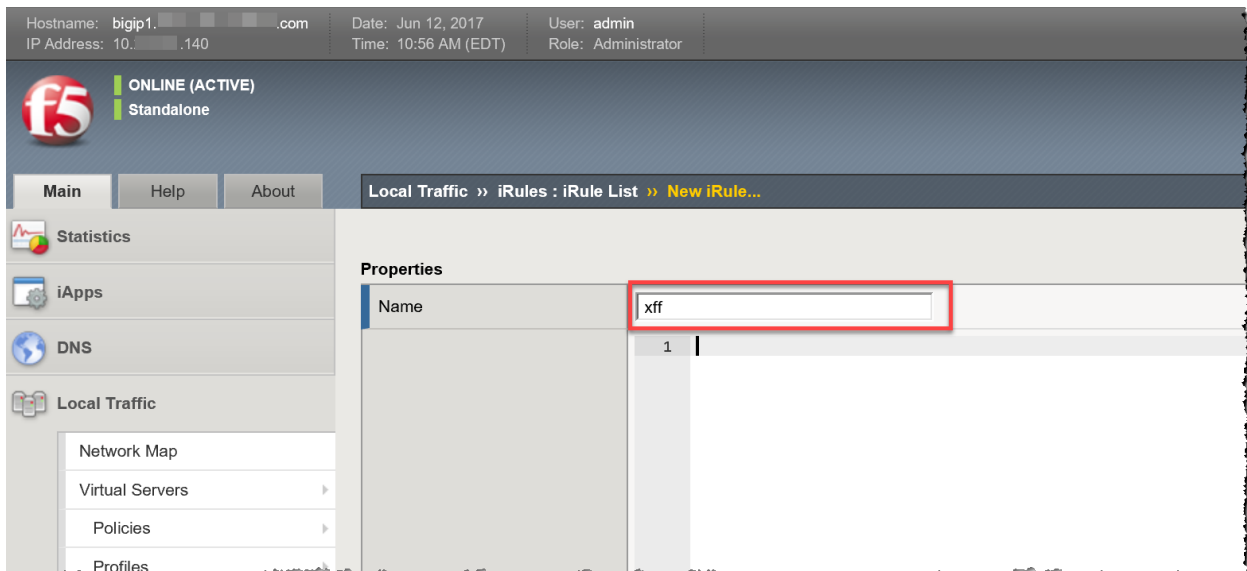
To create an iRule for the XFF header in the F5 Load Balancer, complete the following steps:

1. In the Main tab, click **Local Traffic**.
2. Click **iRules**.

3. Click the **Create** button.



4. In the **Name** field, enter **xff**.



continued...

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

```

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
  }
}

```

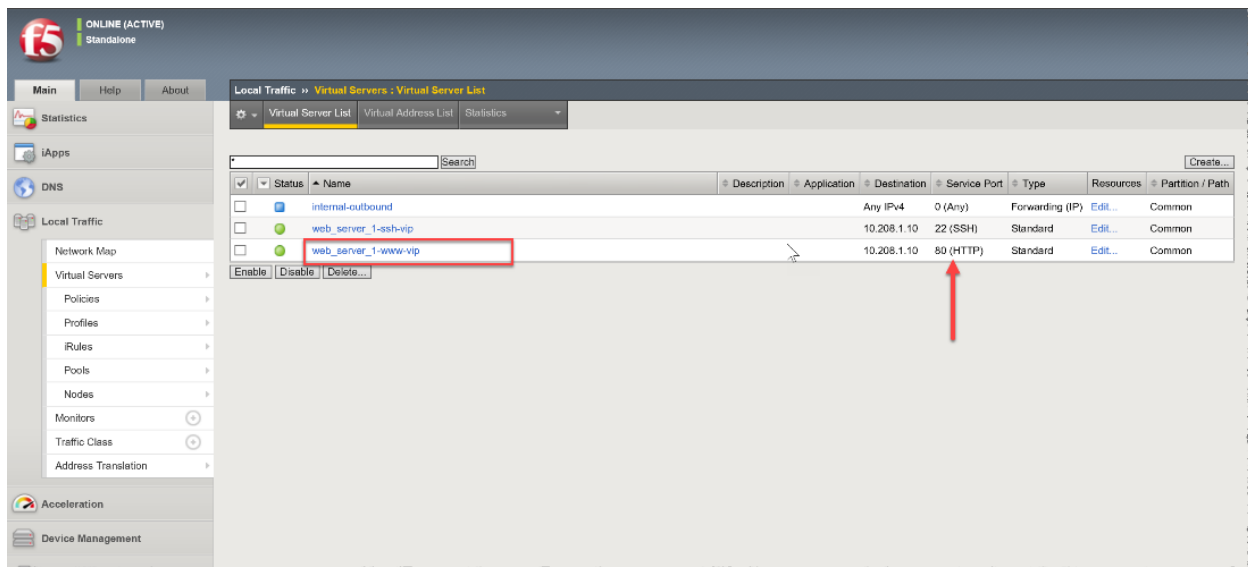
6. Click the **Finished** button to save and exit.

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

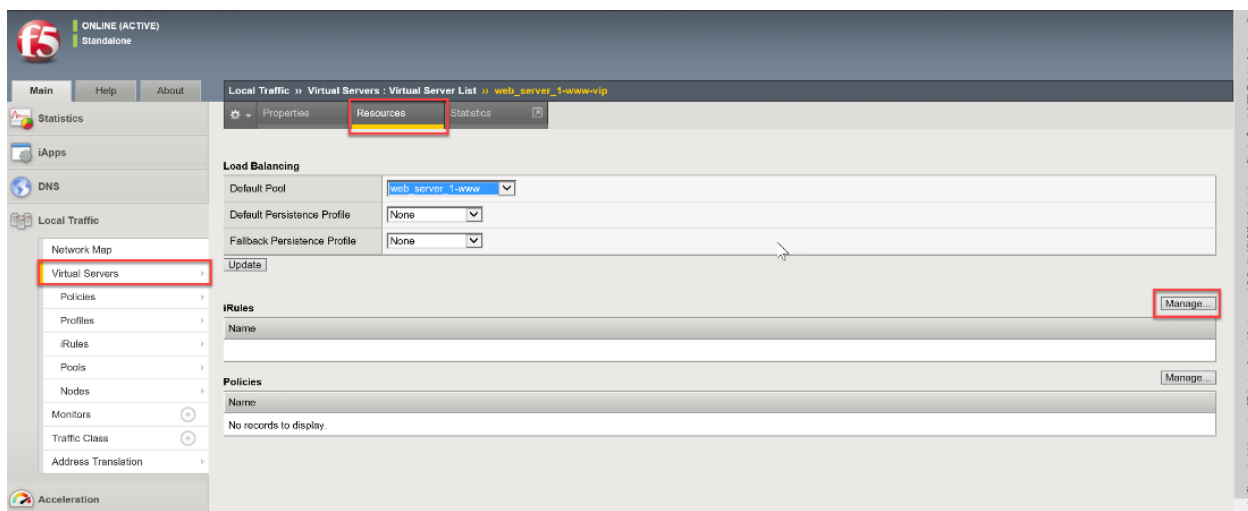
Adding the iRule as a Virtual Server Resource

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.

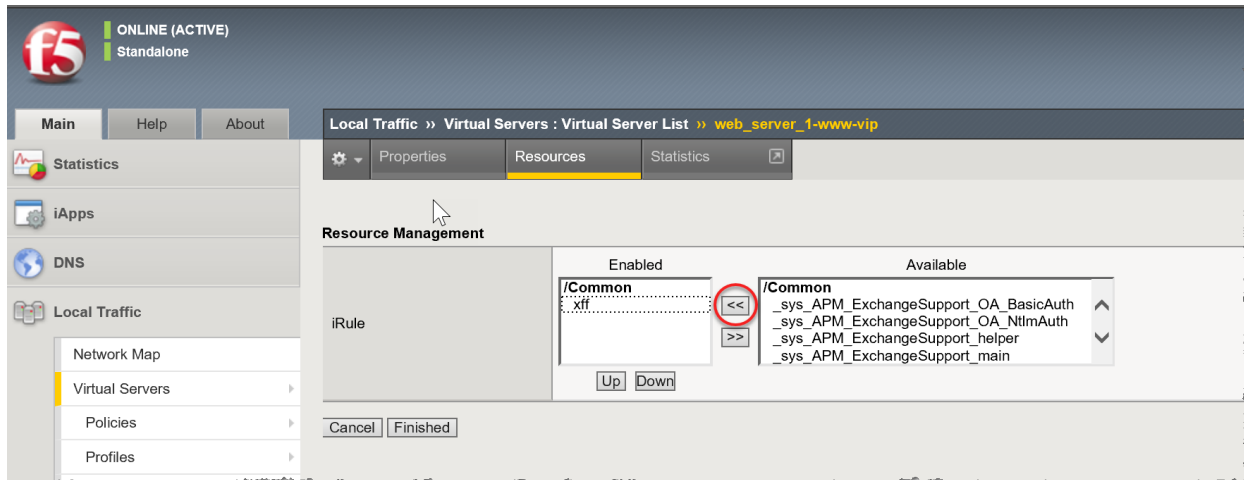
1. Under the Main tab, click **Local Traffic**.
2. Click **Virtual Servers**.
3. Locate the **Service Port** column and find **Service Port 80 (HTTP)** or **443 (HTTPS)** that is handling the traffic handled by the device. Click the **Virtual Server** name.



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.

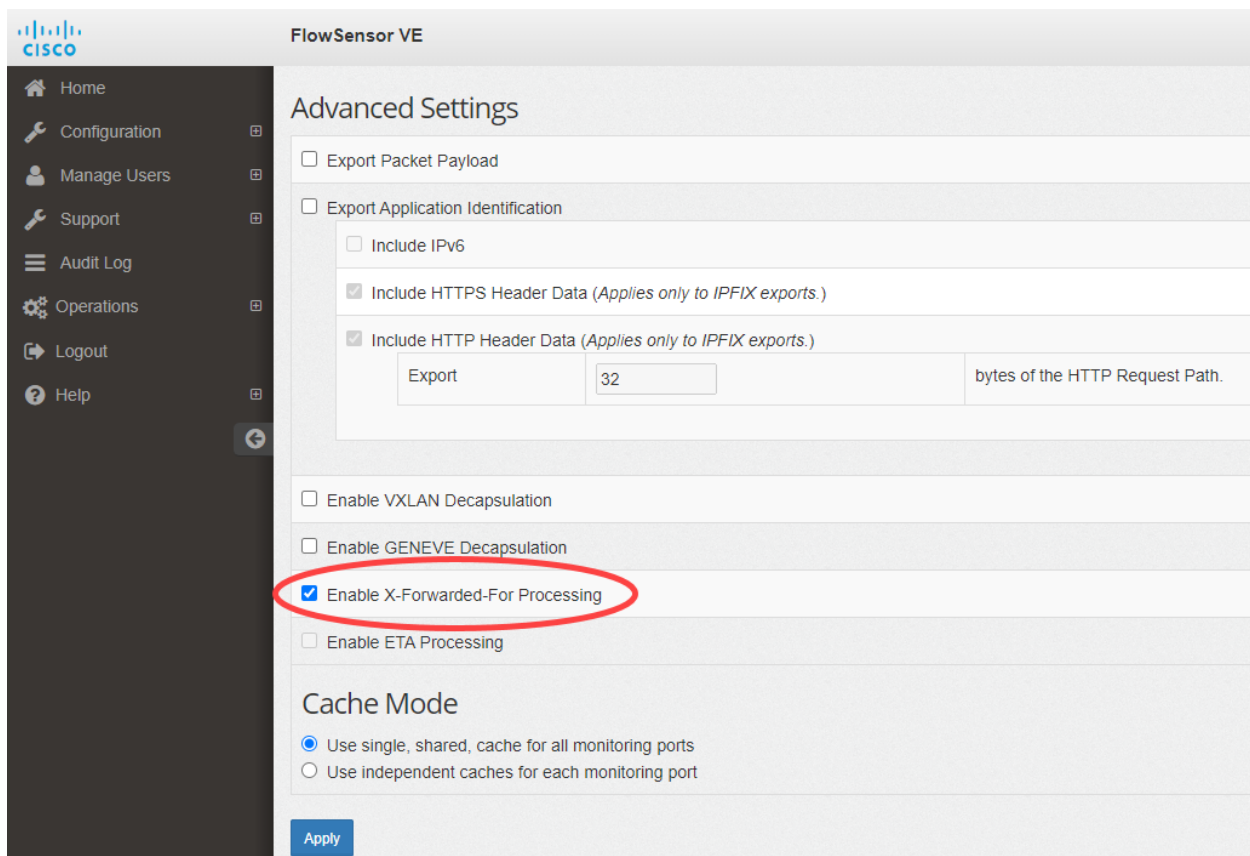
Configuring the Load Balancer instructions include the following:

- [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 your Manager.
2. Click **Configure > Global > Central Management**.
3. Click the **⋯ (Ellipsis)** icon for your Flow Sensor, then click **View Appliance Statistics**. The Flow Sensor Admin interface opens.
4. Click **Configuration > Advanced Settings**.
5. Check the **Enable X-Forwarded-For Processing** check box.



The screenshot shows the Cisco FlowSensor VE Advanced Settings page. The left sidebar contains navigation options: Home, Configuration, Manage Users, Support, Audit Log, Operations, Logout, and Help. The main content area is titled 'Advanced Settings' and includes several sections:

- Export Packet Payload**:
- Export Application Identification**:
 - Include IPv6
 - Include HTTPS Header Data (Applies only to IPFIX exports.)
 - Include HTTP Header Data (Applies only to IPFIX exports.)
 - Export: bytes of the HTTP Request Path.
- Enable VXLAN Decapsulation
- Enable GENEVE Decapsulation
- Enable X-Forwarded-For Processing** (circled in red)
- Enable ETA Processing
- Cache Mode**: Use single, shared, cache for all monitoring ports; Use independent caches for each monitoring port

An **Apply** button is located at the bottom left of the settings area.

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 Desktop Client or the Web App. The Desktop Client provides the load balancer IP address and port, and the Web Client provides the load balancer IP address.

Verifying the Configuration in the Manager Desktop Client

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

1. To generate X-Forwarded-For traffic on a client in front of the F5 Load Balancer, use a browser on a web server located behind the load balancer to log in to the Desktop Client.
2. Locate the Flow Sensor in the Enterprise Tree. Right-click the Flow Sensor name (or IP address).
3. Click **Flows > Flow Table**.
4. 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)

StealthWatch Management Console (admin -)

Enterprise Tree:

- Enterprise
 - SMC
 - UDP Directors
 - Host Groups
 - Network Devices
 - Maps
 - FlowCollectors
 - FlowSensors
 - f5-c...local
 - Identity Services
 - External Devices

Flow Table - 3 records

| Translated Host | Translated Port | Client Host | Server Host | Duration | Application |
|-----------------|-----------------|--------------|--------------|----------|------------------------|
| | | 192.168.1.10 | 192.168.1.10 | 03:07:35 | HTTP (unclassified) |
| | | 192.168.1.10 | 192.168.1.10 | 03:07:35 | SSH/SCP (unclassified) |
| 10.10.10.10 | 52 | 192.168.1.10 | 192.168.1.10 | 00:00:02 | HTTPS (unclassified) |

Adding Columns to the Flow Table (Desktop Client)

If the Translated Host and Translated Port columns are not shown in the 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 Web App

Use the following instructions to review the load balancer IP address in the Web App. The translated port is not available in the Web App. See [Verifying the Configuration in the Manager Desktop Client](#) to verify the port.

1. Open a web page on the server (behind the F5 Load Balancer).
2. Log in to the Manager.
3. Click **Investigate > 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 the flow.

Flow Search Results (10)

[Edit Search](#) Time Range: Last 5 minutes

Subject: Orientation: Either

| START | DURATION | SUBJECT IP ADDRESS | SUBJECT PORT/PROTOCOL | SUBJECT NAT | SUBJECT HOST GROUPS | SUBJECT BYTES | CONNECTION APPLICATION |
|---------------------------|----------|-----------------------------------|-----------------------|-------------|---------------------------|---------------|------------------------|
| ▶ Aug 10, 2017 9:17:40 AM | 2m 17s | 192 View URL Data | 52851/TCP | -- | Catch All | 11.5K | HTTP (unclassified) |
| ▶ Aug 10, 2017 9:17:40 AM | 2m 19s | 192 View URL Data | 54733/TCP | -- | Catch All | 9.74K | HTTP (unclassified) |
| ▶ Aug 10, 2017 9:17:40 AM | 2m 17s | 192 View URL Data | 60374/TCP | -- | Catch All | 9.42K | SSH/SCP (unclassified) |
| ▶ Aug 10, 2017 9:16:40 AM | 17s | 192 View URL Data | 52851/TCP | -- | Catch All | 3.83K | HTTP (unclassified) |
| ▶ Aug 10, 2017 9:16:40 AM | 19s | 192 View URL Data | 54733/TCP | -- | Catch All | 3.25K | HTTP (unclassified) |
| ▶ Aug 10, 2017 9:17:40 AM | 2m 15s | 192 View URL Data | 46467/TCP | -- | Catch All | 7.64K | SSH/SCP (unclassified) |
| ▶ Aug 10, 2017 9:16:40 AM | 17s | 192 View URL Data | 60374/TCP | -- | Catch All | 3.14K | SSH/SCP (unclassified) |
| ▶ Aug 10, 2017 9:16:40 AM | 15s | 192 View URL Data | 46467/TCP | -- | Catch All | 2.63K | SSH/SCP (unclassified) |
| ▶ Aug 10, 2017 9:17:40 AM | 1m 43s | 10 View URL Data | 50459/TCP | 192 | Catch All | 716 | HTTP |
| ▶ Aug 10, 2017 9:16:40 AM | 20s | 10 View URL Data | 50459/TCP | 192 | Catch All | 548 | HTTP |

First < 1 > Last

Contacting Support

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

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

| Document Version | Published Date | Description |
|------------------|----------------|------------------|
| 1_0 | August 9, 2024 | Initial Version. |

Copyright Information

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: <https://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. (1721R)

