



Imperva with Gigamon Deployment Guide

COPYRIGHT

Copyright © 2016 Gigamon. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without Gigamon's written permission.

TRADEMARK ATTRIBUTIONS

Copyright © 2016 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

Contents

1 Overview	4
Deployment Prerequisites	5
Architecture Overview	6
Access Credentials	6
2 Configurations	8
Imperva SecureSphere WAF GATEWAY Configuration: Inline Tools	9
<i>Configuring Imperva for Inline Bridge Mode</i>	9
Configuring Imperva Bridge Interfaces.....	11
Configuring SecureSphere GW via SecureSphere MX	12
GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups	14
<i>Configuring the GigaVUE-HC2 Inline Network and Inline Tools</i>	15
Step 1: Configure the Inline Network Bypass Pair	15
Step 2: Configure the Inline Network Group	17
Step 3: Configure the Inline Tools.....	19
Step 4: Configure the Inline Tool Group	20
<i>Configuring the Inline Traffic Flow Maps</i>	22
Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule	22
Step 2: Configure the Inline Traffic Collector Map	23
Step 3: Change Inline Network Traffic Path to Inline Tool	24
Step 4: Configure GigaVUE HC2 for Inline Monitor Mode	26
<i>Testing the Functionality of the Imperva Inline Tool</i>	27
Assign the Policy to the Imperva Gateways	29
Test the policy	30
3 Summary and Conclusions	31

1 Overview

SecureSphere from Imperva is a comprehensive, cyber security software platform that includes Web, Database and File Security. Imperva SecureSphere appliances support a broad array of deployment options, enabling seamless integration into any data center environment. SecureSphere can be configured as a transparent bridge or an out-of-band network monitor (sniffer). Because of this flexibility, customers can roll out comprehensive application-level security without changing their data center infrastructure. There is no need to reconfigure IP addresses, routing schemes, or applications – allowing SecureSphere to easily be introduced into any network. The SecureSphere appliances protect critical business applications and database servers. Therefore, high availability is an essential customer requirement. To meet this requirement, the Imperva and Gigamon solution offers a range of options that ensure business continuity and application availability.

The GigaVUE-HC2 Series is part of the GigaSECURE[®] Security Delivery Platform from Gigamon. The GigaBPS module in the GigaVUE[®]-HC2 Series provides bypass protection to the Imperva SecureSphere WAF inline tools. The module leverages two levels of bypass protection: Physical and Logical. Physical bypass preserves network traffic, failing to wire in the event of a power outage. Logical bypass protects against inline tool failures that could disrupt network traffic. Bidirectional heartbeats monitor the health of the inline tool and in the event of a loss of link or loss of heartbeat, the traffic can be bypassed around the failing tool; alternatively, the network link can be brought down so that the traffic can be routed to a redundant network path. GigaBPS pertains specifically to fiber links. For copper bypass, Gigamon offers a GigaVUE-HC2 copper TAP module. This module includes electrical relays that can be used for bypass protection.

Aside from the above, deploying Imperva and Gigamon together has the following benefits:

- **Traffic Distribution for load sharing:** Improve the scalability of inline security by distributing the traffic across multiple Imperva SecureSphere WAF appliances, allowing them to share the load and inspect more traffic.
- **Agile Deployment:** Add, remove, and/or upgrade Imperva SecureSphere WAF appliances without disrupting network traffic; convert Imperva SecureSphere WAF appliances from out-of-band monitoring to inline inspection on the fly without rewiring.

The solution tested and described in this guide is based on a standard active inline network and tool deployment where two or more Imperva SecureSphere WAF appliances are directly cabled to one GigaVUE-HC2 chassis. Upon full deployment, the GigaVUE-HC2 sends only the traffic of interest to the Imperva inline tool group for application protection.

The solution described in this guide was tested with one GigaVUE-HC2 visibility node, one GigaVUE-FM Fabric Manager, two Imperva X6500 WAF appliances, and one SecureSphere (MX) management node.

This chapter covers the following:

- [Deployment Prerequisites](#)
- [Architecture Overview](#)
- [Access Credentials](#)

Deployment Prerequisites

The Gigamon plus Imperva Web Application Firewall (WAF) solution consists of the following:

- GigaVUE-HC2 chassis with GigaVUE-OS 4.7.00 software, one TAP-HC0-G100C0 and one PRT-HC0-X24. A BPS-HC0-D25A4G (optional) is also discussed
- GigaVUE-FM version 3.4 software for GigaVUE-HC2 GUI configuration
- Two Imperva appliances, model Gateways. This includes the following:
 - Software version 11.5.0.20
- One Imperva SecureSphere (MX) virtual machine. This includes the following:
 - Software version 11.5.0.20

NOTE: This guide assumes all appliances are fully licensed for all features used, management network interfaces have been configured, and an account with sufficient admin privileges is used.

Architecture Overview

This section presents the combined solution using a GigaVUE-HC2 inline bypass module with two Imperva SecureSphere WAF appliances/Gateways. The reference architecture in Figure 1-1 shows each component's position in the overall network infrastructure, where all network components and inline security tools are connected directly to the GigaVUE-HC2.

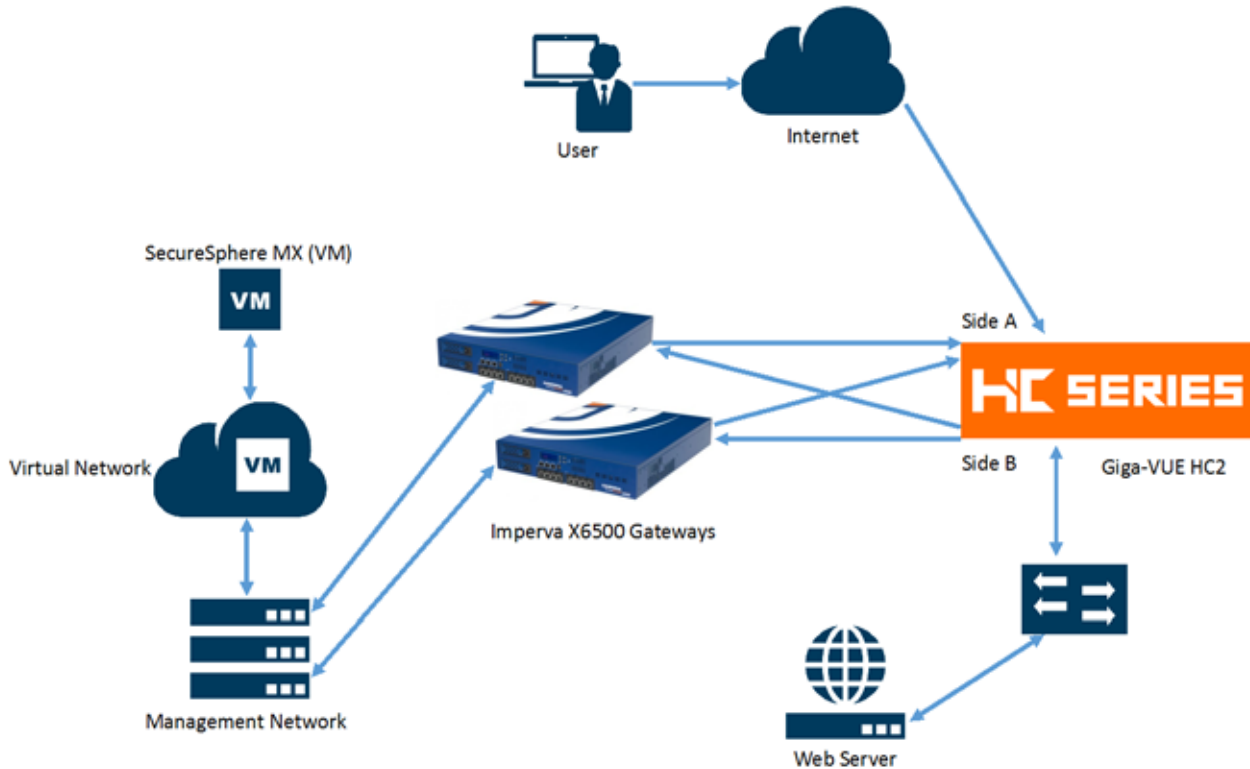


Figure 1-1: Gigamon Inline Bypass with Imperva SecureSphere WAF

NOTE: It is essential that the inline network and inline tool device bridge links are connected to the GigaVUE-HC2 correctly relative to Side A and Side B so that traffic is distributed correctly to the Imperva devices of the inline tool group.

Access Credentials

The default access credentials for the Gigamon GigaVUE-FM and Imperva SecureSphere WAF GATEWAY's are as follows:

- Gigamon GigaVUE-FM access defaults:
 - Username: admin
 - Password: admin123A!
 - There is no default management IP address
- Imperva SecureSphere MX VM:
 - Username: root
 - Password: webco123
 - There is no default management IP address.

NOTE: The GigaVUE-HC2 supports a Graphical User Interface (GUI) named H-VUE[®] and a Command Line Interface (CLI). This document shows only the steps for configuring the GigaVUE-HC2 with GigaVUE-FM. For the equivalent H-VUE and CLI configuration commands, refer to the *GigaVUE-OS H-VUE User's Guide* and *GigaVUE-OS CLI User's Guide* respectively for the 4.7 release.

2 Configurations

This chapter describes the configuration procedures for the GigaVUE-HC2 and Imperva SecureSphere WAF GATEWAY, an inline tool group solution through the Imperva CLI/GUI and Gigamon GigaVUE-FM. The procedures are organized as follows:

- *Imperva SecureSphere WAF GATEWAY Configuration: Inline Tools*
- *Gigamon GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups*

The Imperva CLI/GUI procedures focus on Transparent Bridge mode. The configuration procedures will configure the GigaVUE-HC2 to send live traffic to the Imperva inline tool group (Imperva GW) which will allow the use of Imperva's web application protection capabilities.

Per Imperva's best practices guidelines, the Gigamon GigaVUE-HC2 will be configured to distribute the traffic to the two Imperva appliances in the inline tool group, assuring all traffic for any given client (by IP address) goes to the same member of the Imperva inline tool group.

NOTE: This chapter assumes the Imperva appliances are directly connected to the GigaVUE-HC2 as shown in Figure 1-1. All GigaVUE-HC2 ports to which all Imperva appliances are connected should be configured as port type *Inline Tool*. Furthermore, all GigaVUE-HC2 inline bypass ports to which the network devices are connected should be configured as *Inline Network* type ports. For specific instructions on how to complete these tasks, refer to the User Guides & Technical Documentation in the Customer Portal, which you can access from the Gigamon website.

Imperva SecureSphere WAF GATEWAY Configuration: Inline Tools

The procedures described in this section apply to the shaded area highlighted in the reference architecture diagram shown in Figure 2-1.

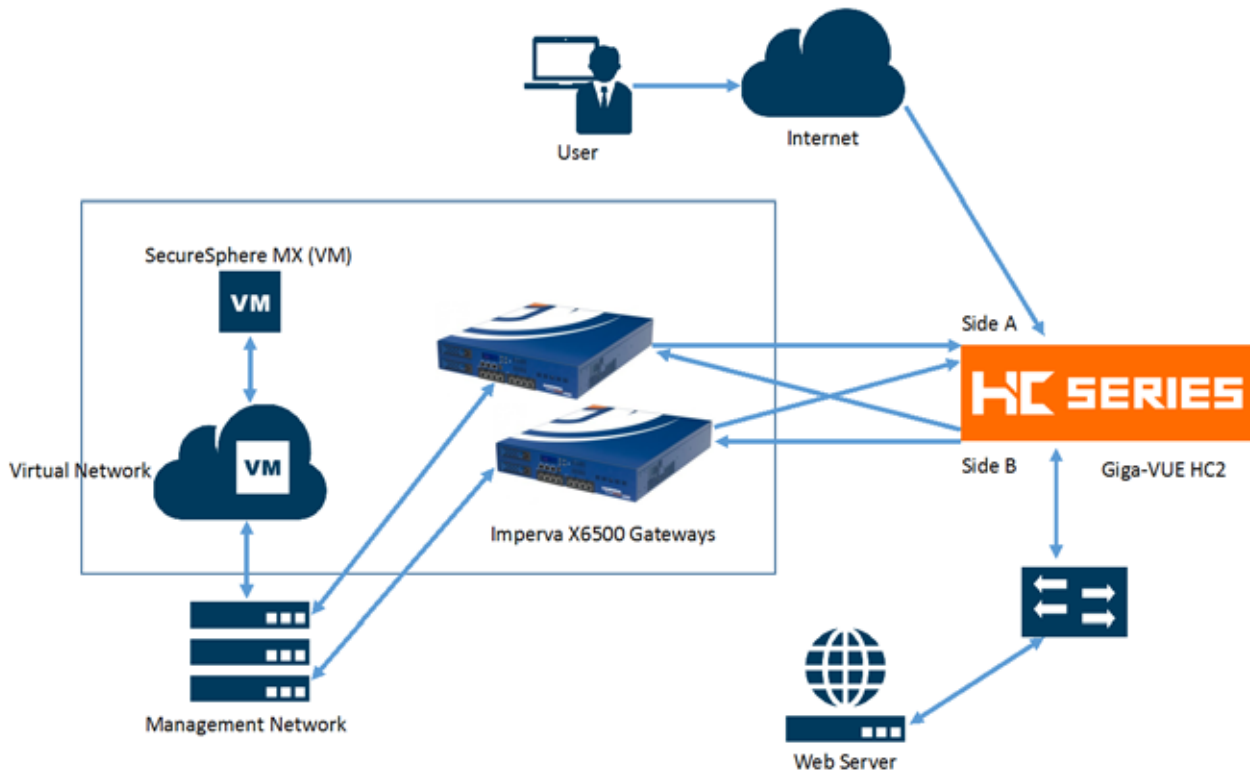


Figure 2-1: Imperva SecureSphere WAF GATEWAY Inline Tools

Configuring Imperva for Inline Bridge Mode

If you already have the Imperva interfaces configured for Bridge Mode you can skip these steps and proceed to Configuring Imperva Using SecureSphere.

To individually configure Imperva SecureSphere WAF GATEWAY for Inline Bridge Mode, do the following steps for each Imperva appliance:

1. In the Imperva CLI enter the following commands:
 - [root@imperva_gw_2 ~]# impcfg
 - Choose option 2 > Manage SecureSphere Gateway as shown in Figure 2-2.

```

-----
SecureSphere 11.5.0.6_0 - impcfg Top Screen
-----

Configuration target:      local (appliance, X4500, reachable)
Gateway status:           registered,running
Setting markers:          C: changed, I: invalid, P: pending (saved but not applied)
Navigation:               Top

Gateway settings
Gateway name:             imperva_gw_2
Gateway mode:             Sniffing
Server address:           10.115.154.25
'secure' user password:   <is-set>
Cluster Configuration:    Disable

1) Manage SecureSphere Management Server.
2) Manage SecureSphere Gateway.
3) Manage platform.

s) Show changes.
D) Discard changes.

S) Save settings.
A) Apply settings.
q) Quit (discarding not-saved changes).

Your choice: █

```

Figure 2-2: Manage SecureSphere Gateway on Imperva Appliance

2. Select option 4 > **Change operation mode**, as indicated in the following figure.

```

-----
SecureSphere 11.5.0.6_0 - Gateway Management Screen
-----

Configuration target:      local (appliance, X4500, reachable)
Gateway status:           registered,running
Setting markers:          C: changed, I: invalid, P: pending (saved but not applied)
Navigation:               Top -> Gateway

Gateway settings
Gateway name:             imperva_gw_2
Gateway mode:             Sniffing
Server address:           10.115.154.25
'secure' user password:   <is-set>
Cluster Configuration:    Disable

1) Perform actions (start, stop, etc.).
2) Change gateway name.
3) Change Management Server address/password.
4) Change operation mode.
5) Manage hardware security modules (HSM).
6) Manage remote agents.
7) Manage interfaces and routes.
8) Change Cluster configuration.

e) End this level. j) Jump to a previous level. t) Top level.
q) Quit (discarding not-saved changes).

Your choice: █

```

3. Choose option 3 > **Bridge IMPVHA**, as shown in the following figure.

Your choice: 4

The SecureSphere gateway operation modes are:

- 1) Sniffing.
- 2) Bridge STP.
- 3) Bridge IMPVHA.
- 4) Reverse Proxy Apache.
- 5) Reverse Proxy Kernel.

Operation mode: █

Configuring Imperva Bridge Interfaces

After configuring the gateway operation mode, configure the interfaces connecting to the Gigamon node as *bridge interfaces*:

1. Enter **e** to end this level and return to the previous screen.
2. Select **7 > Manage interfaces and routes**.
3. Select **1 > Create bridge** as shown in [Figure 2-3](#) and specify the interface connected to Gigamon as Bridge (in this example eth2 and eth3) as shown in the following figure:

```
-----
SecureSphere 11.5.0.6_0 - Bridges Configuration Screen
-----

Configuration target:      local (appliance, X4500, reachable)
Setting markers:          C: changed, I: invalid, P: pending (saved but not applied)
Navigation:               Top -> Gateway -> Interfaces

Gateway name:             imperva_gw_2
C Gateway mode:           Bridge IMPVHA
Server address:           10.115.154.25

Data interfaces:          eth2 eth3 eth4 eth5
Used interfaces:          eth2 eth3 eth4 eth5
Free interfaces:          eth2 eth3 eth4 eth5

C IMPVHA Bridges:        <not-set>

1) Create bridge.
2) Delete bridge.
3) Toggle high-availability on a bridge.

e) End this level. j) Jump to a previous level. t) Top level.
q) Quit (discarding not-saved changes).

Your choice: █

Your choice: 1

Select two free interfaces (space separated) [eth2 eth3 eth4 eth5]: eth2 eth3█
```

Figure 2-3: Imperva Bridge Customization Screen

4. Return to the Top level **t** to Save and then Apply the changes.

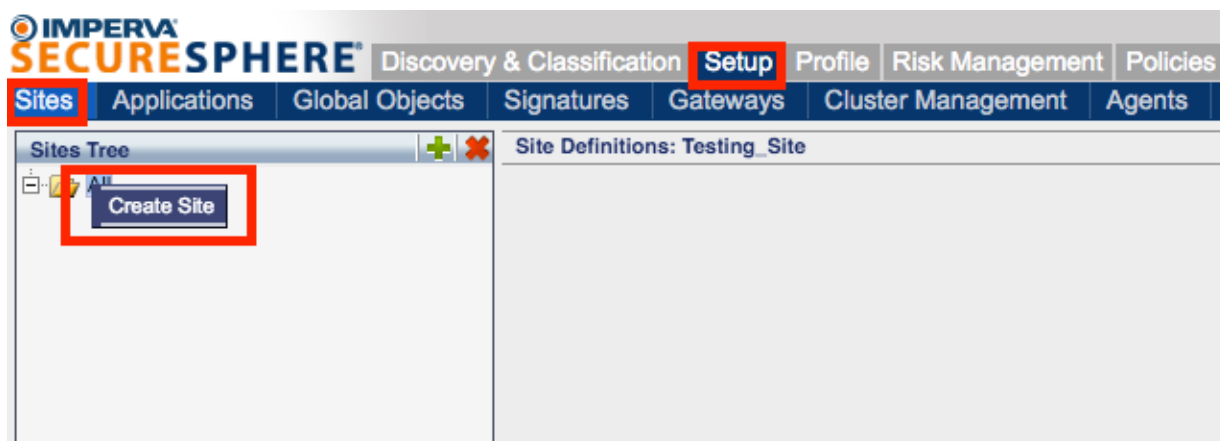
Configuring SecureSphere GW via SecureSphere MX

This section covers configuring the Imperva GATEWAY GW using the SecureSphere management node (MX). These instructions assume you have already added the Imperva Gateways to the SecureSphere management node.

If you already have your Imperva GATEWAY appliances properly configured in SecureSphere, you can skip these steps and proceed to the GigaVUE-HC2 Configuration section.

Create a Site

1. Login to Secure Sphere
2. Select **Setup > Sites**
3. Right click on **All** and choose **Create Site** (or click the green + icon)
4. Name the site and click **Create** (“Imperva_Gateways” in this example)



Create a Server Group

1. Right click on the newly created site (“Imperva_Gateways” in this example), and then select **Create Server Group** (or click the green + icon).
2. Give a name to the Server Group and click **Create** (“Imperva_Server_Group” in this example).



Configuration of Definitions page

1. Select **Mode > Active**.
2. In the **Protected IP Addresses** field, enter the IP address or address of the server or servers protected by the Gateway Group ("10.1.1.25" in this example), and then click **Save**.

Server Group: Imperva_Gateways > Imperva_Server_Group

Definitions Services And Ports Servers Agents Applied Policies

Name: Imperva_Server_Group

Operation
Mode: Active Simulation Disabled

Windows Domain
Windows Domain: None

Windows domain configuration includes Kerberos & Credentials; required for File and MSSQL services only.

Protected IP Addresses

Upload from CSV

IP	Gateway Group	Comments
10.1.1.25	imperva_gw_1	

Show All

Create a Service:

1. Right Click Imperva_Server_Group and select Create Service.

IMPERVA SECURESPHERE Discovery & Classification Setup Profile Risk

Sites Applications Global Objects Signatures Gateways Cluster Ma

Sites Tree

- All
- Imperva
- Imperva_Server_Group

Create Service
Delete Server Group

Server Group: Imperva > Imperva_Group

Definitions Services And Ports Se

Name: Imperva_Gro

Operation
Mode: Active

Windows Domain

2. Name the Service (HTTP in this example), and then click **Create**.

Create Service

Name: HTTP

HTTP Service

Create Cancel

GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups

This section covers configuring the GigaVUE-HC2 for all inline network and inline tool elements that you will use to create traffic flow maps. There are some configuration differences, depending upon if you are using BPS (Bypass fiber) or BPC (Bypass copper) interfaces for inline bypass. These differences are explained in this section. This configuration consists of the following procedures:

- *Configuring the GigaVUE-HC2 Inline Network and Inline Tools*
- *Configuring the Inline Traffic Flow Maps*
- *Testing the Functionality of the Imperva Inline Tool*

The configuration procedures described in this section apply to the highlighted area in Figure 2-4.

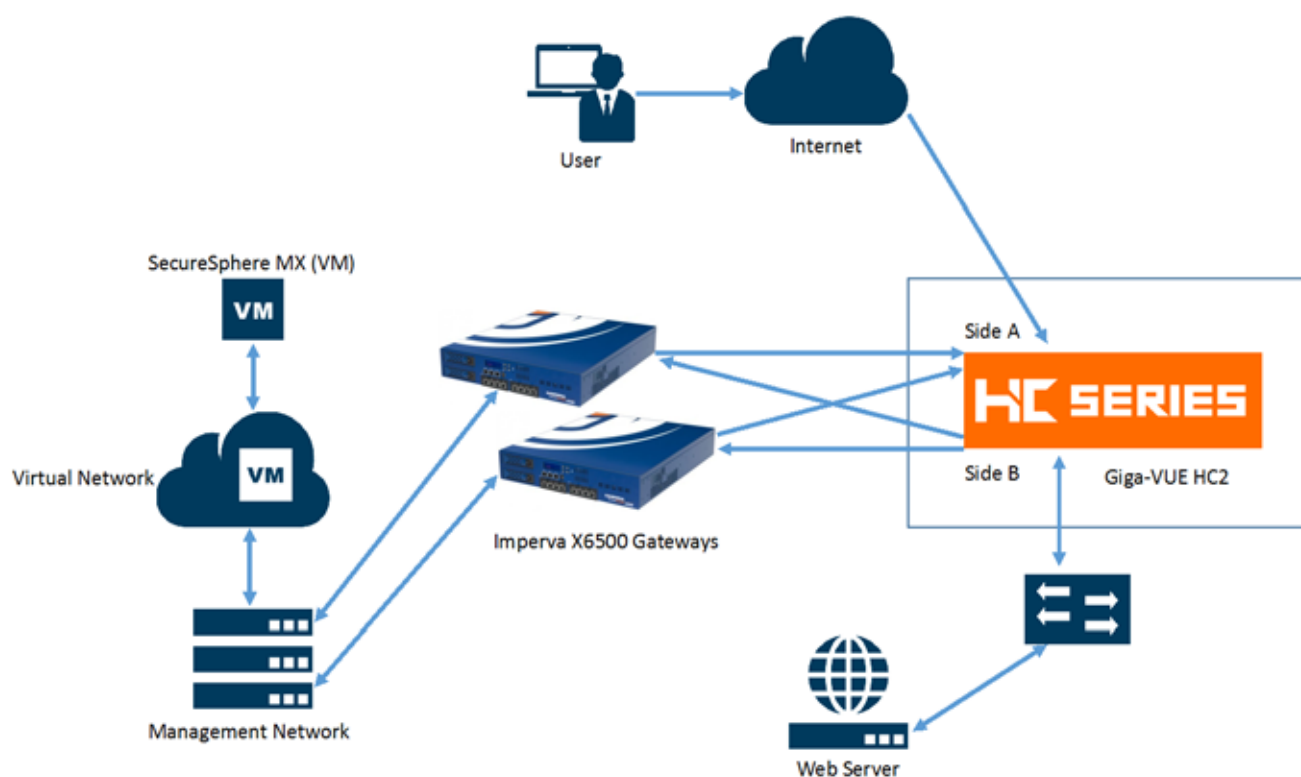


Figure 2-4: Gigamon GigaVUE-HC2 Configurations

Configuring the GigaVUE-HC2 Inline Network and Inline Tools

This section walks you through the steps needed to configure inline network bypass pairs and an inline network group for those pairs. As the enterprise infrastructure grows, you can add additional inline network pairs to the inline network group. The basic steps are as follows:

- *Step 1: Configure the Inline Network Bypass Pair*
- *Step 2: Configure the Inline Network Group*
- *Step 3: Configure the Inline Tools*
- *Step 4: Configure the Inline Tool Group*

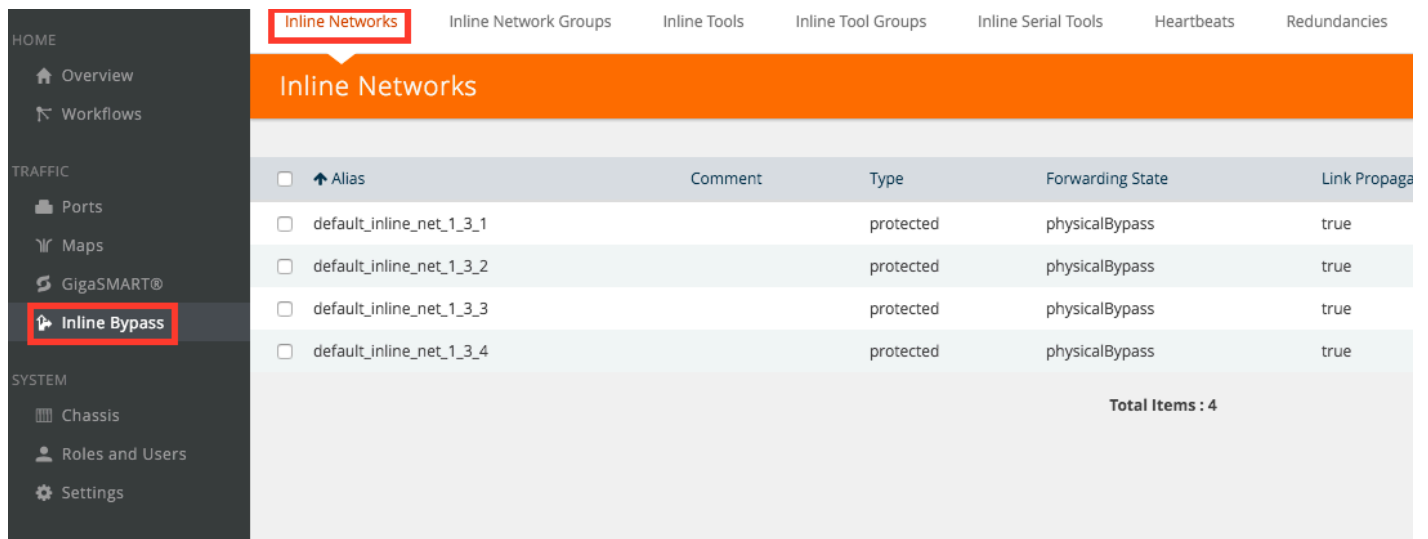
NOTE: This section assumes all the ports to which the network devices are connected are set as Inline Network port types. For specific instructions on completing these tasks, refer to the User Guides & Technical Documentation in the Customer Portal, which you can access from the Gigamon website.

Step 1: Configure the Inline Network Bypass Pair

To configure the inline network bypass pair, do the following:

1. Log into GigaVUE-FM, select **Physical Nodes**
2. Select the GigaVUE-HC2 from the list of physical nodes GigaVUE-FM is managing.
3. Select **Inline Bypass > Inline Networks**.

NOTE: If there the GigaVUE-HC2 has a bypass combo module, there will be four preconfigured Inline Network port pairs as shown in Figure 2-5. If your network is 1G or 10G fiber, use one of these preconfigured inline bypass pairs and move on to Step 2. If your network is 1G copper, follow the instructions below.



Alias	Comment	Type	Forwarding State	Link Propagation
<input type="checkbox"/> default_inline_net_1_3_1		protected	physicalBypass	true
<input type="checkbox"/> default_inline_net_1_3_2		protected	physicalBypass	true
<input type="checkbox"/> default_inline_net_1_3_3		protected	physicalBypass	true
<input type="checkbox"/> default_inline_net_1_3_4		protected	physicalBypass	true

Total Items : 4

Figure 2-5: Inline Networks Page

4. Click **New**. The Inline Network configuration page displays.
5. On the Inline Network page, do the following, and then click **Save** when you are done.

- In the **Alias** field, type an alias that will help you remember which network link this Inline Network bypass pair represents. For example, InLineNet1.
- Select the port for **Port A** by using the drop-down list or by typing the port label in the Port A field for the A Side port as it is represented in the network topology diagram shown in Figure 1-1.

The value in the Port B field automatically populates once you have selected the port for Port A.

Important: It is essential Side A and B of the GigaVUE-HC2 match the Side A and B of the GATEWAY or traffic distribution for the Inline Tool Group will not work correctly.

- Leave the **Traffic Path** and **Link Failure Propagation** set to the default values.
- Select **Physical Bypass**. This minimizes packet loss during traffic map changes.

The configuration page should look like the example shown in Figure 2-6.

NOTE: Traffic Path is set to Bypass to prevent packet loss until the inline tool groups and maps have been set up. After the inline tool groups and maps are configured, the traffic path can be set to inline tool as described in a subsequent section.

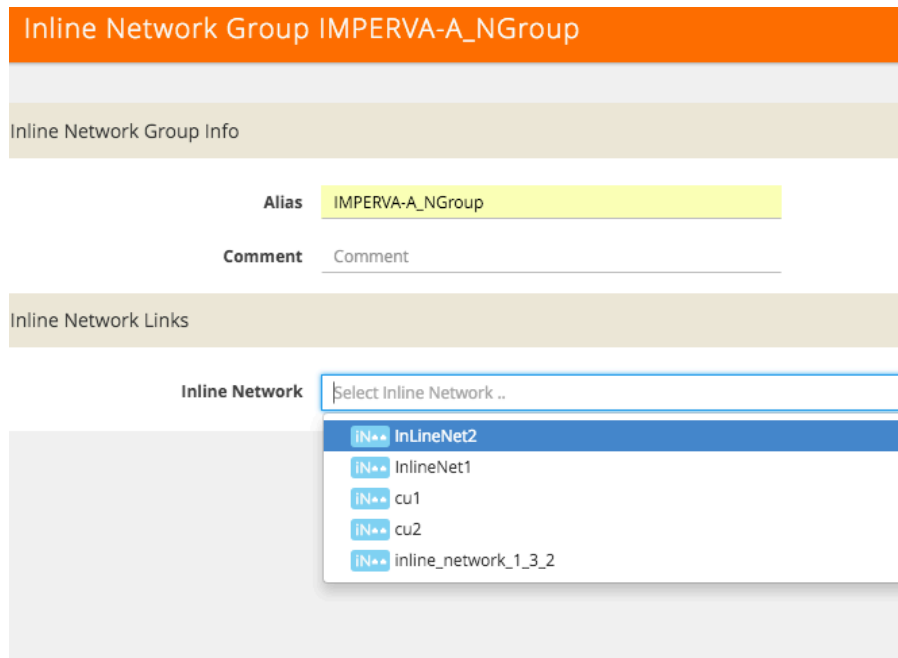
Figure 2-6: Inline Network Pair Configuration

6. Repeat these steps for all other network links.

Step 2: Configure the Inline Network Group

To configure the inline network group, do the following:

1. In GigaVUE-FM, select **Inline Bypass > Inline Network Groups**.
2. Click **New**.
3. In the **Alias** field, type an alias that represents the inline network group. For example, IMPERVA-A_NGroup.
4. Click the **Inline Network** field and either select from the drop-down list as shown in Figure 2-7 or start typing any portion of the alias associated with Inline Network that you want to add to the Inline Network Group.



The screenshot displays the configuration interface for an Inline Network Group. At the top, the title is "Inline Network Group IMPERVA-A_NGroup". Below this, there is a section titled "Inline Network Group Info" containing two fields: "Alias" with the value "IMPERVA-A_NGroup" and "Comment" with the value "Comment". Underneath is the "Inline Network Links" section, which features a dropdown menu labeled "Inline Network". The dropdown is open, showing a list of available inline networks: "InLineNet2", "InlineNet1", "cu1", "cu2", and "inline_network_1_3_2".

Figure 2-7: Inline Network Selection

5. Continue adding inline networks until all port pairs are in the **Inline Network** field as shown in Figure 2-8.

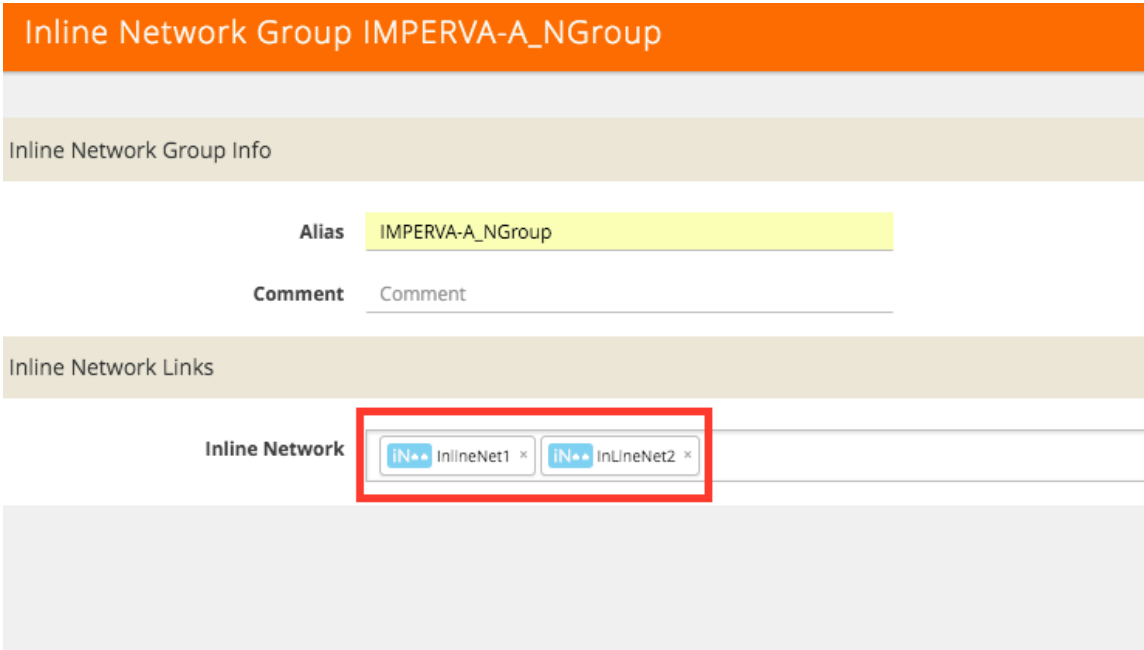


Figure 2-8: Inline Networks added to the Inline Network Group

6. Click **Save** when you are done.

The Inline Network Groups page should look similar to what is shown in Figure 2-9.

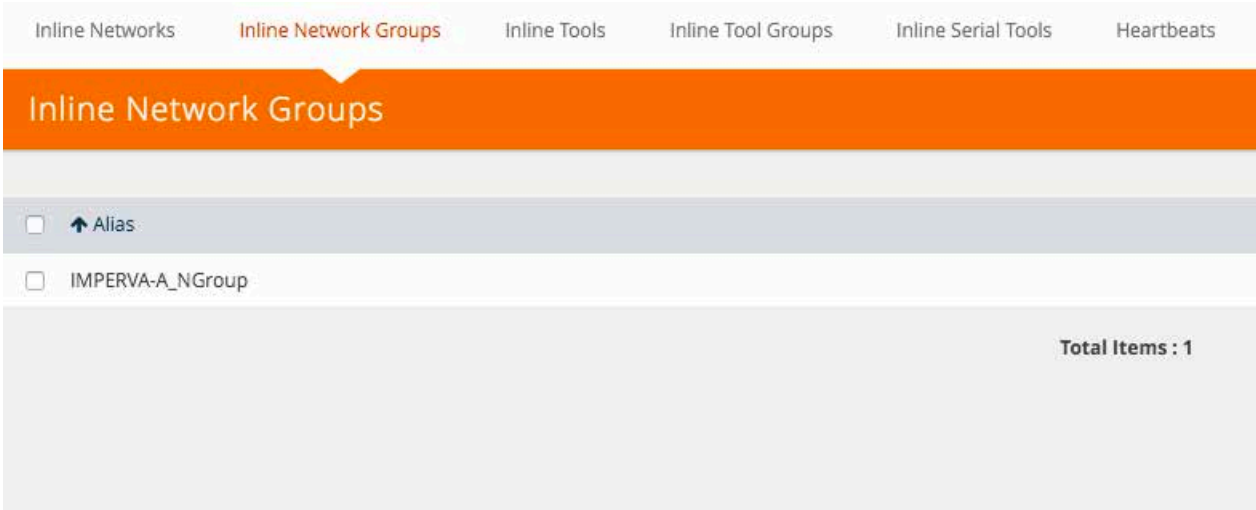


Figure 2-9: Finished list of Inline Network Groups

Step 3: Configure the Inline Tools

This section walks you through the steps necessary to define the inline tool port pairs and the inline tool group that will be used in the traffic flow map defined in later steps.

1. In GigaVUE-FM, select **Inline Bypass > Inline Tools**.

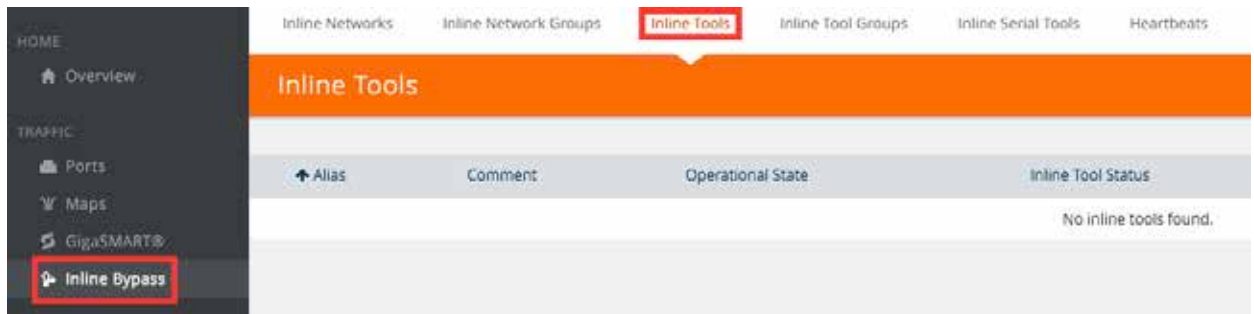


Figure 2-10: Navigating to the Inline Tools page

2. Click **New** to open the configuration page for inline tools.
3. In the **Alias** field, type an alias that will help you remember which inline tool this inline tool pair represents. For example, `Imperva1`.
4. In the Ports section, specify the ports as follows:
 - For **Port A**, specify the port that corresponds to Side A in the network diagram.
 - For **Port B**, specify the port that corresponds to Side B in the network diagram. For the network diagram, refer to Figure 1-1.

Important: It is essential Port A and Port B match Side A and B, respectively, of the inline network port pairs.

5. Leave the default setting for the remaining configuration options.

Your configuration should be similar to the example shown in Figure 2-11.

Figure 2-11: Inline Tool Pair Configuration

6. Click **Save**.
7. Repeat steps 2 through 6 for all additional inline tools.

NOTE: The failure action for this inline tool is **ToolBypass**. This means that the GigaVUE-HC2 will not send traffic to this inline tool if it is considered to be in a failure mode. There are other options for inline tool failure that are fully described in the online help. The other options have very different effects on the overall traffic flow. If the heartbeat feature is not enabled, the failover action will only take place if one of the tool port links go down.

Step 4: Configure the Inline Tool Group

To configure the inline tool group, do the following:

1. In GigaVUE-FM, select Inline Bypass > Inline Tool Groups.
2. Click **New** to open the Inline Tool Groups configuration page.
3. In the **Alias** field, type an alias that describes the inline tool groups. For example:
IT-GRP_IMP1-IMP2.
4. In the Ports section, click the **Inline tools** field and select all the inline tools for this group from the list of available inline tools.

There is an option to select an **Inline spare tool**. When this option is configured, it becomes the primary failure action for this inline tool group.

5. In the Configuration section, do the following, and then click **Save** when you are done:
 - Select **Enable**.
 - Select **Release Spare If Possible** if applicable.
 - Keep the defaults for **Failover action**, **Failover Mode**, and **Minimum Healthy Group Size**.
 - Select **a-srcip-bdstip** for **Hash**.

The configuration should look similar to the example shown in Figure 2-12.

Inline Tool Group IT-GRP_IMP1-IMP2

Inline Tool Group Info

Alias IT-GRP_IMP1-IMP2

Comment Comment

Ports

Inline Tools Imperva1 × Imperva2 ×

Inline Spare Tool Select inline spare tools..

Configuration

Enabled

Release Spare if Possible

Failover Action ToolByPass

Failover Mode Spread

Minimum Healthy Group Size 1

Hash a-srcip-b-dstip

Figure 2-12: Inline Tool Group Configuration

Configuring the Inline Traffic Flow Maps

This section describes the high-level process for configuring traffic to flow from the inline network links to the inline Imperva tool group allowing you to test the deployment functionality of the Imperva appliances within the group. This is done in three steps as follows:

- Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule
- Step 2: Configure the Inline Traffic Collector Map
- Step 3: Change Inline Network Traffic Path to Inline Tool

After completing these steps, you will be ready to test the deployment of the Imperva appliances. The section “Test the Functionality of the Imperva Inline Tool” on page 27 describes the test procedure.

Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule

This section walks you through the configuration of traffic flow map between the Inline Network Group and the Inline Tool Group.

1. In GigaVUE-FM, navigate to the **Maps** page.
2. Click **New**. The New Map page displays.
3. In the Map Info section, do the following:
 - In the **Alias** field, enter a map alias that represents the network source and tool destination.
 - Set **Type** to Inline.
 - Set **Sub Type** to By Rule.
 - Set **Traffic Path** to Bypass.
4. In Map Source and Destination, set the **Source** and **Destination** as follows:
 - Set Source to the inline network group that you created in Step 2: Configure the Inline Network Group.
 - Set Destination to the inline tool groups that you created in Step 4: Configure the Inline Tool Group.
5. In Map Rules, click **Add a Rule**.
6. Specify the following for the rule:
 - a. Click in the Condition search field for the Rule and select **ip4Proto** from the drop-down list.
 - b. Select **Pass**. (This is the default.)
 - c. Select **Bi Directional**.

- d. In the Ipv4 Protocol drop-down list, select **IGMP**.

The map rule should look like the rule shown in [Figure 2-13](#).



The screenshot shows a web interface for configuring map rules. At the top, there is a header 'Map Rules' with a dropdown arrow. Below the header are three buttons: 'Quick Editor', 'Import', and 'Add a Rule'. Underneath, there is a section for 'Rule 1'. It includes a name field (empty), three radio buttons for 'Pass' (selected), 'Drop', and 'Bi Directional' (checked), and a checkbox for 'Bi Directional'. Below this is a configuration box for 'IPv4 Protocol' with a dropdown menu set to 'IGMP' and a priority field set to '2'.

Figure 2-13: Rule for Inline Tool Flow Map

NOTE: Additional traffic can be bypassed by adding rules to the map.

7. Click **Save**.

Step 2: Configure the Inline Traffic Collector Map

This section walks you through the steps to create another traffic map, which is a collector. This map sends all the traffic not matched in the first traffic flow map to the inline tool group. This Collector pass rule must be created because there is no implicit pass for traffic, meaning all inline traffic from any given inline network not matched by a pass rule is discarded.

To configure the collector map, do the following:

1. In GigaVUE-FM, navigate to **Maps** page, and then click **New**. The New Map page displays.
2. In the Map Info section, do the following:
 - In the **Alias** field, type a map alias that identifies that this collector map is for the same inline network as the traffic map you created in [Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule](#). For example, `Collector-ING_ITG`.
 - Set **Type** to Inline.
 - Set **Sub Type** to Collector.
 - Set **Traffic Path** to Normal.
3. In Map Source and Destination, set the **Source** and **Destination** to the same source and destination as the first rule map configured in [Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule](#).

New Map

Map Info

Map Alias: Collector-ING_ITG

Comments:

Type: Inline

Sub Type: Collector

Traffic Path: Normal

Map Source and Destination

Port Editor

Source: IMPERVA-A_NGroup

Destination: IT-GRP_IMP1-IMP2

GSOP: None

Figure 2-14: Configuration for Collector Map

Step 3: Change Inline Network Traffic Path to Inline Tool

After configuring the maps, you need to change the traffic path for the inline networks from Bypass to Inline Tool. However, before setting the traffic path to Inline Tool, make sure that the inline tool ports are up. You can check the status of the ports by going to the Chassis View page in GigaVUE-FM by selecting **Chassis** from the main navigation pane.

To change the traffic path from bypass to inline tool, do the following:

1. In GigaVUE-FM, select **Inline Bypass > Inline Networks**.
2. Select one of the inline networks that you defined previously (refer to Step 2: Configure the Inline Network Group), and then click **Edit**.
3. In the Configuration section, make the following changes:
 - Set **Traffic Path** to Inline Tool.
 - Uncheck **Physical Bypass**.

Inline Network InlineNet1

Inline Network Info

Alias InlineNet1

Comment Comment

Ports

Port Editor

Port A iN 1/3/g11

Port B iN 1/3/g12

Configuration

Traffic Path To Inline Tool

Link Failure Propagation

Physical Bypass

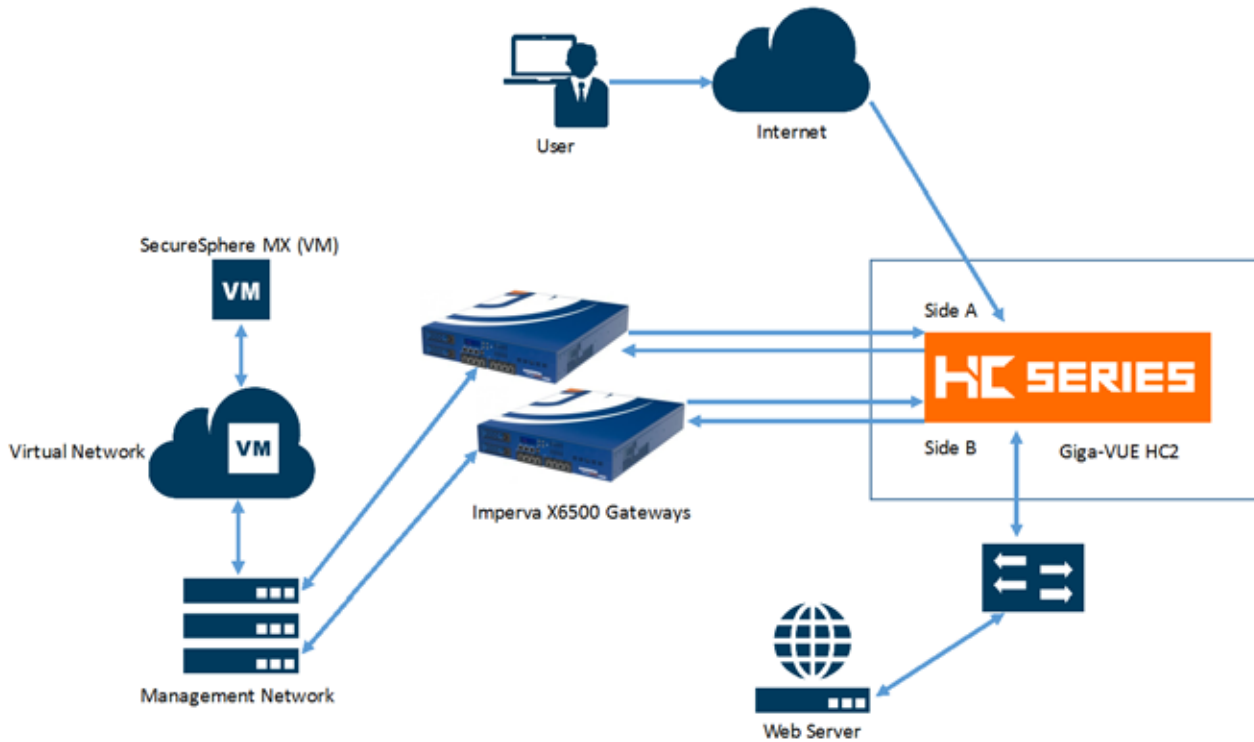
Redundancy Profile Select redundancy profile ..

Figure 2-15: Inline Network Traffic Path Changed to Inline Tool, Physical Bypass Unchecked

4. Click **Save**.
5. Repeat step 3 and step 4 for each inline network in the inline network group.

Step 4: Configure GigaVUE HC2 for Inline Monitor Mode

The procedures described in this section apply to the shaded area highlighted in the reference architecture diagram shown in the following figure.



1. Edit Inline Network Group

The screenshot shows the configuration interface for an inline network group named 'Inline Network InlineNet1'. The interface includes the following sections:

- Inline Network Info:** Alias: inlineNet1, Comment: Comment
- Ports:** Part Editor, Part A: 1/1g11, Part B: 1/1g12
- Configurations:** Traffic Path: Bypass, Link Failure Propagation: , Physical Bypass: , Redundancy Profile: default-standby-2000

2. Uncheck **Physical Bypass** and click **Save**.

Testing the Functionality of the Imperva Inline Tool

While testing the functionality of Imperva, it may be helpful to monitor the port statistics on the GigaVUE-HC2. To access the port statistics for the inline tool ports, do the following:

1. Launch a serial console or SSH session to the GigaVUE-HC2.
2. Log in as admin and enter the following commands at the command prompt, where the port lists in the command are the inline tool ports:

```
HC2-C03-29 > en
HC2-C03-29 # conf t
HC2-C03-29 (config) # clear port stats port-list 1/2/x13..x14
HC2-C03-29 (config) # show port stats port-list 1/2/x13..x14
```

3. Open a web browser and make an HTTP request to the web server. Reload the page several times or click on some of the links.
4. Issue the **show ports stats** command again from the GigaVUE-HC2 CLI. It should look like the following example output:

```
HC2-C03-29 # show port stats port-list 1/2/x13..x14
```

Counter Name	Port: 1/2/x13	Port: 1/2/x14
IfInOctets:	417284603	300347411
IfInUcastPkts:	340852	346126
IfInNUcastPkts:	320	170747
IfInPktDrops:	0	0
IfInDiscards:	5	5
IfInErrors:	0	0
IfInOctetsPerSec:	0	1313
IfInPacketsPerSec:	0	12
IfOutOctets:	300311475	417309114
IfOutUcastPkts:	345988	341091
IfOutNUcastPkts:	170828	315
IfOutDiscards:	0	0
IfOutErrors:	0	0
IfOutOctetsPerSec:	1313	0
IfOutPacketsPerSec:	12	0

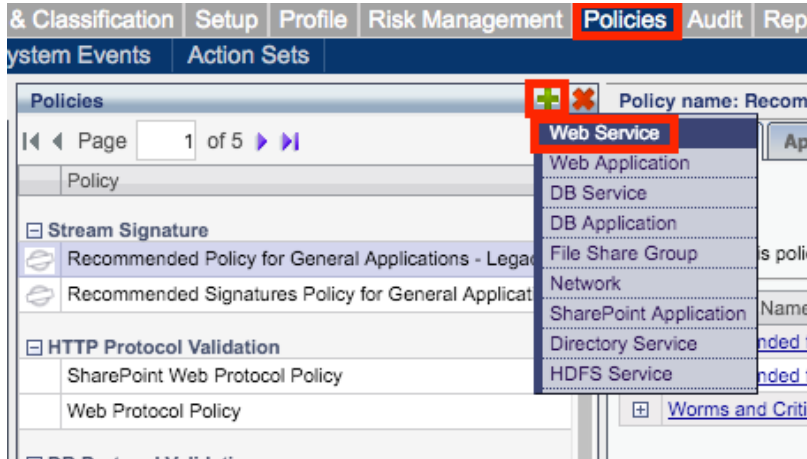
```
HC2-C03-29 # show port stats port-list 1/2/x13..x14
```

Counter Name	Port: 1/2/x13	Port: 1/2/x14
IfInOctets:	417297884	300405247
IfInUcastPkts:	340936	346260
IfInNUcastPkts:	322	171074
IfInPktDrops:	0	0
IfInDiscards:	5	5
IfInErrors:	0	0
IfInOctetsPerSec:	2638	3185
IfInPacketsPerSec:	15	29
IfOutOctets:	300369311	417322395
IfOutUcastPkts:	346122	341175
IfOutNUcastPkts:	171155	317
IfOutDiscards:	0	0
IfOutErrors:	0	0
IfOutOctetsPerSec:	3185	2638
IfOutPacketsPerSec:	29	15

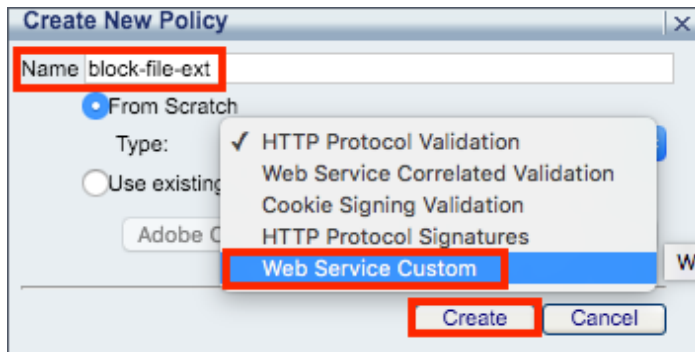
- Look at the IfInOctets stats in the column on the left. After the first **show stats** command the value was 417284603. After the second **show stats** command the value was 417297884, an increase of 13281 packets. Similar behavior can be seen in the stats in the column on the right.

Another way to verify that it is working is to create a blocking policy then test whether it works. To create a blocking policy, do the following:

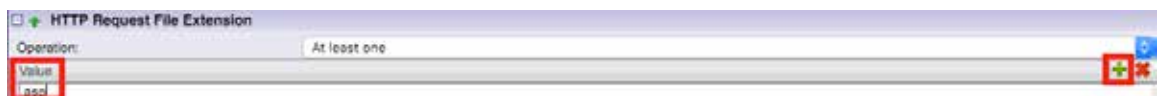
- From the SecureSphere MX GUI go to Policies



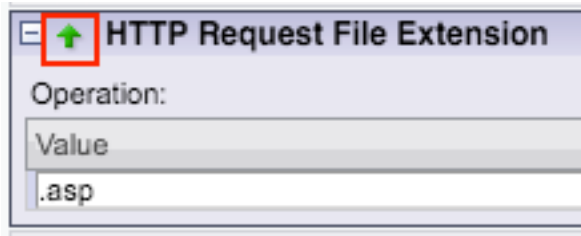
- Click the green plus sign to the right of **Policies**. Choose **Web Service**.



- Enter a name in the **Name** field (block-file-ext in this example). Select **Web Service Custom**, then under **Type**, click **Create**.
- Under Available Match Criteria find HTTP Request File Extension, click the plus sign to expand this.
- Click the green plus sign on the far right. For the Value enter a file extension (foo.asp in this example), and then click the green up arrow to move this up to the Match Criteria section.



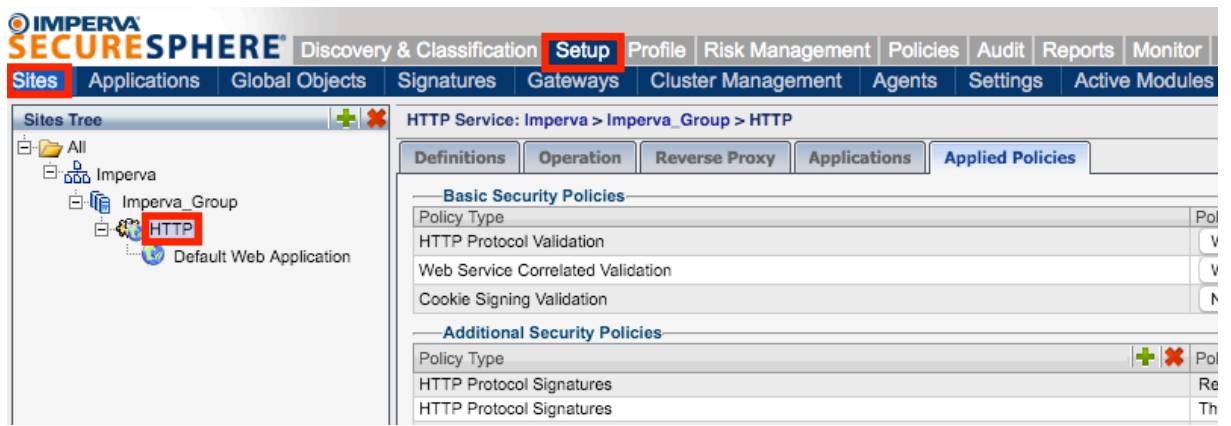
- Click the green up arrow to move this up to the Match Criteria section



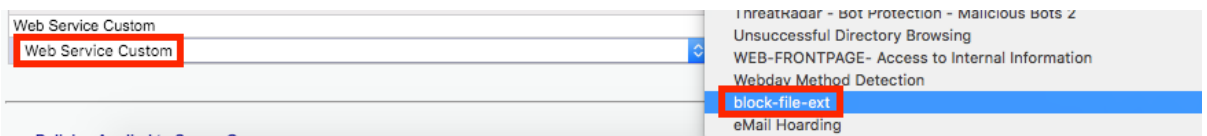
- Click Save.

Assign the Policy to the Imperva Gateways

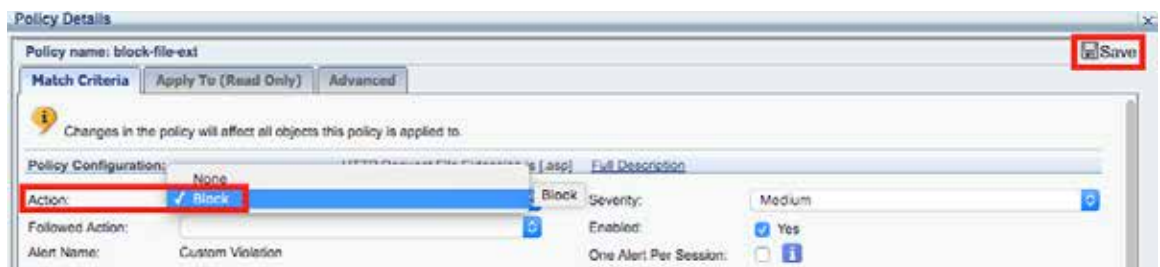
- From the SecureSphere MX GUI, select **Setup > Sites > HTTP**.



- From the Applied Policies tab click the green plus sign under Additional Security Policies.
- Scroll to the bottom of the screen and click the last rule. Choose **Web Service Custom**.
- Click in the field on the right and scroll to the bottom. Select **block-file-ext**.

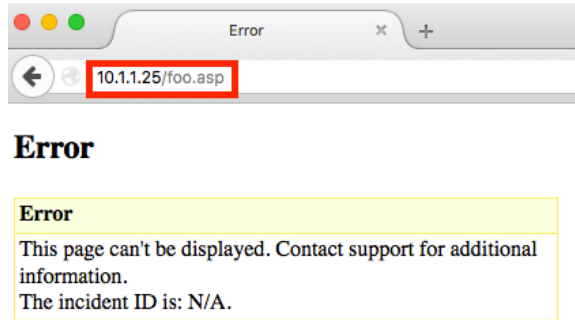


- Click **Save** at the top right.
- Find the new rule at the bottom of the screen and click the pencil to edit.
- Set the **Action** to **Block** and click **Save**.



Test the policy

1. Open a Web browser and connect to the site.
2. Attempt to open a page similar to the following (10.1.1.25/foo.asp in this example):



Notice that the content of this error page is different than what is normally returned by your Web server. That is because this error page is coming from the Imperva SecureSphere WAF appliance, not your Web server.

Make sure to delete the block-file-ext policy when testing is finished.

3 Summary and Conclusions

The previous chapters showed how to deploy Gigamon GigaVUE-HC2 bypass protection with Imperva SecureSphere WAF appliances. This combined solution using the Gigamon-GigaVUE-HC2 chassis achieves the following objectives:

- High availability of Imperva SecureSphere WAF because each inline security solution can be put into a Gigamon inline tool group with tool failover actions. The inline tool group can be optimized for each security need, regardless of whether the tool goes off-line due to an outage or planned maintenance.
- Traffic distribution to multiple Imperva SecureSphere WAF appliances for load sharing across the multiple instances
- Seamless scalability for an increasing network infrastructure as well as the inline security tools to accommodate the additional traffic.
- Ultimate flexibility of adding new types of inline security tools without physical change control because all new tools are physically added to the GigaVUE-HC2 and logically added to the path through traffic flow maps.

For more information on the GigaVUE-HC2 bypass protection, high availability, and scalability provided by Gigamon's Security Delivery Platform, go to www.gigamon.com.

How to get Help

For issues with Gigamon products, refer to <http://www.gigamon.com/support-and-services/contact-support> and your Support Agreement with Gigamon. You can also email Technical Support at support@gigamon.com.

For issues with Imperva products, refer to <https://www.imperva.com/Login>. You'll need to create a customer support portal account. You can also email Technical Support at support@imperva.com.

See Inside Your Network™

4062-02
11/16