Deploying FireEye® Inline with Gigamon

COPYRIGHT

TRADEMARK ATTRIBUTIONS

Contents

Chapter 1

Overview

Gigamon and FireEye offer a combined solution that meets today's active inline security needs. This solution can scale as the protected network infrastructure grows with the addition of network links. As the network grows, Gigamon provides inline tool groups for FireEye appliances to provide Security Service Assurance (SSA) for inline advanced malware protection. The FireEye inline tool group ensure that the inline security *service* remains available regardless of appliance maintenance or failure. Additionally, Gigmon's interface modules for network bypass protection provide network availability in the event of a power outage on the GigaVUE-HC2 nodes.

The solution tested and described in this guide is based on a standard active inline network and tool deployment where two or more FireEye Network Threat Prevention Platform (NX Series) appliances are directly cabled to one GigaVUE-HC2 chassis. Upon full deployment, the GigaVUE-HC2 sends only the traffic of interest to the FireEye inline tool group for malware inspection.

The solution described in this guide was tested with one GigaVUE-HC2 four module node and two FireEye NX 2400 advanced malware protection appliances.

This chapter covers the following:

- *Deployment Prerequisites*
- *Architecture Overview*
- *Access Credentials*

Deployment Prerequisites

The Gigamon plus FireEye Scalable Service Assurance (SSA) solution consists of the following:

- GigaVUE-HC2 chassis with GigaVUE-OS 4.4.01, one TAP-HC0/G24/MB and one GigaSMART SMT-HC0-X16 module.
- GigaVUE-FM version 3.1 for GigaVUE-HC2 GUI configuration
- Two FireEye appliances, model FireEye NX 2400. This includes the following:
  - Software version 7.6.0
  - Content version 404.150
  - IPMI version 2.67
  - Guest image Information: Winxp Sp3, Win7X64 Sp1, Win7 Sp1 - 15.0210

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 node with two FireEye Network Security (NX) appliances. The reference architecture in Figure 1-1 shows this each component's position in the overall network infrastructure, where all network components and inline security tools are connected directly to the GigaVUE-HC2.

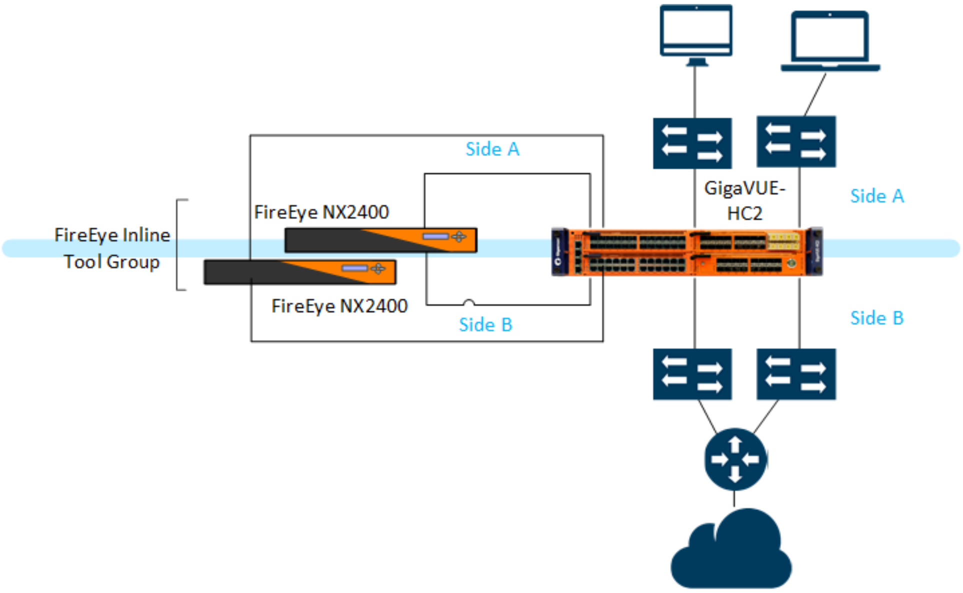


Figure 1-1: Gigamon Inline Bypass with FireEye NX

Notice in Figure 1-1 that there is a *sidedness* to the architecture because data flows to and from side A where the clients reside to side B where the Internet and resources they request reside.

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 FireEye devices of the inline tool group.

Access Credentials

The default access credentials for the Gigamon GigaVUE-FM and FireEye NX 2400s are as follows:

- Gigamon GigaVUE-FM access defaults:
  - Username: admin
  - Password: admin123A!
  - There is no default management IP address
- FireEye NX 2400 access defaults:
  - Username: admin
  - Password: admin
  - 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-HC with Giga-VUE-FM. For the equivalent H-VUE and CLI configuration commands, refer to the *Gigamon-OS H-VUE User's Guide and GigaVUE-OS CLI User's Guide* respectively for the 4.4.01 release.

Chapter 2

Configurations

This chapter describes the configuration procedures for the GigaVUE-HC2 and FireEye NX 2400, a inline tool group solution through the FireEye GUI and Gigamon-OS H-VUE. The procedures are organized as follows:

- *FireEye NX 2400 Configuration: Inline Tools*
- *Gigamon GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups*

The FireEye GUI procedures focus on FireEye inline block operational mode. The configuration procedures will configure the GigaVUE-HC2 to send live traffic to the FireEye inline tool group, which will allow the use of FireEye's on-system deployment testing tools.

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

NOTE: This chapter assumes the FireEye appliances are directly connected to the GigaVUE-HC2 as shown in Figure 1-1. All GigaVUE-HC2 ports that FireEye appliances are connected to should be configured as port type *Inline Tool*. Furthermore, all GigaVUE-HC2 inline bypass ports that the network devices are connected to should be configured as *Inline Network* type ports. For specific instructions on how to complete these tasks, refer to the Help Topics links in H-VUE.

FireEye NX 2400 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.

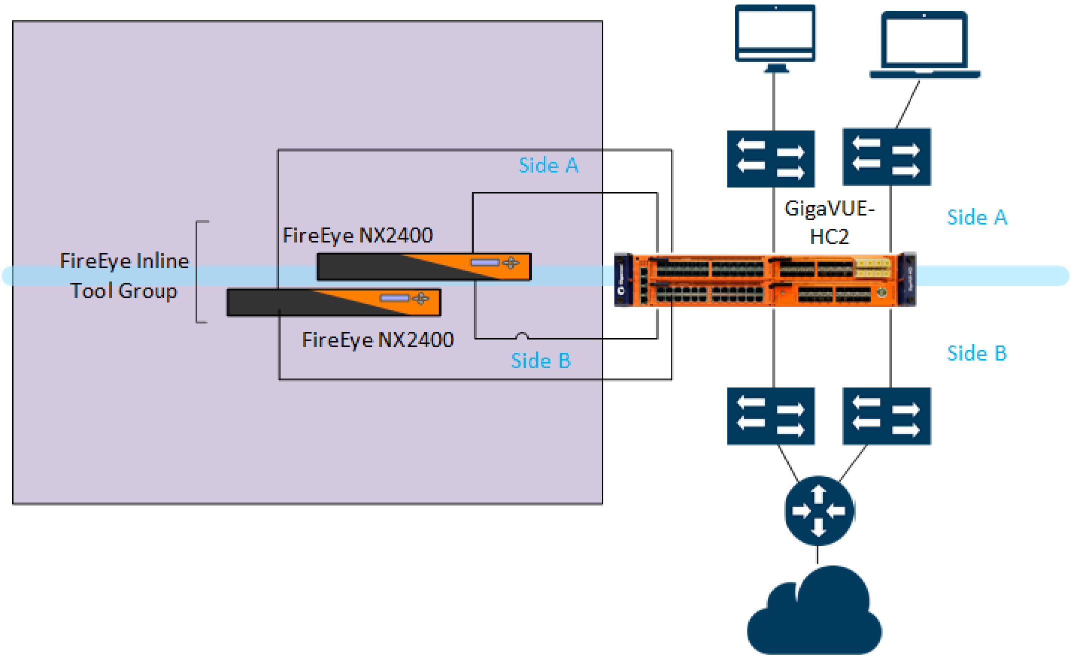
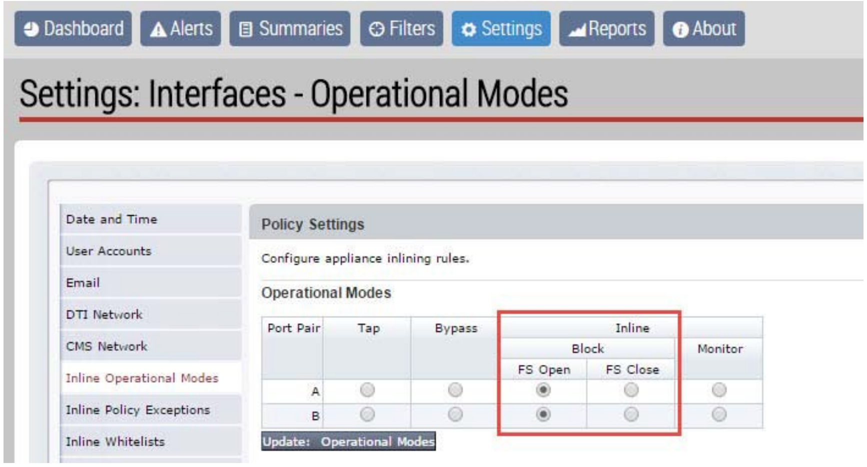


Figure 2-1: FireEye NX 2400 inline Tools

Configuring FireEye for Inline Block Operation Mode

To individually configure FireEye NX 2400 to block traffic so it detects malicious traffic, do the following steps for each FireEye appliance:

1. In the FireEye GUI, select **Settings > Inline Operational Modes**.
2. In the **Policy Settings** section, select the radio button under the **Inline > Block > FS Open** column for both Port Pair A and B as shown in Figure 2-2.



Settings: Interfaces - Operational Modes

Policy Settings

Configure appliance inlining rules.

Operational Modes

Port Pair	Tap	Bypass	Inline		Monitor
			Block		
			FS Open	FS Close	
A	○	○	●	○	○
B	○	○	●	○	○

Update: Operational Modes

Figure 2-2: Inline Block Operational Mode on FireEye Appliance

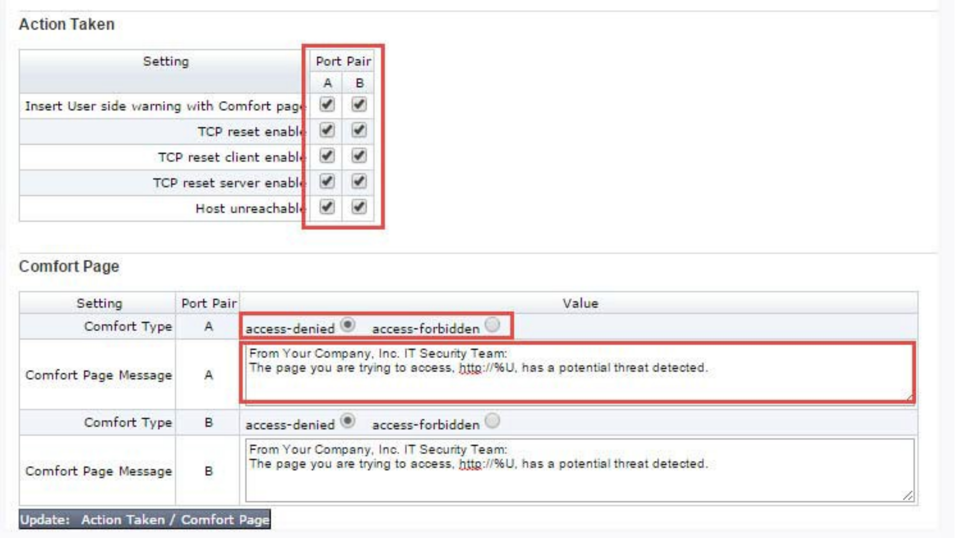
3. Click **Update: Operational Modes**.

Configuring FireEye Actions Taken: Comfort Page, TCP Resets

FireEye NX has several options for actions to be taken when malicious content is detected. The following procedure walks you through the steps for sending a customized comfort page to the client and TCP resets to client and server. These steps are optional.

To set the Actions Take and Comfort Page, do the following:

1. In the **Actions Taken** section of Policy Settings page, check all boxes for Comfort page and TCP resets for both Port Pair A and B as show in Figure 2-3.
2. In the **Comfort Type** section of the Policy Settings page, leave the radio button set to **access-denied** (HTTP response code 401), unless you have a preference for **access-forbidden** (HTTP response code 403).
3. In the **Comfort Page** section, type a customized message in the **Comfort Page Message** dialog box for Port Pair A and B.
4. Click **Update: Action Taken / Comfort Page**.



Action Taken

Setting	Port Pair	
	A	B
Insert User side warning with Comfort pag	☑	☑
TCP reset enabl	☑	☑
TCP reset client enabl	☑	☑
TCP reset server enabl	☑	☑
Host unreachabl	☑	☑

Comfort Page

Setting	Port Pair	Value
Comfort Type	A	access-denied ● access-forbidden ○
Comfort Page Message	A	From Your Company, Inc. IT Security Team: The page you are trying to access, http://%U, has a potential threat detected.
Comfort Type	B	access-denied ● access-forbidden ○
Comfort Page Message	B	From Your Company, Inc. IT Security Team: The page you are trying to access, http://%U, has a potential threat detected.

Figure 2-3: FireEye Action Taken/Comfort Page Customization

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. 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 FireEye Inline Tool*

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

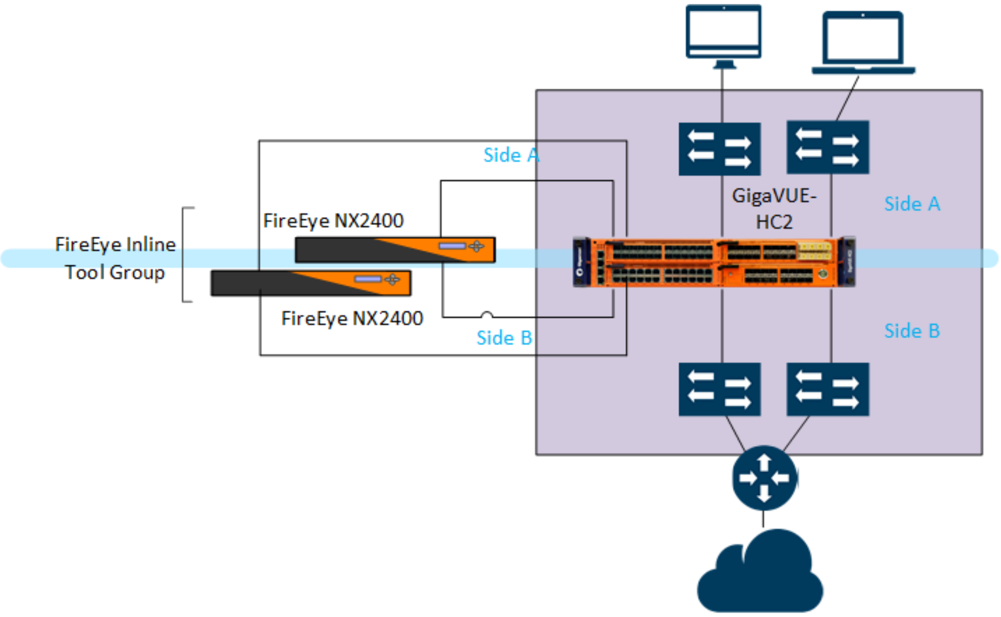


Figure 2-4: Gigamon GigaVUE-HC2 Configurations

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 company architecture grows, additional inline network pairs can be added 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*

The steps described in this section assume that you are logged in to GigaVUE-FM, selected **Physical Nodes** in the left pane and then select the GigaVUE-HC2 on the Physical Nodes page.

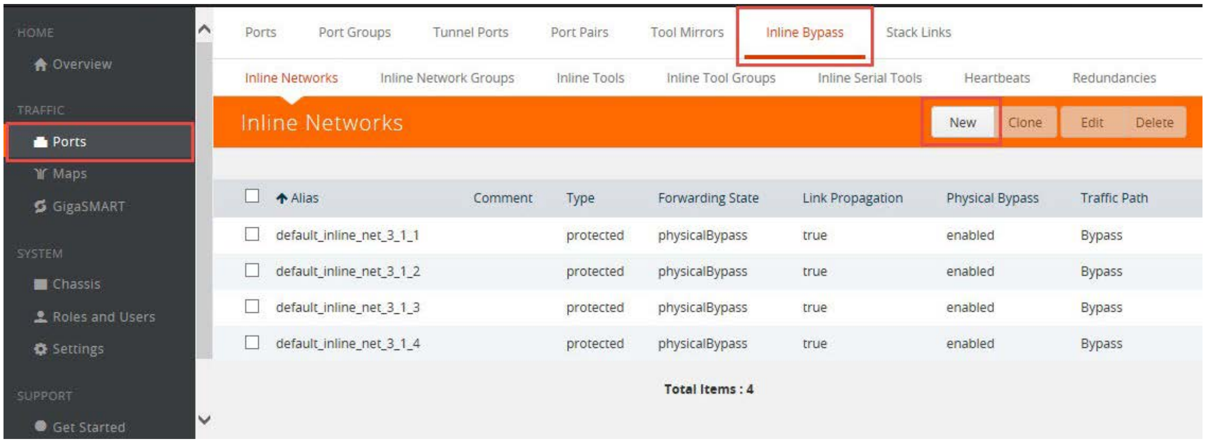
NOTE: This section assumes all the ports that the network devices are connected to are set as Inline Network port types. For specific instructions on completing these tasks, refer to Help Topics links in the H-VUE or the *Gigamon-OS H-VUE User's Guide*.

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 **Ports > Inline Bypass > Inline Networks**.

NOTE: If there is a bypass combo module in the GigaVUE-HC2, there will be four preconfigured Inline Network port pairs as shown in Figure 2-5. If you are using BPS ports, the step will be similar to those covered but limited. Notably you will not be able to change the alias and port A and B are preselected. If your network is 1G or 10G fiber, use one of these preconfigured inline bypass pairs. Otherwise, go to step 2.



□	Alias	Comment	Type	Forwarding State	Link Propagation	Physical Bypass	Traffic Path
□	default_inline_net_3_1_1		protected	physicalBypass	true	enabled	Bypass
□	default_inline_net_3_1_2		protected	physicalBypass	true	enabled	Bypass
□	default_inline_net_3_1_3		protected	physicalBypass	true	enabled	Bypass
□	default_inline_net_3_1_4		protected	physicalBypass	true	enabled	Bypass

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.

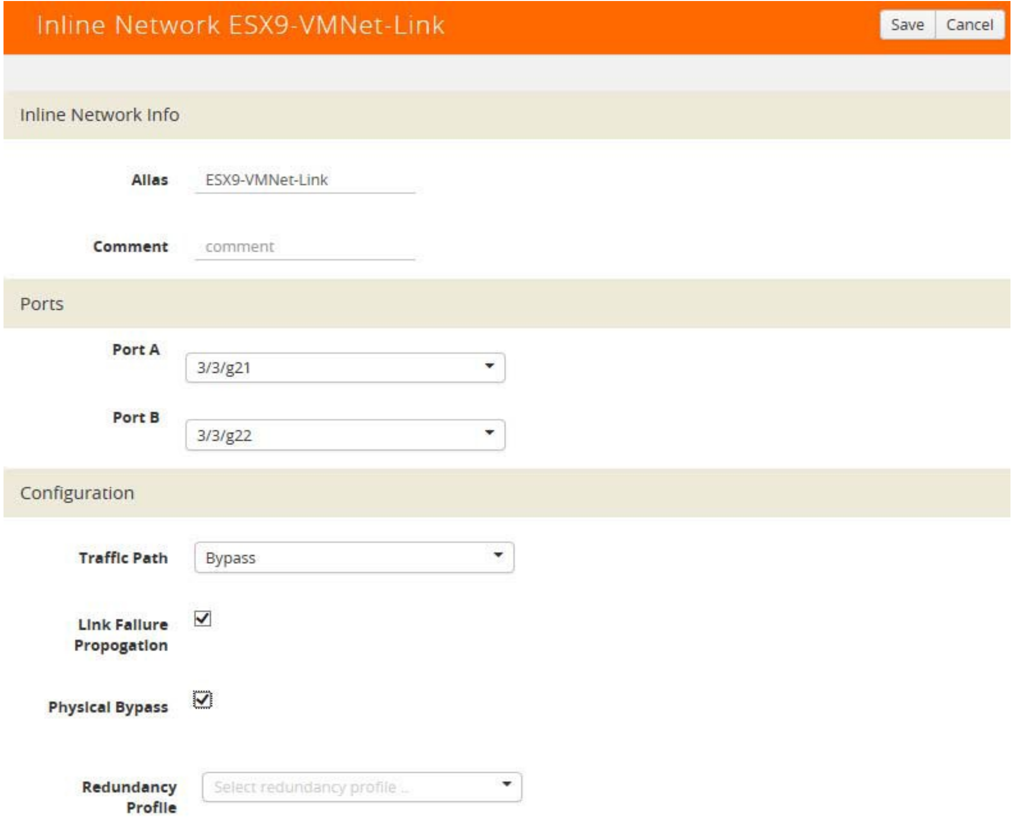
   - In the **Alias** field, type an alias that will help you remember which network link this Inline Network bypass pair represents. For example, `ESX9-VMNet-Link`.
   - Select the port for **Port A** by using the drop-down list or by typing the port label in the Port A field for the A Side port as it 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 HC2 match the Side A and B of the NX 2400 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.



Inline Network ESX9-VMNet-Link

Inline Network Info

Alias: ESX9-VMNet-Link

Comment: comment

Ports

Port A: 3/3/g21

Port B: 3/3/g22

Configuration

Traffic Path: Bypass

Link Failure Propogation: ☑

Physical Bypass: ☑

Redundancy Profile: Select redundancy profile ...

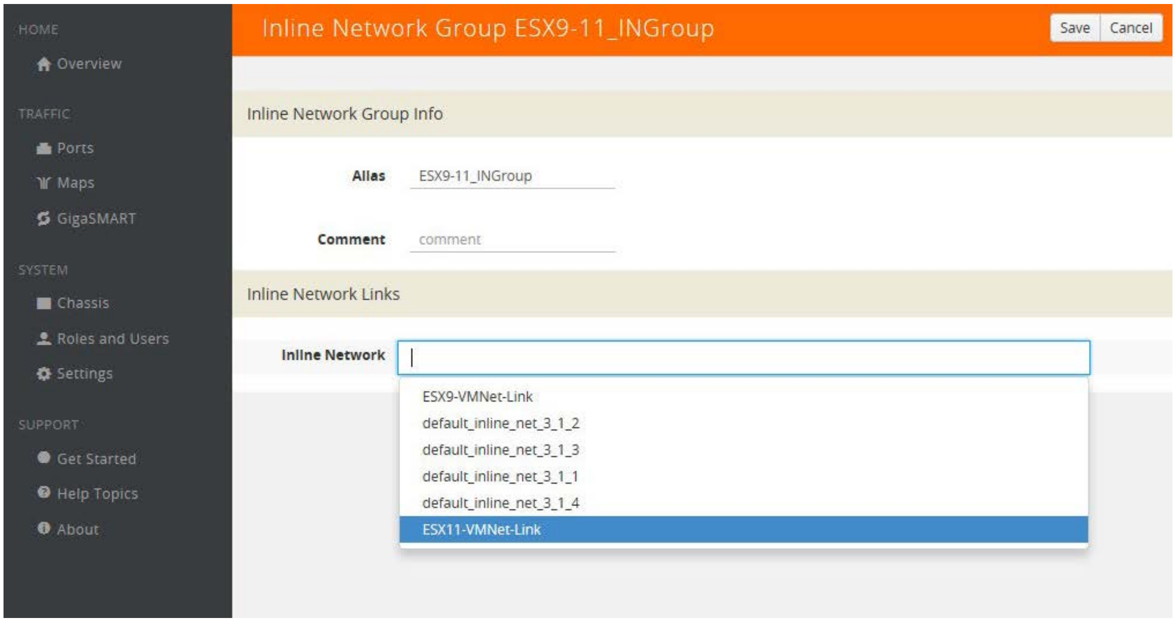
Figure 2-6: Inline Network Pair Configuration

6. Repeat step 2 and 3 for all other network links.

Step 2: Configure the Inline Network Group

To configure the inline network group, do the following:

1. In H-VUE, select **Ports > Inline Bypass > Inline Network Groups**.
2. Click **New**.
3. In the **Alias** field, type an alias that represents the inline network group. For example, `ESX9-11_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 you want to add to the Inline Network Group.



Inline Network Group ESX9-11_INGroup

Inline Network Group Info

Alias: ESX9-11_INGroup

Comment: comment

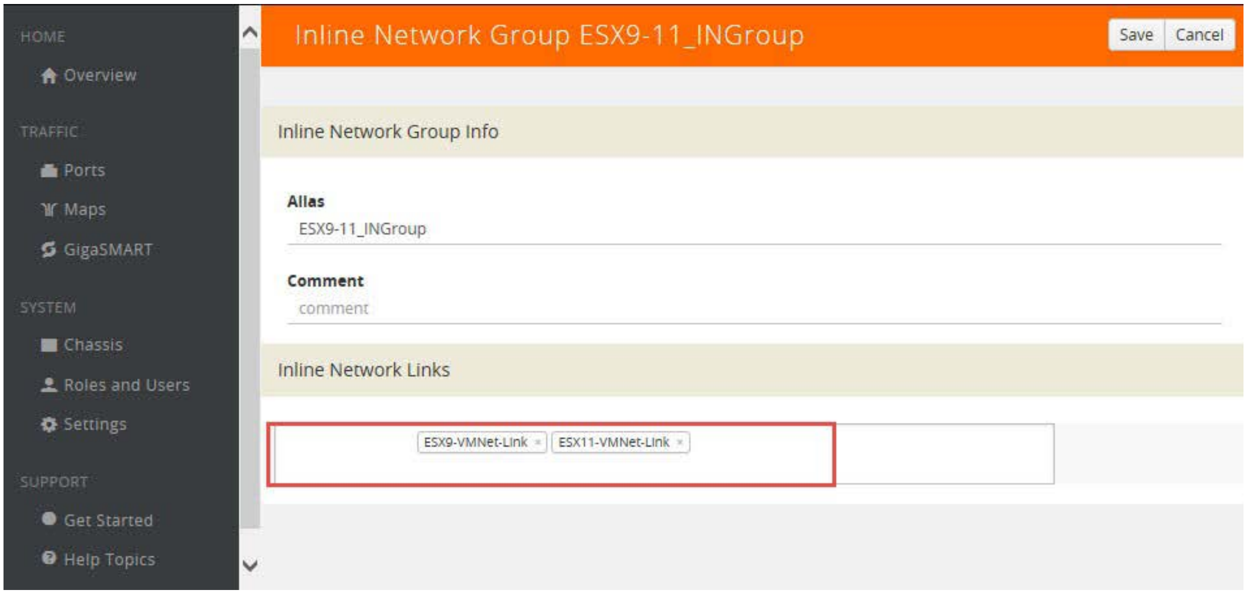
Inline Network Links

Inline Network:

ESX9-VMNet-Link
default_inline_net_3_1_2
default_inline_net_3_1_3
default_inline_net_3_1_1
default_inline_net_3_1_4
ESX11-VMNet-Link

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.



Inline Network Group ESX9-11_INGroup

Inline Network Group Info

Alias
ESX9-11_INGroup

Comment
comment

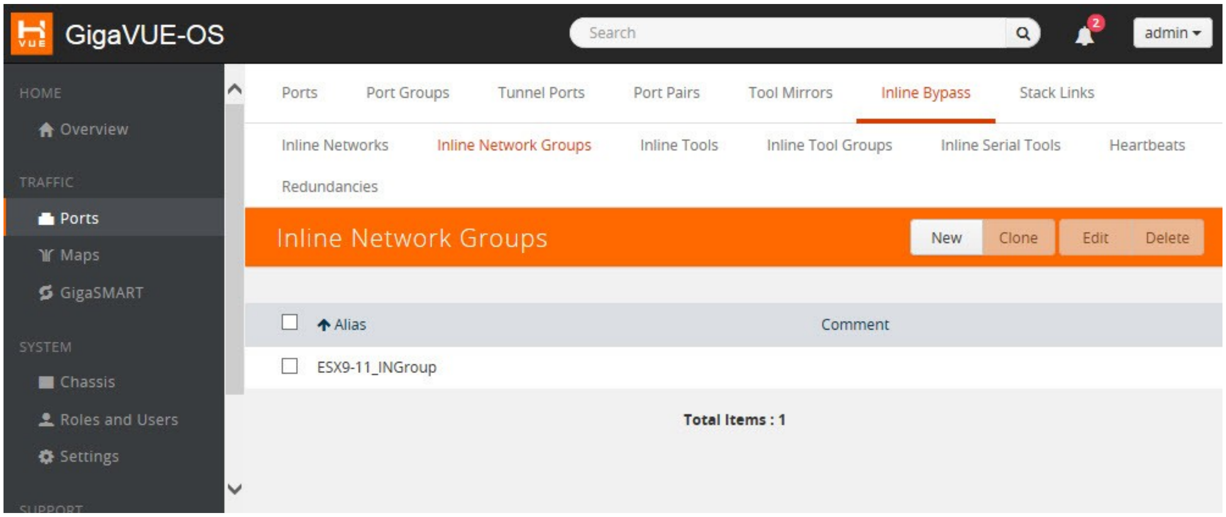
Inline Network Links

ESX9-VMNet-Link × ESX11-VMNet-Link ×

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.



□	Alias	Comment
□	ESX9-11_INGroup	

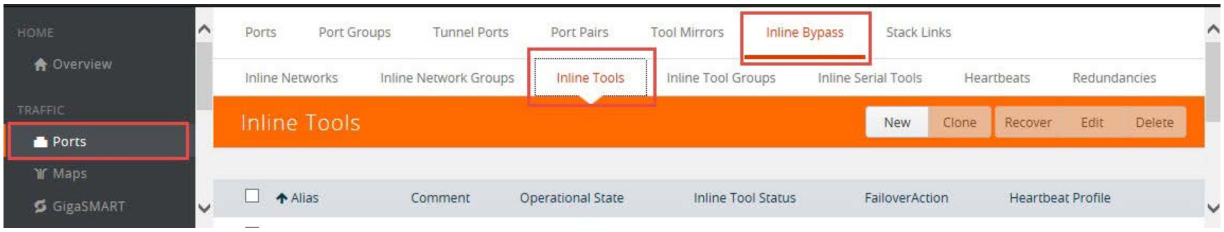
Total Items : 1

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 subsequent steps.

1. In H-VUE, select **Ports > Inine Bypass > Inline Tools**.



□	Alias	Comment	Operational State	Inline Tool Status	FailoverAction	Heartbeat Profile

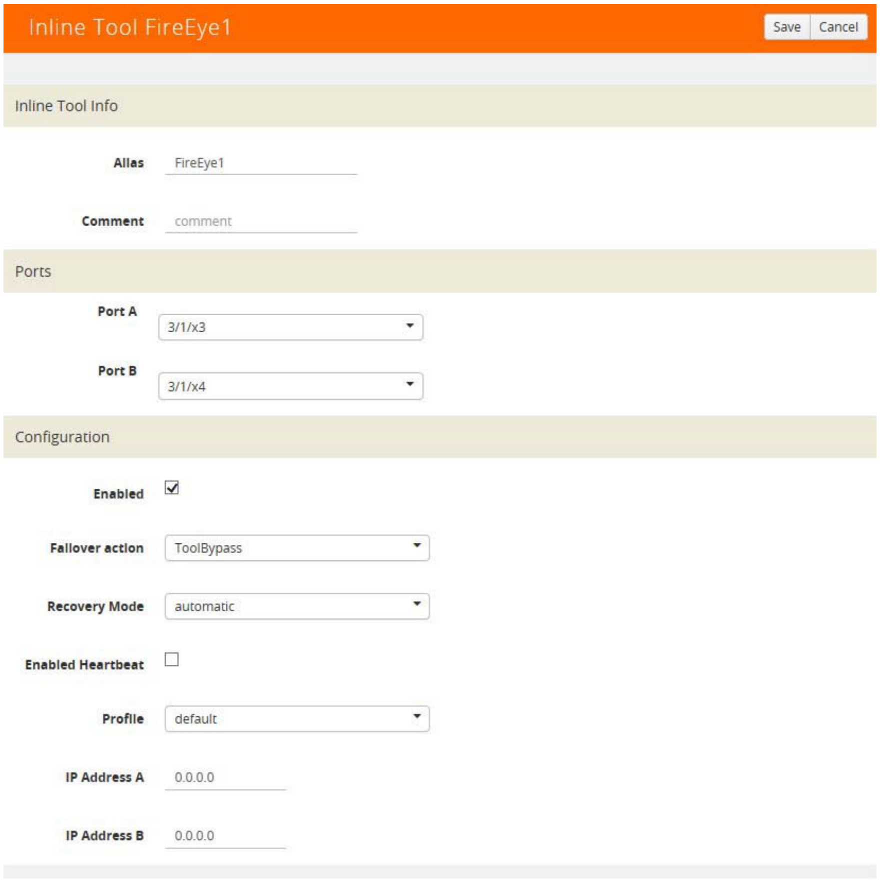
Figure 2-10: Navigating to the Inline Tools page

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, `FireEye1`.
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.



Inline Tool FireEye1

Inline Tool Info

Alias: FireEye1

Comment: comment

Ports

Port A: 3/1/x3

Port B: 3/1/x4

Configuration

Enabled ☑

Failover action: ToolBypass

Recovery Mode: automatic

Enabled Heartbeat ☐

Profile: default

IP Address A: 0.0.0.0

IP Address B: 0.0.0.0

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. Because 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

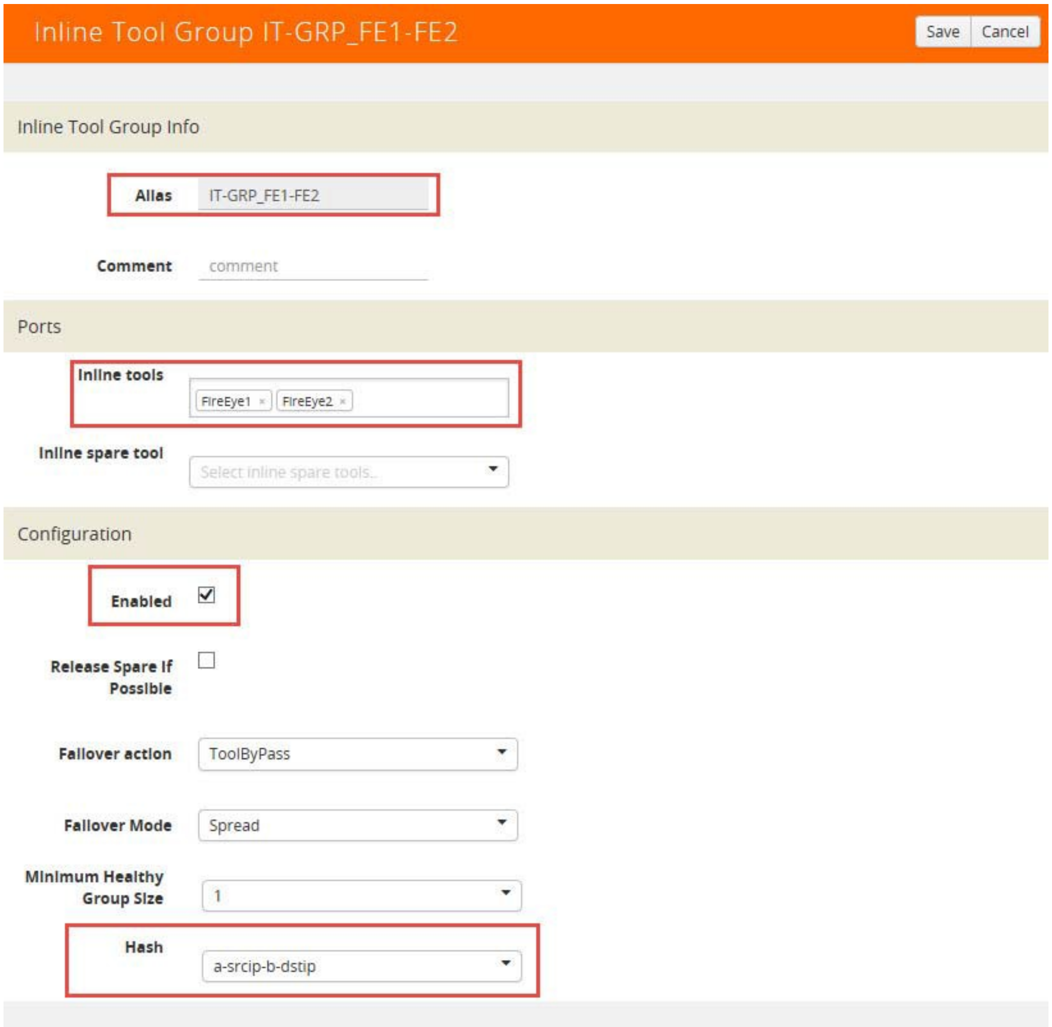
To configure the inline tool group, do the following:

1. In H-VUE, select **Ports > 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_FE1-FE2`.
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_FE1-FE2

Inline Tool Group Info

Alias: IT-GRP_FE1-FE2

Comment: comment

Ports

Inline tools: FireEye1 × FireEye2 ×

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 FireEye tool group allowing you to test the deployment functionality of the FireEye appliances within the group. This will be 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 FireEye appliances. The test procedure is described in *Testing the Functionality of the FireEye Inline Tool* on page 26.

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

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

1. In H-VUE, 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:

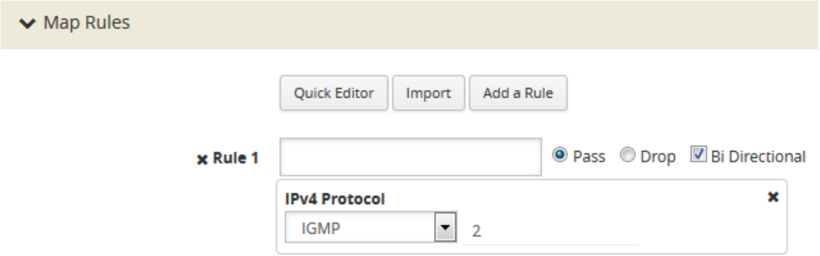
   a. Click in the Condition search field for the Rule and select **ip4Proto** from the drop-down list.

   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.



Rule 1 ● Pass ○ Drop ☑ Bi Directional

IPv4 Protocol: IGMP 2

Figure 2-13: Rule for Inline Tool Flow Map

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

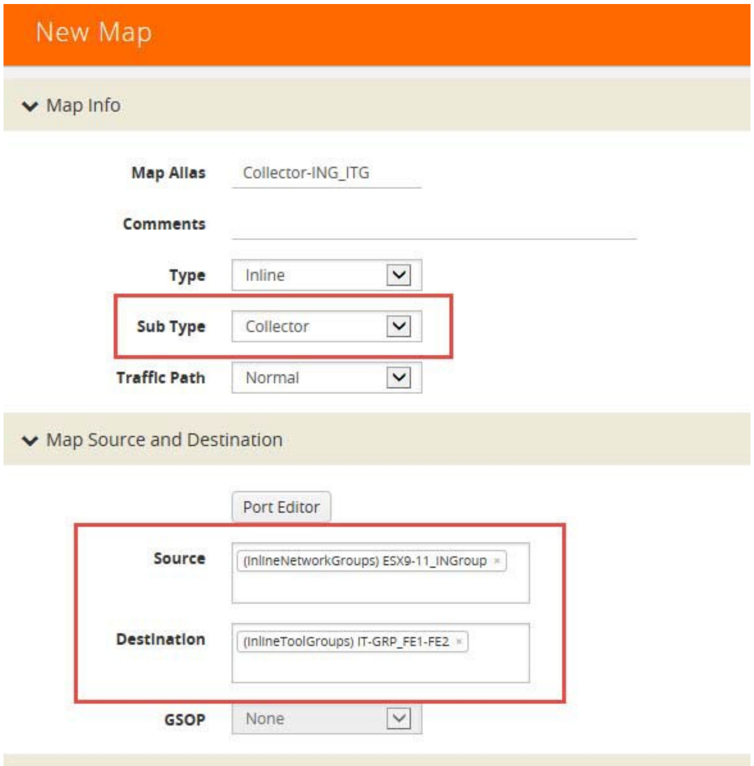
7. Click **Save**.

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:

1. in H-VUE, 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*.



Map Alias: Collector-ING_ITG

Comments:

Type: Inline

Sub Type: Collector

Traffic Path: Normal

Source: (InlineNetworkGroups) ESX9-11_INGroup ×

Destination: (InlineToolGroups) IT-GRP_FE1-FE2 ×

GSOP: None

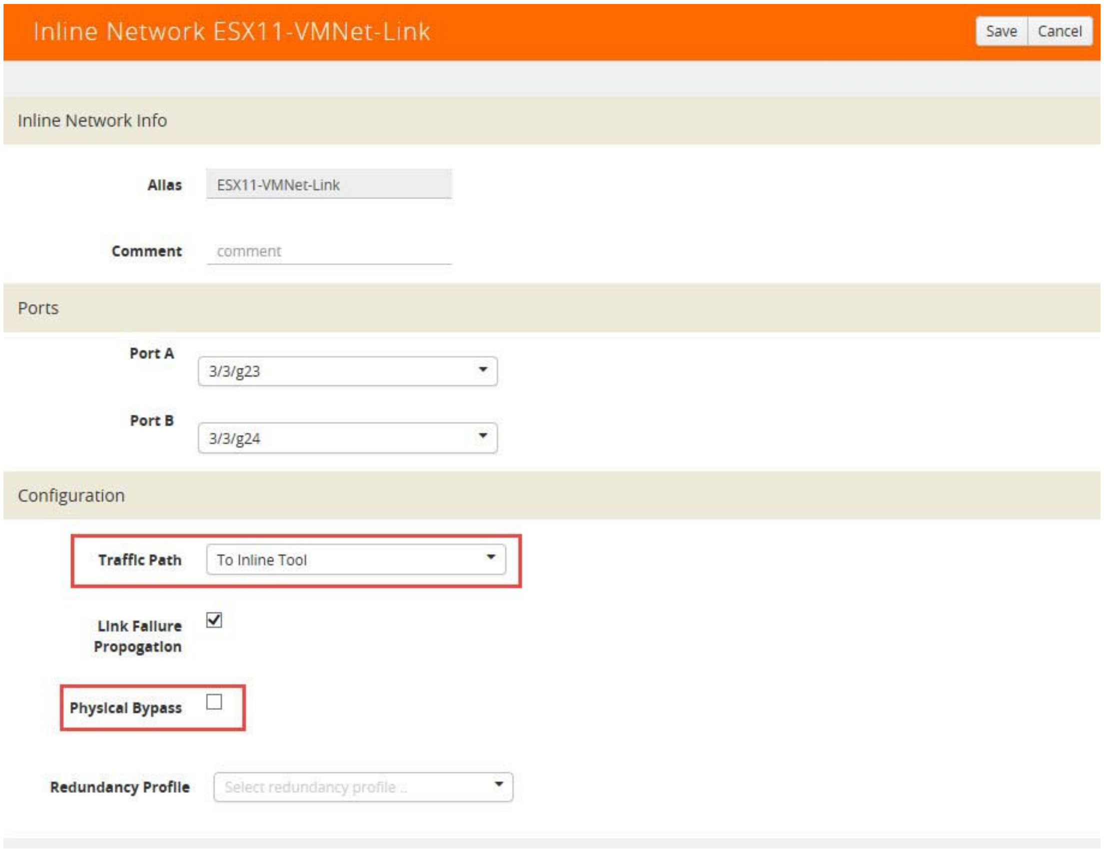
Figure 2-14: Configuration for Collector Map

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 H-VUE by selecting **Chassis** from the main navigation pane.

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

1. In H-VUE, select **Ports > 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 ESX11-VMNet-Link

Inline Network Info

Alias: ESX11-VMNet-Link

Comment: comment

Ports

Port A: 3/3/g23

Port B: 3/3/g24

Configuration

Traffic Path: To Inline Tool

Link Failure Propogation ☑

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.

Testing the Functionality of the FireEye Inline Tool

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

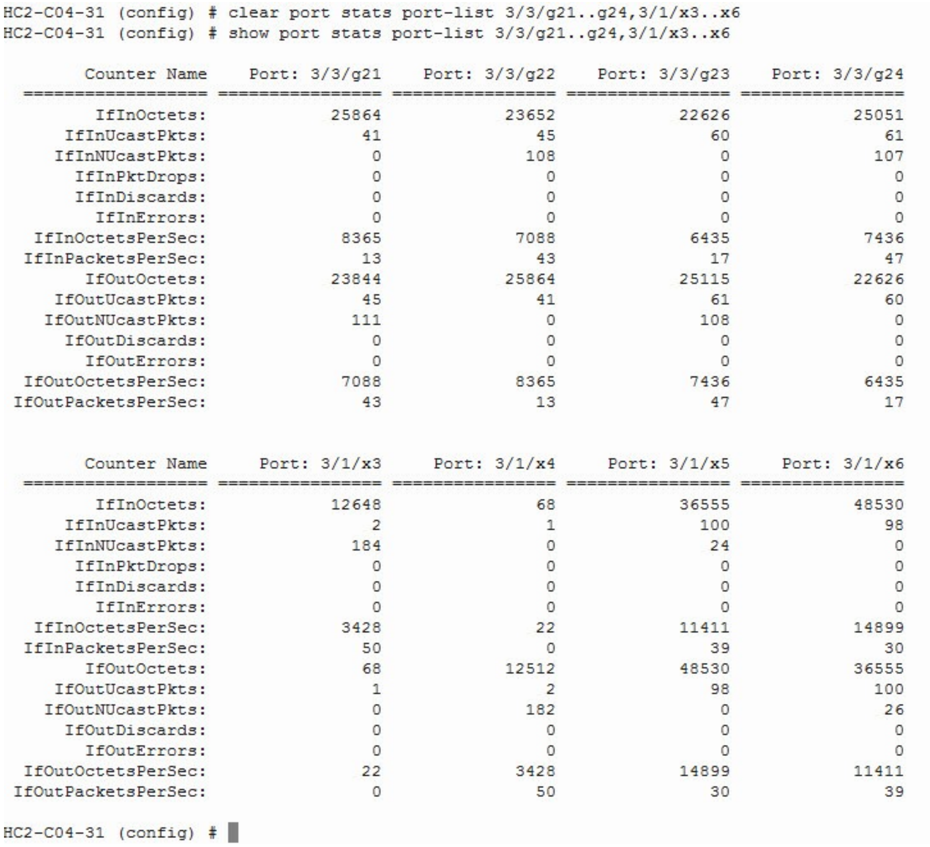
1. Get the statistics for the inline network and the inline tool ports from the GigaVUE-HC2.

   a. Launch a serial console or SSH session to the GigaVUE-HC2.

   b. Log in as admin and enter the following commands at the command prompt (HC2>), where the port lists in the command are the inline network and inline tool ports:

   HC2 > en
   HC2 # config t
   HC2 (config) # clear port stats port-list
   3/3/g21..g24,3/1/x3..x6 HC2 (config) # show port stats
   port-list 3/3/g21..g24,3/1/x3..x6

   After entering the show port command, you should see the port statistics for the specified port list similar to the example shown in *Inline Network Pair Configuration*

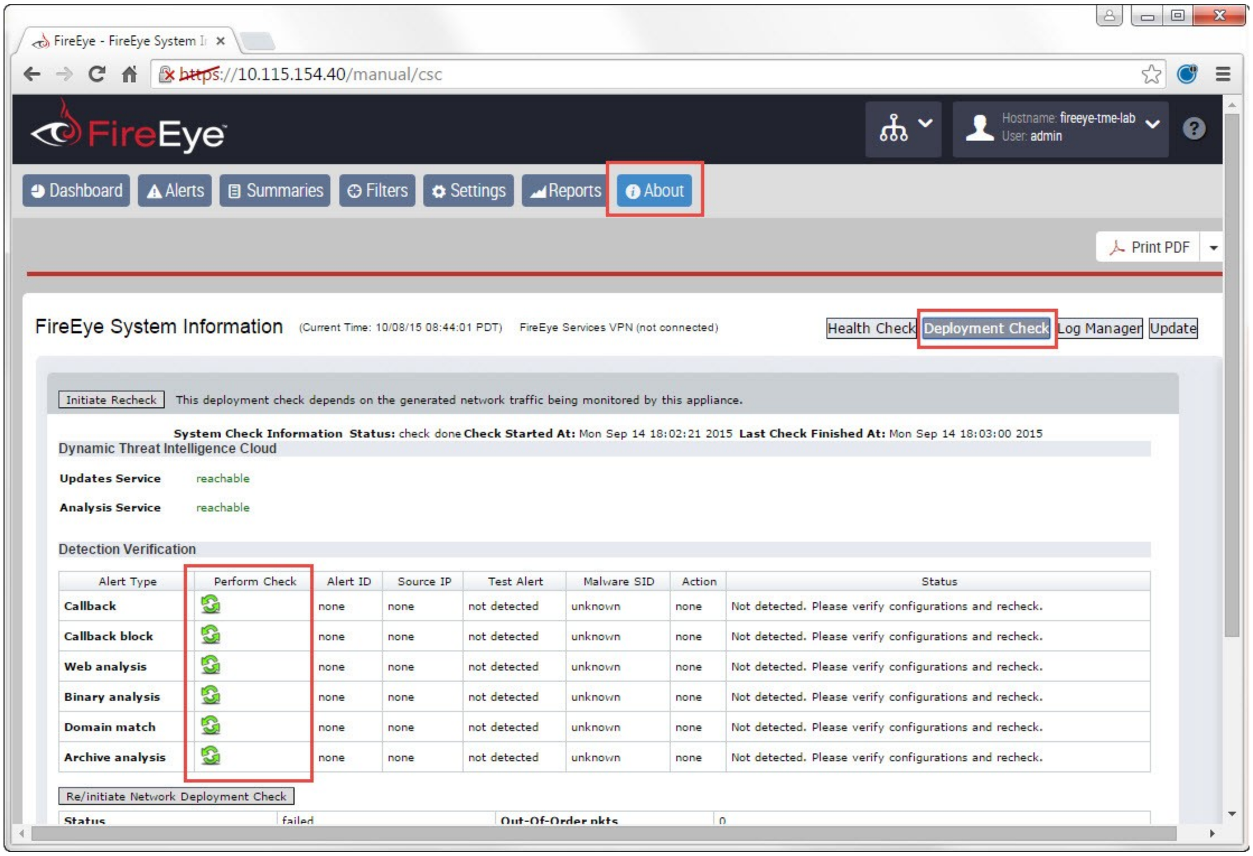


```
HC2-C04-31 (config) # clear port stats port-list 3/3/g21..g24,3/1/x3..x6
HC2-C04-31 (config) # show port stats port-list 3/3/g21..g24,3/1/x3..x6

       Counter Name    Port: 3/3/g21    Port: 3/3/g22    Port: 3/3/g23    Port: 3/3/g24
 ================== ================ ================ ================ ================
        IfInOctets:            25864            23652            22626            25051
     IfInUcastPkts:               41               45               60               61
    IfInNUcastPkts:                0              108                0              107
      IfInPktDrops:                0                0                0                0
      IfInDiscards:                0                0                0                0
        IfInErrors:                0                0                0                0
  IfInOctetsPerSec:             8365             7088             6435             7436
 IfInPacketsPerSec:               13               43               17               47
       IfOutOctets:            23844            25864            25115            22626
    IfOutUcastPkts:               45               41               61               60
   IfOutNUcastPkts:              111                0              108                0
     IfOutDiscards:                0                0                0                0
       IfOutErrors:                0                0                0                0
 IfOutOctetsPerSec:             7088             8365             7436             6435
IfOutPacketsPerSec:               43               13               47               17


       Counter Name     Port: 3/1/x3     Port: 3/1/x4     Port: 3/1/x5     Port: 3/1/x6
 ================== ================ ================ ================ ================
        IfInOctets:            12648               68            36555            48530
     IfInUcastPkts:                2                1              100               98
    IfInNUcastPkts:              184                0               24                0
      IfInPktDrops:                0                0                0                0
      IfInDiscards:                0                0                0                0
        IfInErrors:                0                0                0                0
  IfInOctetsPerSec:             3428               22            11411            14899
 IfInPacketsPerSec:               50                0               39               30
       IfOutOctets:               68            12512            48530            36555
    IfOutUcastPkts:                1                2               98              100
   IfOutNUcastPkts:                0              182                0               26
     IfOutDiscards:                0                0                0                0
       IfOutErrors:                0                0                0                0
 IfOutOctetsPerSec:               22             3428            14899            11411
IfOutPacketsPerSec:                0               50               30               39

HC2-C04-31 (config) # █
```

Figure 2-16: Inline Network and Inline Tool Port Statistics

2. The following steps need to be repeated from five or more workstations with sequentially increasing IP addresses. For example, from IP address 10.10.10.21 to 10.10.10.26. This is to make sure that the distribution of FireEye deployment test traffic is as even as possible across the members of the FireEye inline tool group.
   a. Launch a browser on a workstation that will pass traffic through one of the inline network links within your inline network tool group. Log in as admin to one of the FireEye appliances through the GUI.
   b. Select **About > Deployment Check**.
   c. Click each of the Detection Verification Perform Check links a shown in Figure 2-17.

NOTE: You should see a series of client response pages that correspond to each test including the deployment test and callback block as shown in Figure 2-18.



FireEye System Information (Current Time: 10/08/15 08:44:01 PDT) FireEye Services VPN (not connected)

This deployment check depends on the generated network traffic being monitored by this appliance.

System Check Information **Status:** check done **Check Started At:** Mon Sep 14 18:02:21 2015 **Last Check Finished At:** Mon Sep 14 18:03:00 2015

Dynamic Threat Intelligence Cloud

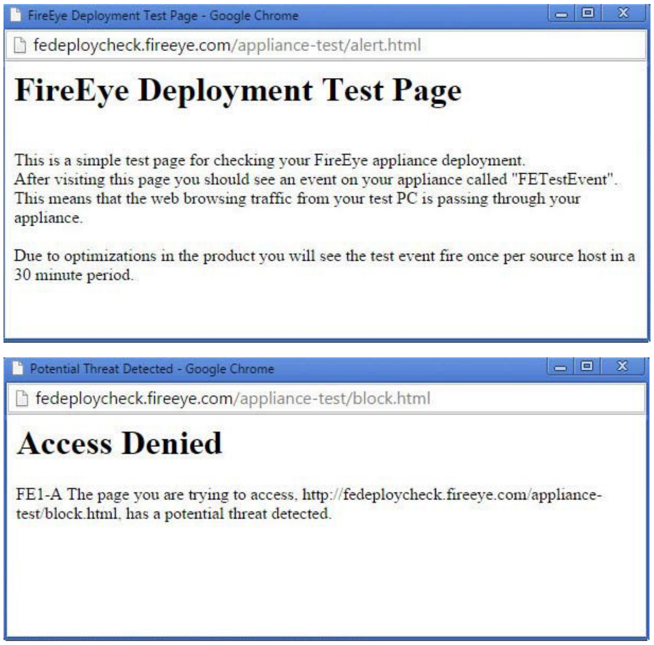
Updates Service	reachable
Analysis Service	reachable

Detection Verification

Alert Type	Perform Check	Alert ID	Source IP	Test Alert	Malware SID	Action	Status
Callback	↻	none	none	not detected	unknown	none	Not detected. Please verify configurations and recheck.
Callback block	↻	none	none	not detected	unknown	none	Not detected. Please verify configurations and recheck.
Web analysis	↻	none	none	not detected	unknown	none	Not detected. Please verify configurations and recheck.
Binary analysis	↻	none	none	not detected	unknown	none	Not detected. Please verify configurations and recheck.
Domain match	↻	none	none	not detected	unknown	none	Not detected. Please verify configurations and recheck.
Archive analysis	↻	none	none	not detected	unknown	none	Not detected. Please verify configurations and recheck.

Status	failed	**Out-Of-Order pkts**	0

Figure 2-17: FireEye Deployment Test Page


FireEye Deployment Test Page - Google Chrome
fedeploycheck.fireeye.com/appliance-test/alert.html

FireEye Deployment Test Page

This is a simple test page for checking your FireEye appliance deployment.
After visiting this page you should see an event on your appliance called "FETestEvent".
This means that the web browsing traffic from your test PC is passing through your appliance.

Due to optimizations in the product you will see the test event fire once per source host in a 30 minute period.

Potential Threat Detected - Google Chrome
fedeploycheck.fireeye.com/appliance-test/block.html

Access Denied

FE1-A The page you are trying to access, http://fedeploycheck.fireeye.com/appliance-test/block.html, has a potential threat detected.

Figure 2-18: Response Pages for FireEye Deployment Test Client

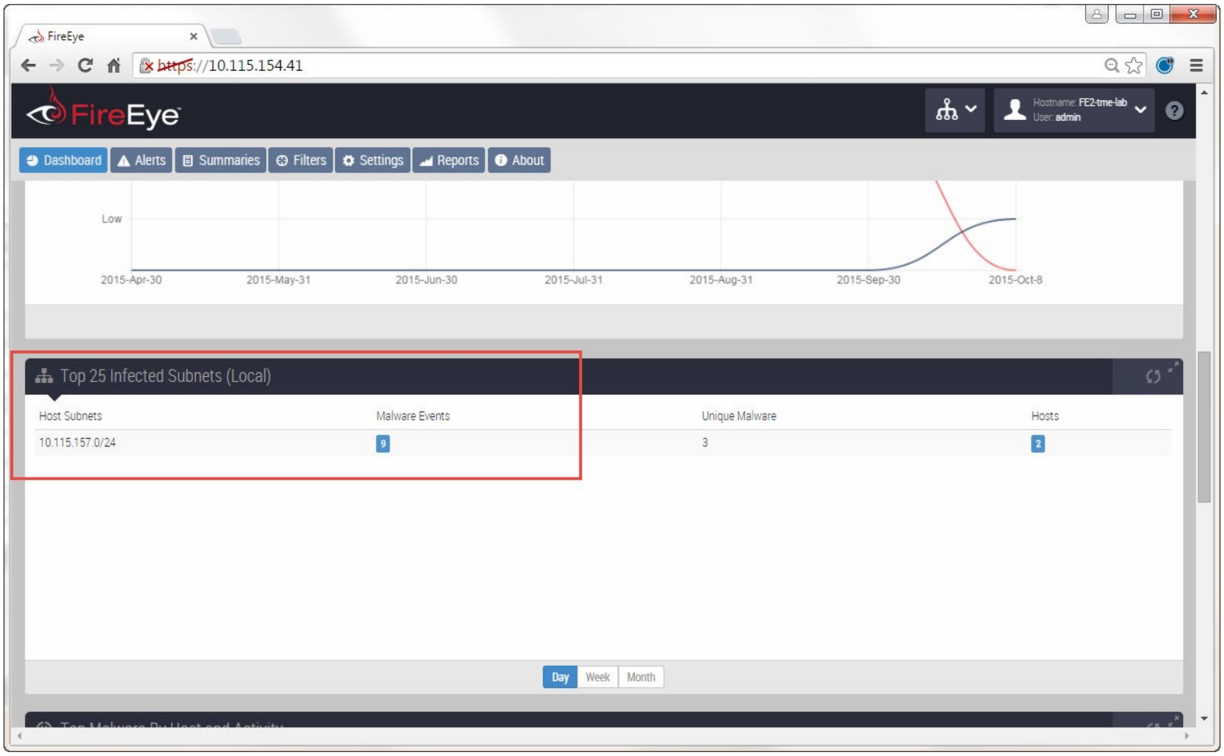
d. Repeat these tests from at least four other workstations with sequential IP addresses as described in the previous note.

e. Log into each FireEye appliance. You will see the spread of test alerts across those systems.

f. Go to the SSH or serial console of your GigaVUE-HC2 to see the packet distribution across the inline tool ports by using the **show port stats** command. You should see that all traffic from any given client IP goes to only one FireEye appliance as the stated best practice from FireEye.

NOTE: Traffic distribution may not be even across all inline tools because the data itself is a factor in the amount of data sent to each inline tool. This means some sessions inherently have more data associated with them than others.

g. Log in to each FireEye appliance, and then scroll down the Dashboard to Top 25 Infected Subnets as shown in Figure 2-19.

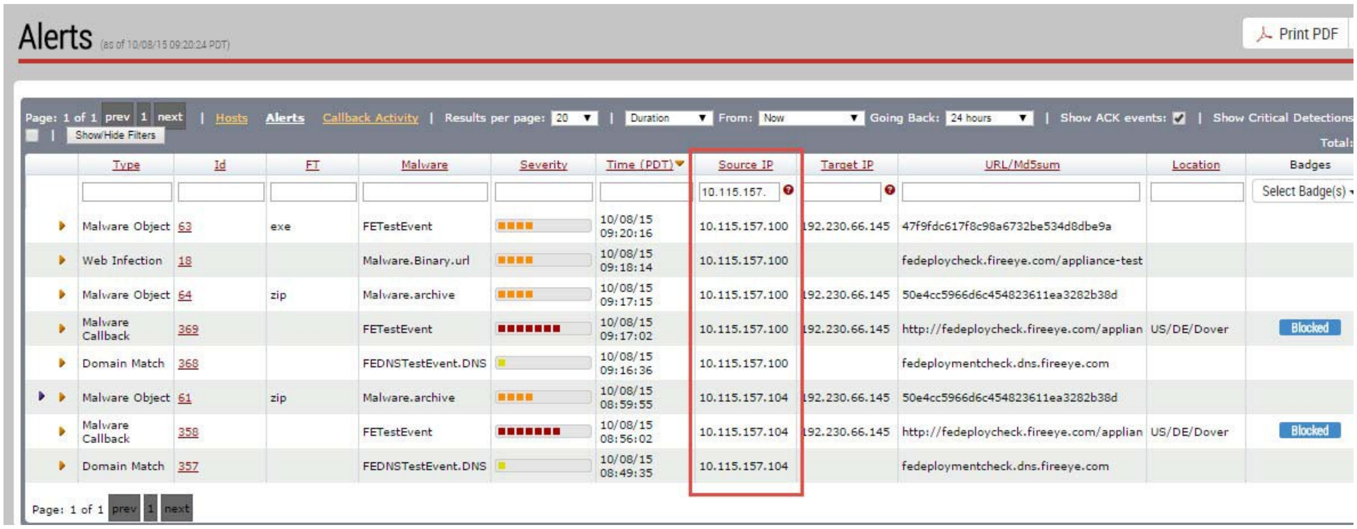


Top 25 Infected Subnets (Local)

Host Subnets	Malware Events	Unique Malware	Hosts
10.115.157.0/24	9	3	2

Figure 2-19: FireEye Dashboard—Top 25 Infected Sites

i. Click the Malware Events link. You should see the list of client IP address in the Source IP column as show in Figure 2-20.



Alerts (as of 10/08/15 09:20:24 PDT)

Print PDF

Page: 1 of 1 prev 1 next | Hosts Alerts Callback Activity | Results per page: 20 | Duration From: Now Going Back: 24 hours | Show ACK events: ☑ | Show Critical Detections
□ | Show/Hide Filters
Total:

Type	Id	FT	Malware	Severity	Time (PDT)	Source IP	Target IP	URL/Md5sum	Location	Badges
						10.115.157.				Select Badge(s)
Malware Object	63	exe	FETestEvent	■■■■	10/08/15 09:20:16	10.115.157.100	192.230.66.145	47f9fdc617f8c98a6732be534d8dbe9a		
Web Infection	18		Malware.Binary.url	■■■■	10/08/15 09:18:14	10.115.157.100		fedeploycheck.fireeye.com/appliance-test		
Malware Object	64	zip	Malware.archive	■■■■	10/08/15 09:17:15	10.115.157.100	192.230.66.145	50e4cc5966d6c454823611ea3282b38d		
Malware Callback	369		FETestEvent	■■■■■■■	10/08/15 09:17:02	10.115.157.100	192.230.66.145	http://fedeploycheck.fireeye.com/applian	US/DE/Dover	Blocked
Domain Match	368		FEDNSTestEvent.DNS	■	10/08/15 09:16:36	10.115.157.100		fedeploymentcheck.dns.fireeye.com		
Malware Object	61	zip	Malware.archive	■■■■	10/08/15 08:59:55	10.115.157.104	192.230.66.145	50e4cc5966d6c454823611ea3282b38d		
Malware Callback	358		FETestEvent	■■■■■■■	10/08/15 08:56:02	10.115.157.104	192.230.66.145	http://fedeploycheck.fireeye.com/applian	US/DE/Dover	Blocked
Domain Match	357		FEDNSTestEvent.DNS	■	10/08/15 08:49:35	10.115.157.104		fedeploymentcheck.dns.fireeye.com		

Page: 1 of 1 prev 1 next

Figure 2-20: FireEye Alerts Showing Client IP Addressed in Source IP Column

j. Repeat the previous steps on all other FireEye appliances in the inline tool group.

Each client IP address should only show up on one of the FireEye appliances. However, the distribution of the client IP addresses may not be even across all FireEye appliances.

Chapter 3

Summary and Conclusions

The previous chapters showed how to deploy Gigamon GgiaVUE-HC2 bypass protection with FireEye network security appliances. This combined solution using the Gigamon-GigaVUE-HC2 chassis for inline tool high availability and traffic distribution achieves the following objectives:

- High availability of FireEye Network Threat Prevention Platform 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.
- 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, please 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 related to FireEye products, please refer to your Support Agreement with FireEye and follow the directions on how to open a Support Case.

See Inside Your Network™

4052-02 12/15