Deploying Blue Coat® and FireEye® Inline with Gigamon

Contents

Overview 5
Deployment Prerequisites 6
Architecture Overview 7
Traffic Path 8
Access Credentials 9
FireEye Configuration 11
FireEye NX 2400 Configuration: Inline Tools 12
Configuring FireEye for Inline Block Operation Mode 12
Configuring FireEye Actions Taken: Comfort Page, TCP Resets 13
..... 14
GigaVUE-HC2 Configuration: Inline Network and Tool Groups 14
Configuring the GigaVUE-HC2 Inline Network and Inline Tools 15
Configuring the Inline Traffic Flow Maps 22
Testing the Functionality of the FireEye Inline Tool 26
Blue Coat SSLVA Configuration 32
Configuring the Blue Coat SSLVA 32
Configure/Generate Resigning Certificate Authorities 33
Creating IP Addresses and Host Configuration Lists 34
Creating Ruleset Policy 37
Creating Ruleset Rules 38
Creating Segment Policy and Assigning the Ruleset 41
GigaVUE-HC2 Inline Tool Configuration for Blue Coat SSLVA 44
Configuring Inline Tool and Inline Network Port Pairs for the SSLVA 45
Changing the Traffic Flow Maps 47
Test SSLVA Decryption by Using FireEye SSL Test URLs 53
Test SSLVA Decryption by Using FireEye SSL Test URLs 53
Test Non-SSL Traffic Again 54
Summary and Conclusions 55
Configuration Sample 56

Chapter 1

Overview

Gigamon, Blue Coat, 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 the Blue Coat SSL Visibility Appliance (SSLVA) and FireEye appliances to provide Security Service Assurance (SSA) for inline SSL decryption and advanced malware protection. The SSLVA and FireEye inline tool groups ensure that the combined inline security *service* remains available regardless of appliance maintenance or failure. Additionally, GIMO's interface modules for network bypass protection provide network availability in the event of a power outage on the GigaVUE-HC2 nodes.

The solution described and validated in this guide is based on a standard deployment of an active inline network and tools where two or more SSLVAs and FireEye Network Threat Prevention Platform (NX Series) appliances are directly cabled to one GigaVUE-HC2 chassis. Upon full deployment, the GigaVUE-HC2 first sends traffic to the SSLVA inline tool group that decrypts SSL traffic based upon a user defined policy, and then sends decrypted traffic along with all other traffic to the GigaVUE-HC2. The GigaVUE-HC2 then forwards only traffic of interest to the FireEye inline tool group for malware inspection.

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

This chapter covers the following:

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

Deployment Prerequisites

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

- GigaVUE-HC2 chassis with the following:
  - GigaVUE-OS 4.4.01
  - TAP-HC0G100C0 module
  - GigaSMART SMT-HC0-X16 module
- One Blue Coat SV3800. This includes the following:
  - SSL Appliance Linux Distribution 3.8.5-16
  - Linux Kernel 3.8.0-29-generic
  - Blue Coat Host Categorization License
  - A management LAN with Internet access for security tool updates
- Two FireEye appliances, model 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 a Blue Coat SSLVA and 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.

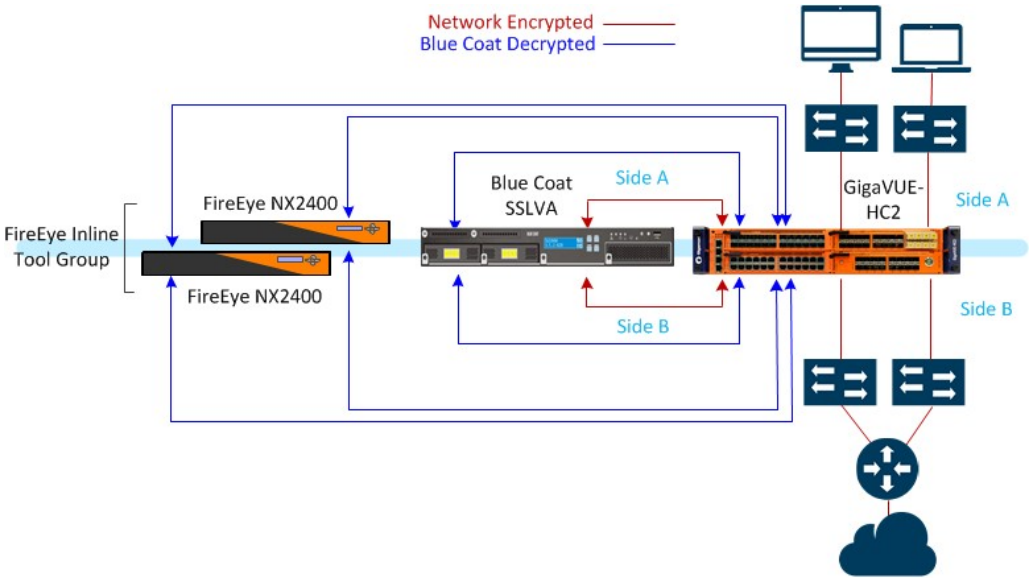


Figure 1-1: Gigamon Inline Bypass with Blue Coat SSLVA and FireEye NX

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. Also, there is encrypted and decrypted traffic on both the A and B side.

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.

Traffic Path

This solution involves a complex traffic path where the same data is entering and exiting a GigaVUE-HC2 node several times before and after each inline security tool. This path is shown in Figure 1-2. The figure shows the two GigaVUE-HC2 interface modules necessary for bypass protection of one gigabit copper network links and the second for inline security tools.

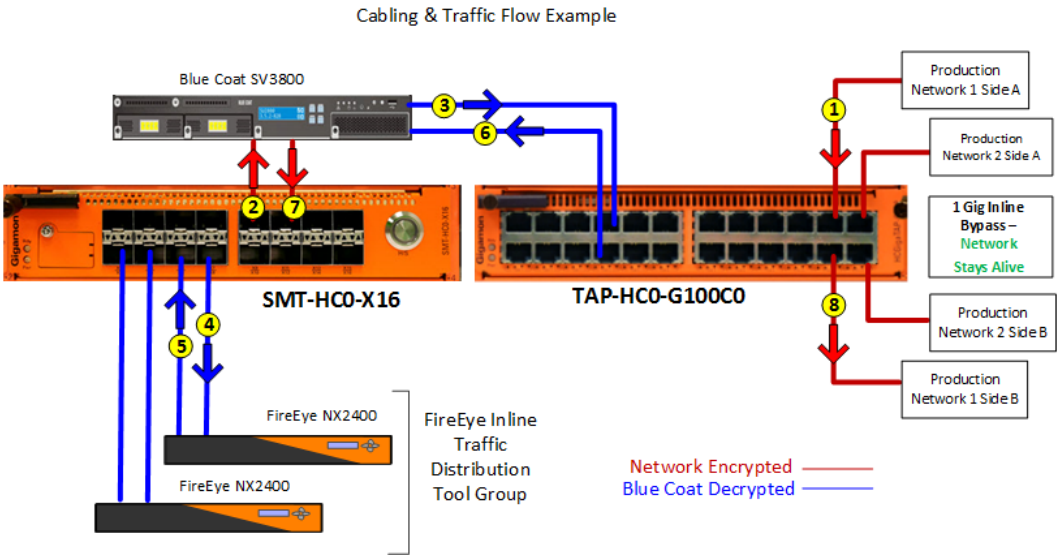


Figure 1-2: Cabling and Traffic Flow Example

In Figure 1-1, the traffic flows as follows:

1. When an internal client (Side A) sends a request for a server resource on the Internet (Side B) the request enters the GigaVUE-HC2 on an inline network port.
2. The live traffic is then sent to the Blue Coat SSLVA 3800 for decryption of SSL traffic as necessary.
3. The SSLVA 3800 decrypts traffic based on a user defined policy and sends a copy of the decrypted traffic along with all other traffic to the GigaVUE-HC2.
4. The GigaVUE-HC2 in turn distributes the traffic to the NX 2400 inline tool group for inspection.
5. If the request is not blocked, the request is returned through Side B of NX 2400 to the GigaVUE-HC2.
6. The GigaVUE-HC2 sends the request back to the decrypted Side B of the SSLVA 3800.
7. The SSLVA 3800 then completes its task for the outbound direction of that TCP session based on the NX 2400 inspection by either sending a reset or allow the encrypted traffic out to Side B of its encrypted link to the GigaVUE-HC2.
8. Finally, the GigaVUE-HC2 sends the request out Side B of the inline network port on its way to the server resource requested. The return path of the server response is handled in the same way but in the reverse direction.

Access Credentials

The default access credentials for the Gigavue-HC2, FireEye NX 2400s, and Blue Coat SSLVA 3800s are as follows:

- Gigavue-HC2 access defaults:
  - Username: admin
  - Password: admin123A!
  - There is no default management IP address.
- Blue Coat SSLVA 3800 access defaults:
  - Default username and password is set during initial configuration
  - Default management IP address is 192.168.2.42
- 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 H-VUE. For the equivalent CLI configuration commands, refer to the *GigaVUE-OS CLI User's uide* for the 4.4.01 release.

Chapter 2

FireEye Configuration

This chapter describes the configuration procedures for the GigaVUE-HC2 and FireEye NX 2400, an 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 and Figure 1-2. 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.

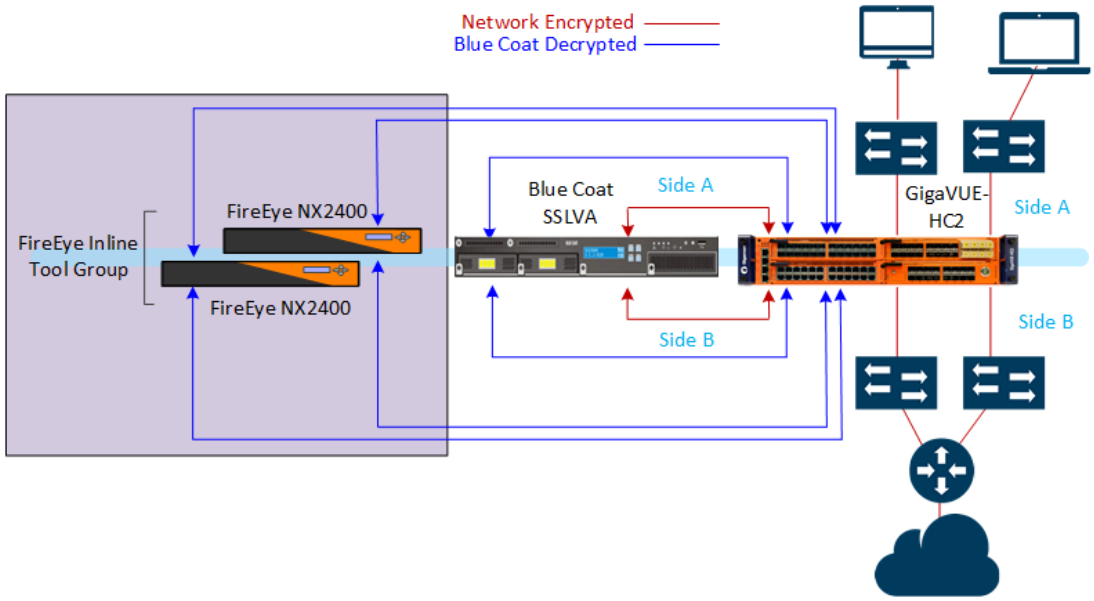


Figure 2-1: FireEye NX 2400 inline Tools

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.

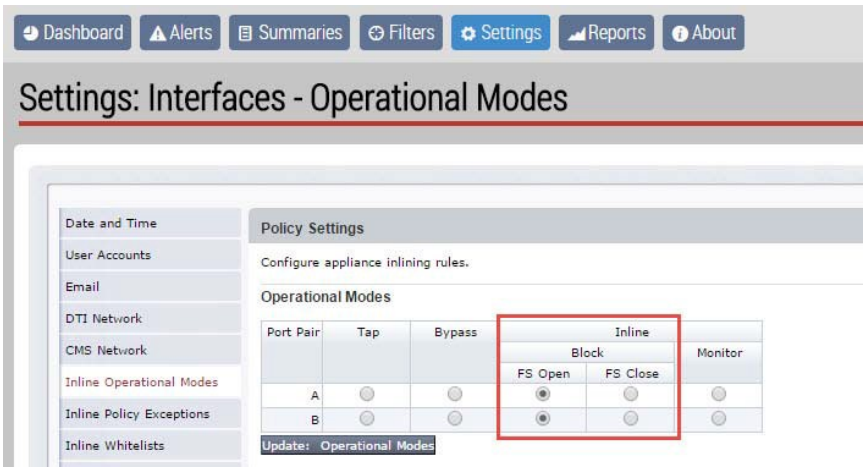


Figure 2-2: Inline Block Operational Mode on FireEye Appliance

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**.

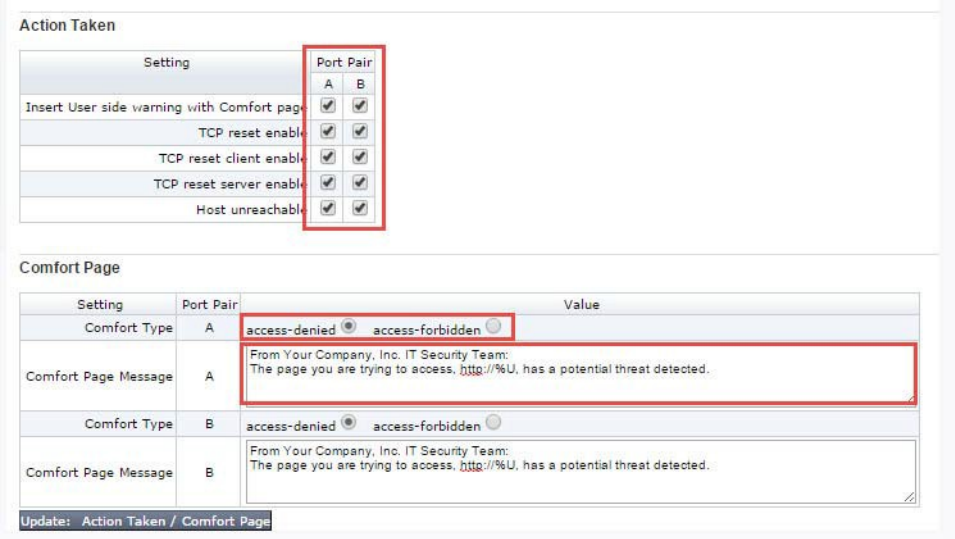


Figure 2-3: FireEye Action Taken/Comfort Page Customization

GigaVUE-HC2 Configuration: Inline Network and 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.

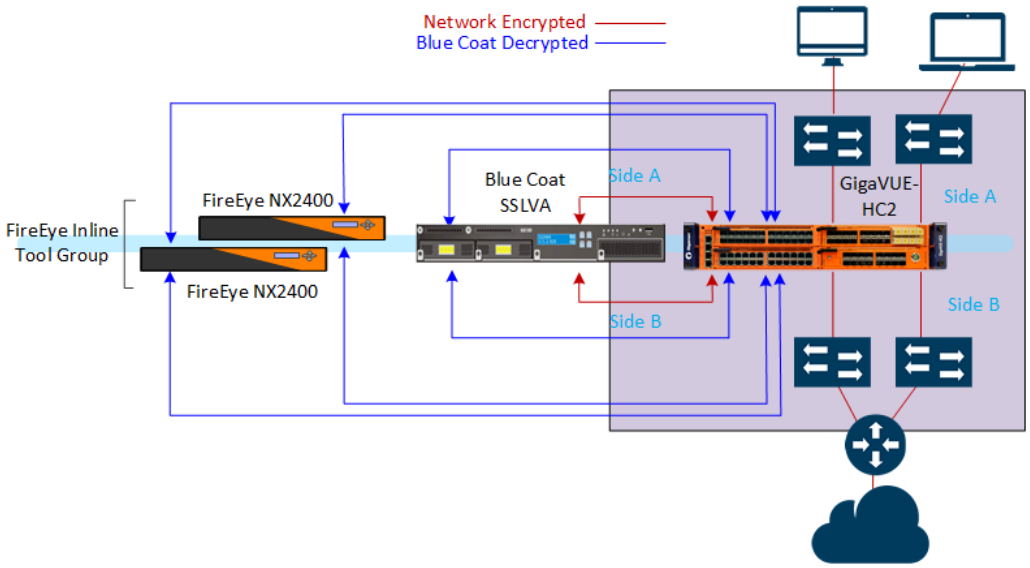


Figure 2-4: Gigavue-*GigaVUE-HC2 Configurations*

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-OS H-VUE. You can also use GigaVUE-FM, in which case you will need to select the **Physical Nodes** from the main navigation pain after you log in, 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. In H-VUE, 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 your network is 1G or 10G fiber, use one of these preconfigured inline bypass pairs. Otherwise, go to step 2.

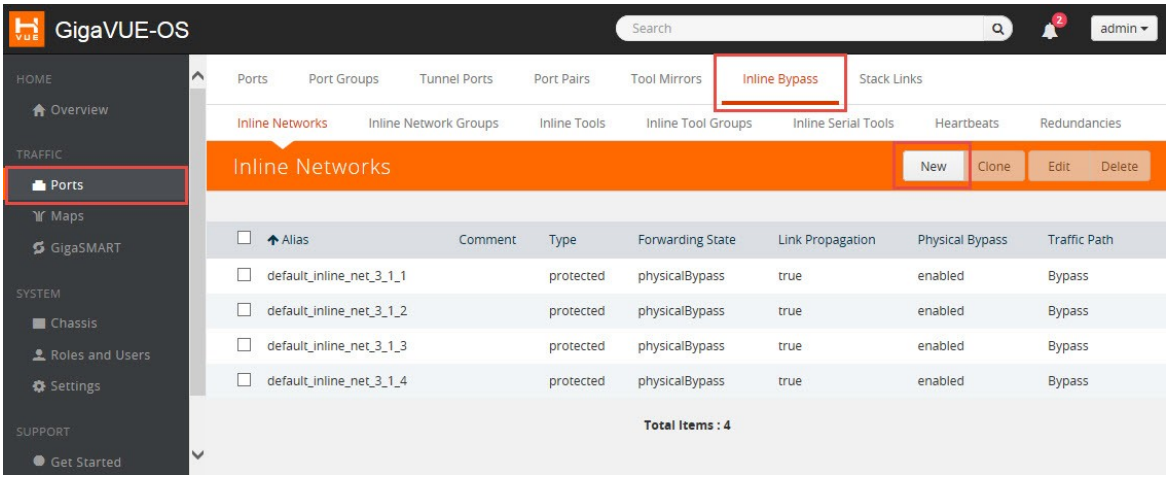


Figure 2-5: Inline Networks Page

2. Click **New**. The Inline Network configuration page displays.
3. 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 GigaVUE-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 *Step 3: Change Inline Network Traffic Path to Inline Tool*.

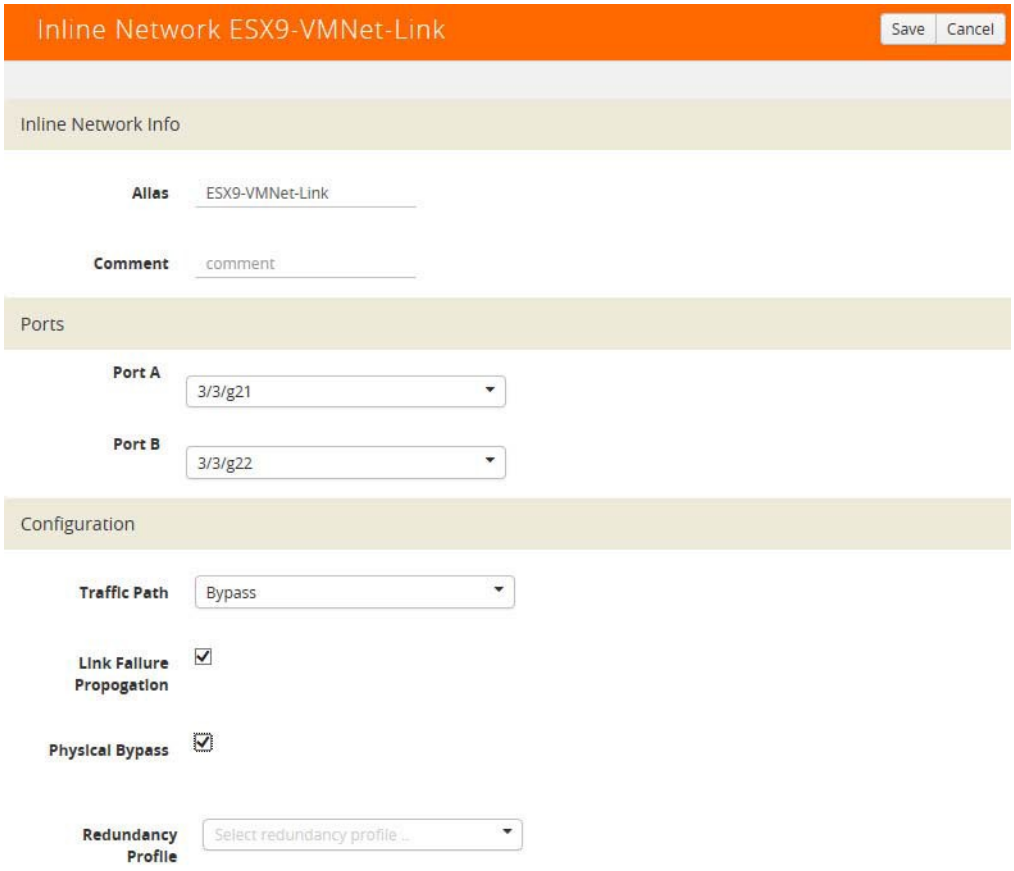


Figure 2-6: Inline Network Pair Configuration

4. 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.

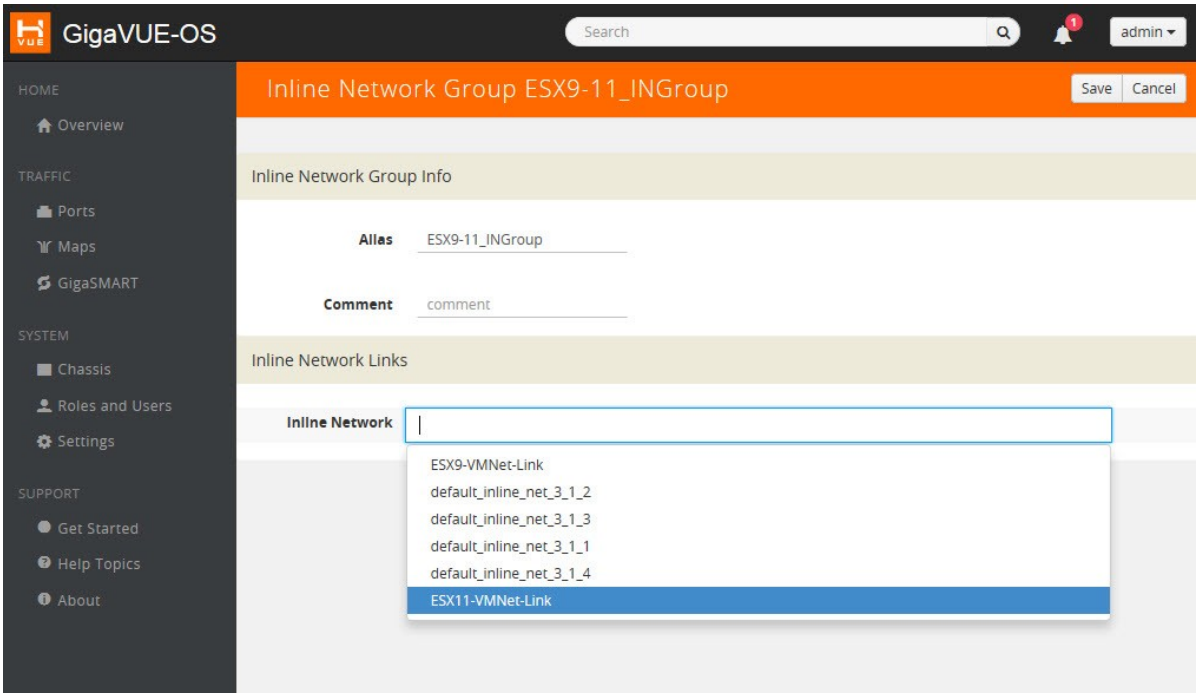


Figure 2-7: Inline Network Selection

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

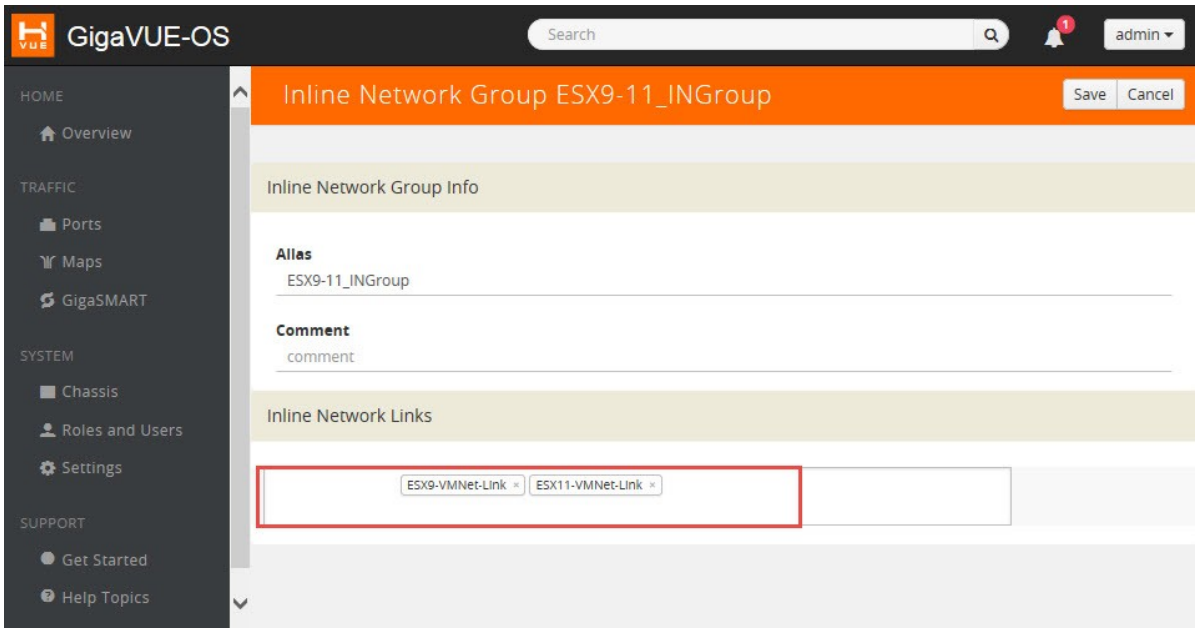


Figure 2-8: Inline Networks Added to the Inline Network Group

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

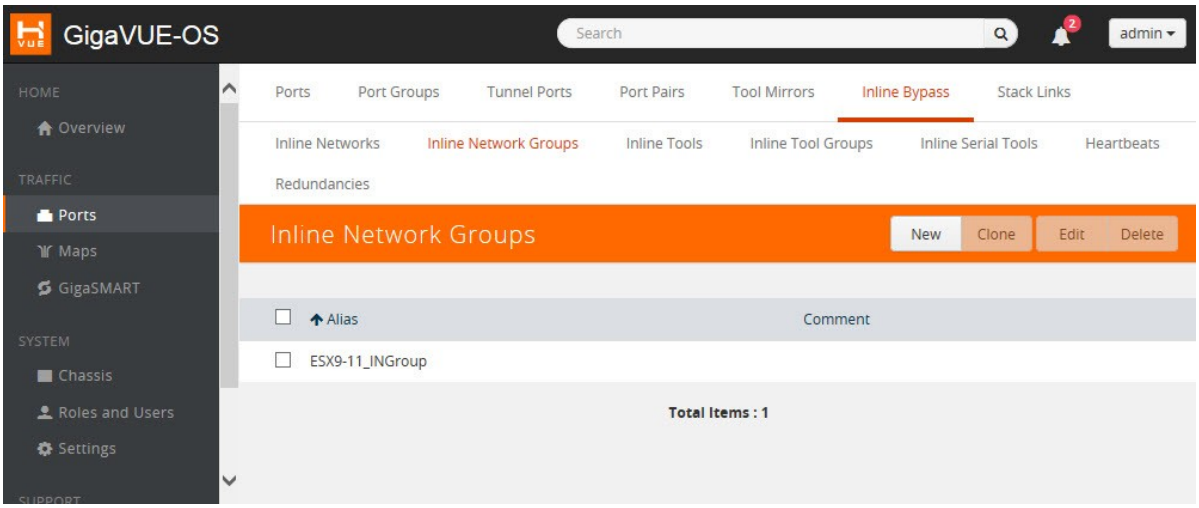


Figure 2-9: Finished List of Inline Network Groups

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 > Inline Bypass > Inline Tools**.

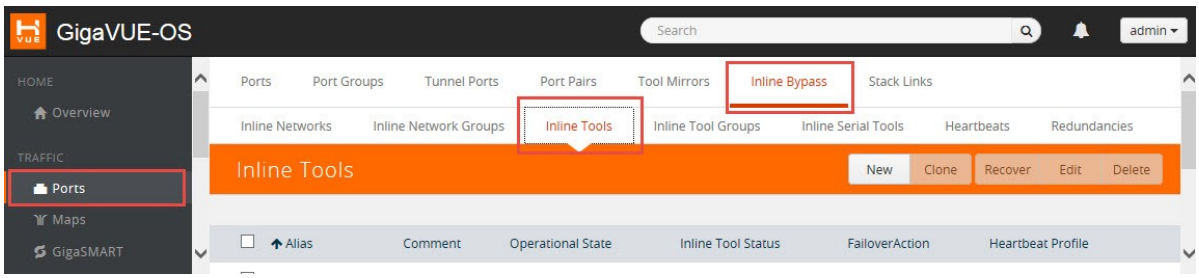


Figure 2-10: Navigating to the Inline Tools page

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, `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.

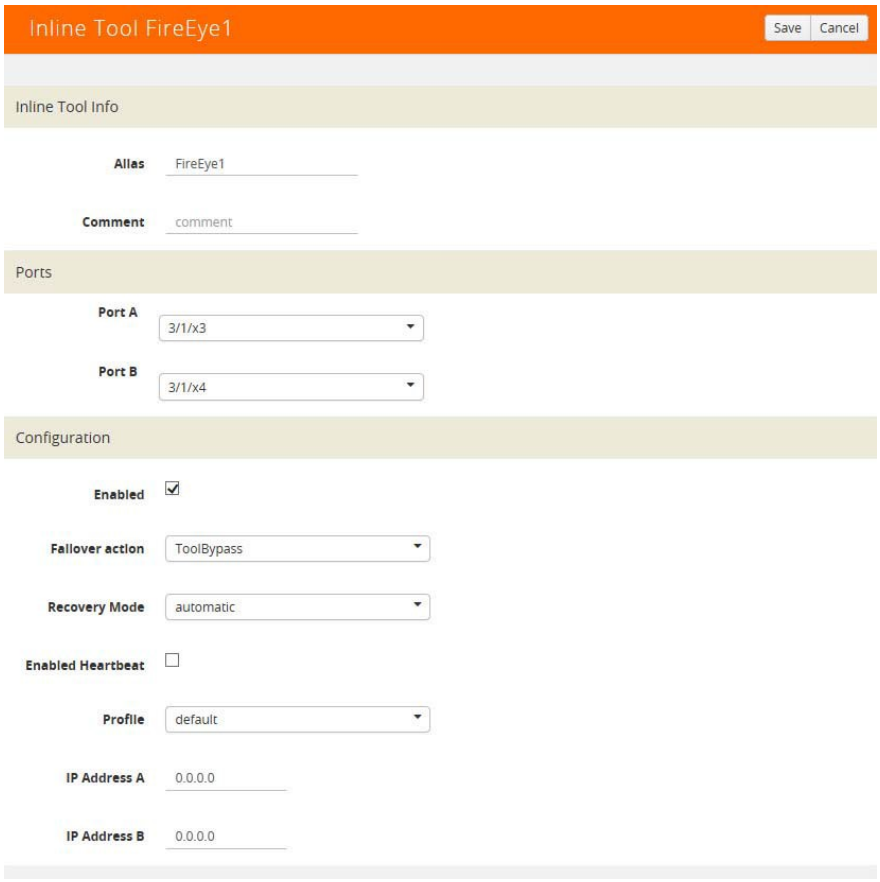


Figure 2-11: Inline Tool Pair Configuration

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 tool will be considered failed if either link is 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.

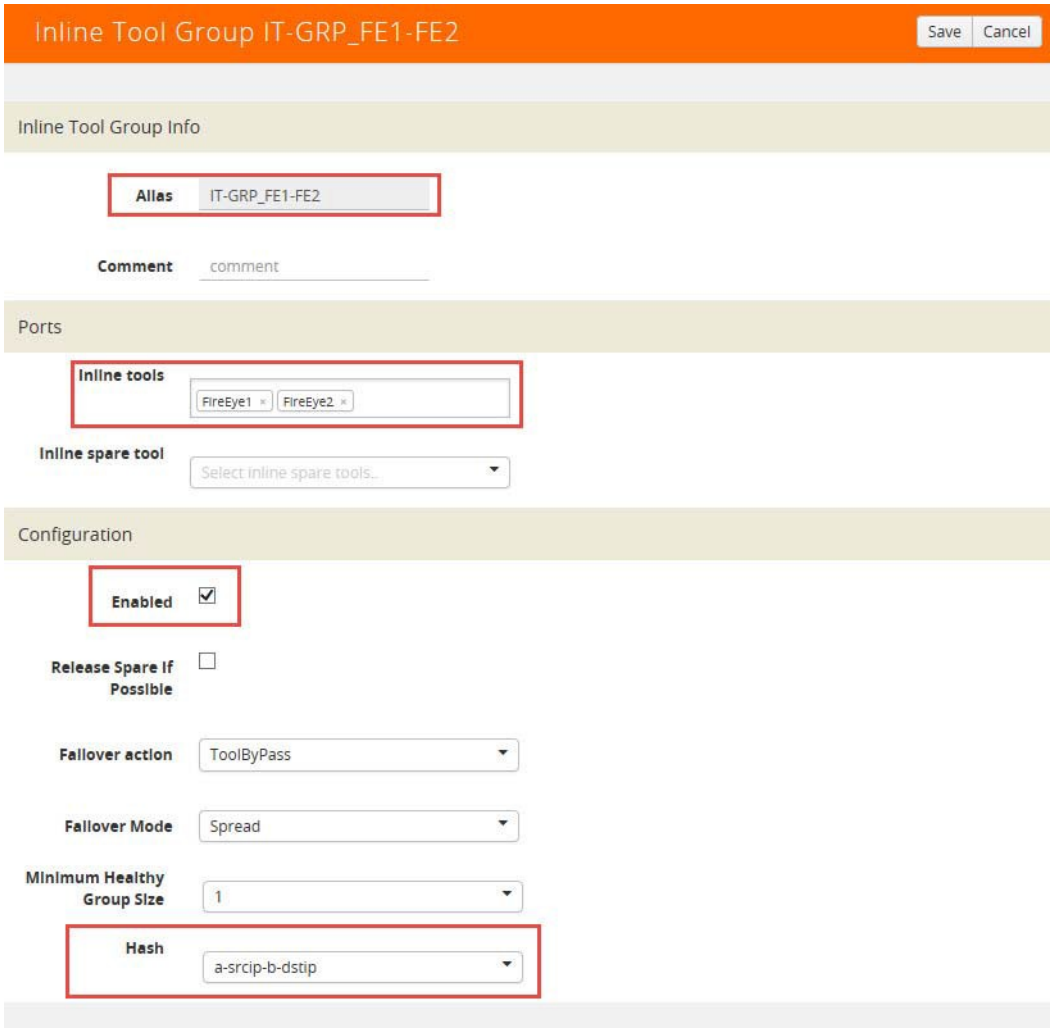


Figure 2-12: Inline Tool Group Configuration

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*.

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.

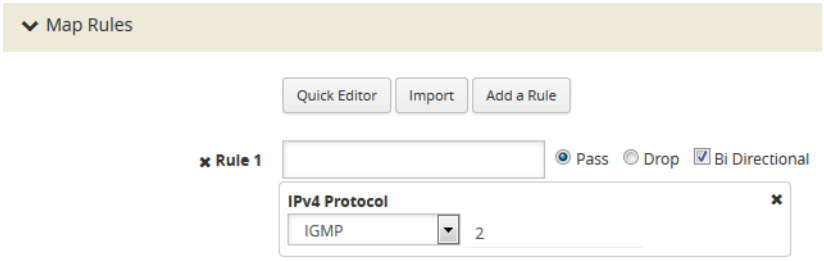


Figure 2-13: Rule for Inline Tool Flow Map

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; without defining a collector, all inline traffic from any given inline network not matched by a pass rule would be 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*.

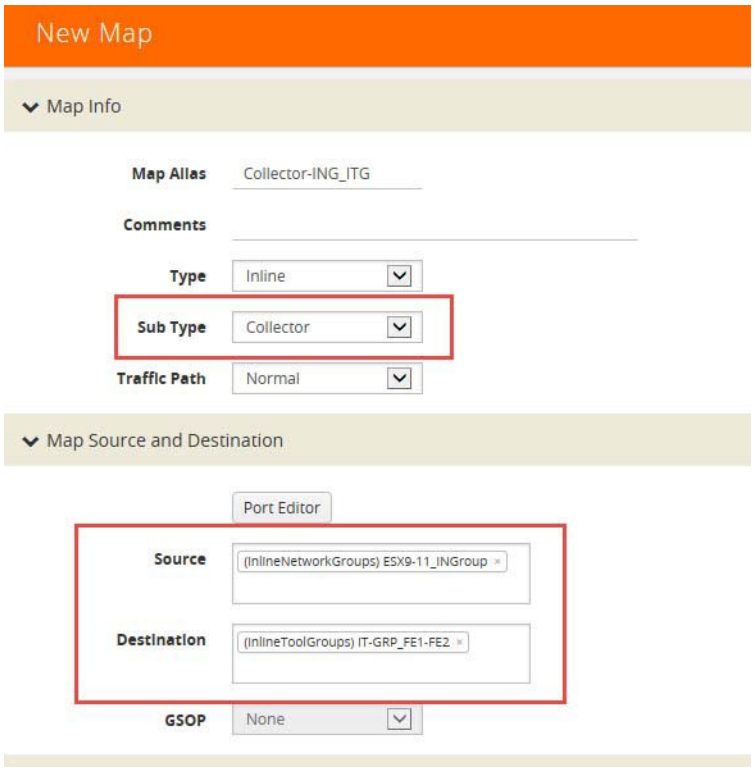


Figure 2-14: Configuration for Collector Map

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**.

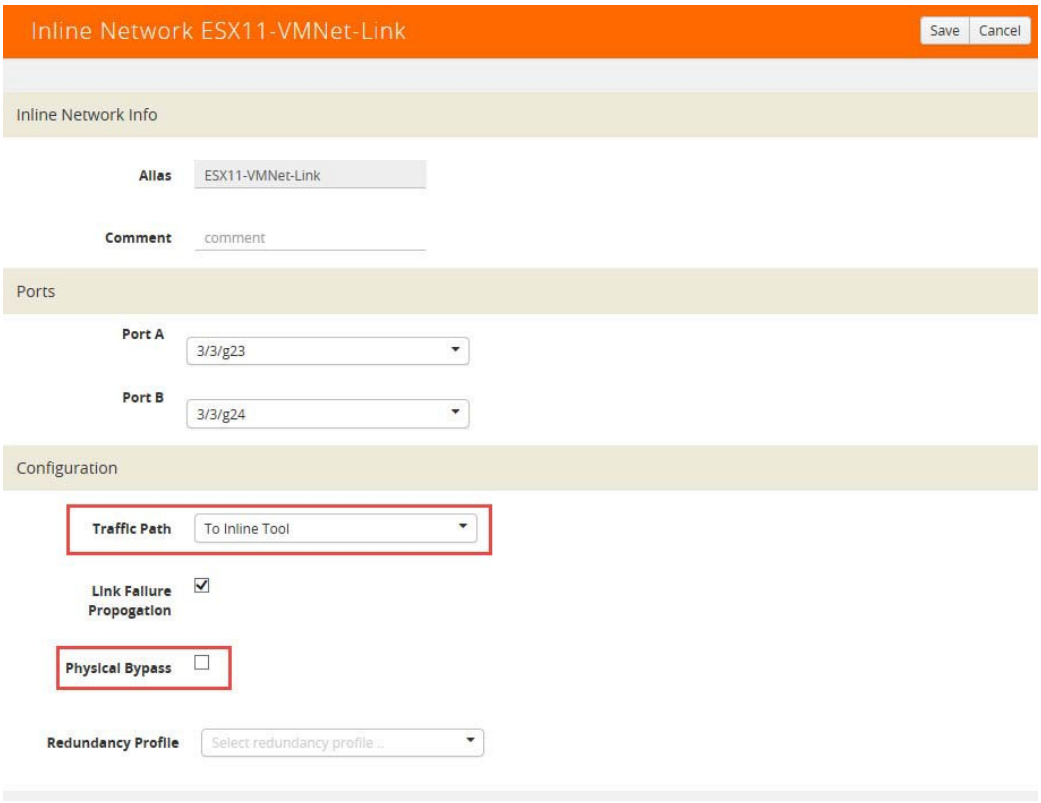


Figure 2-15: Inline Network Traffic Path Changed to Inline Tool, Physical Bypass Unchecked

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

To test the functionality of the FireEye Inline tool, 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.

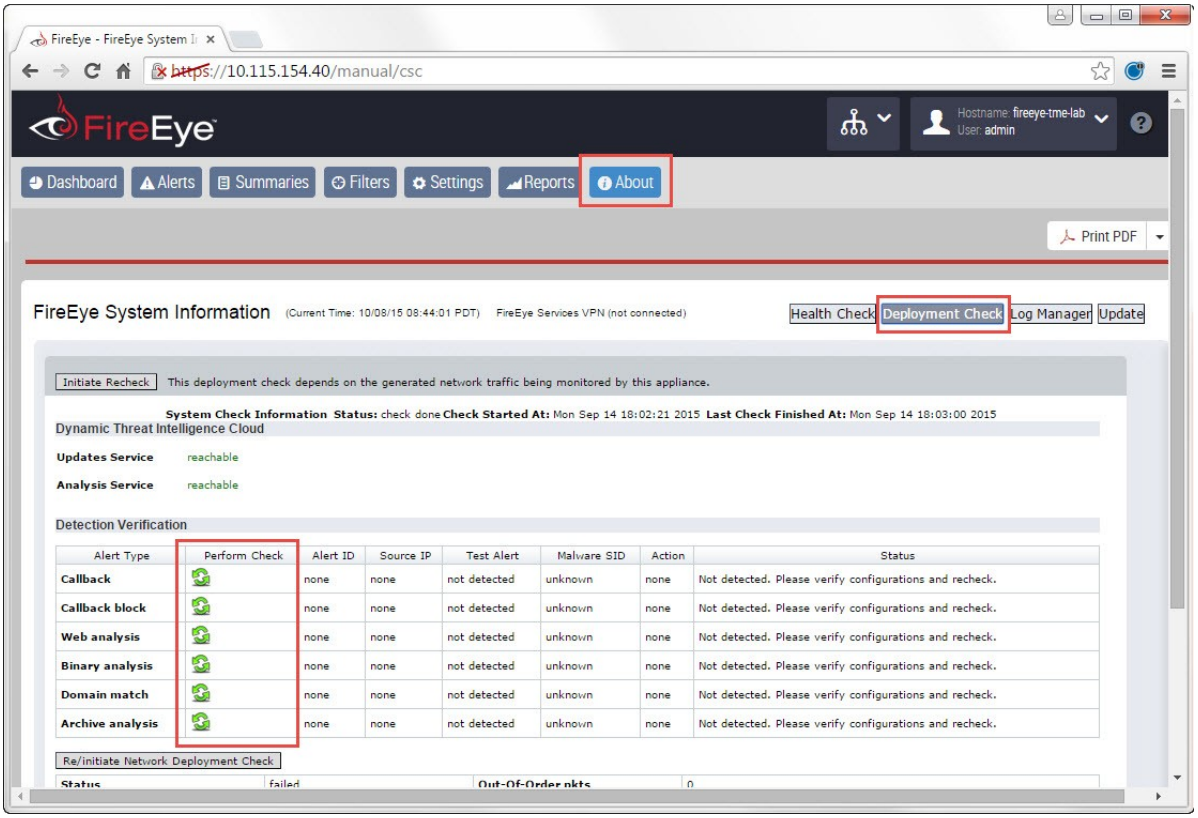


Figure 2-17: FireEye Deployment Test Page

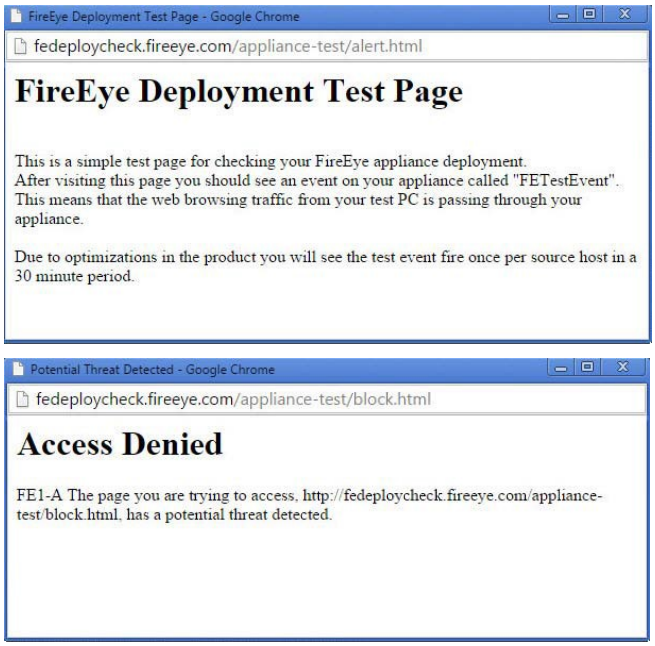


Figure 2-18: Response Pages for FireEye Deployment Test Client

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.

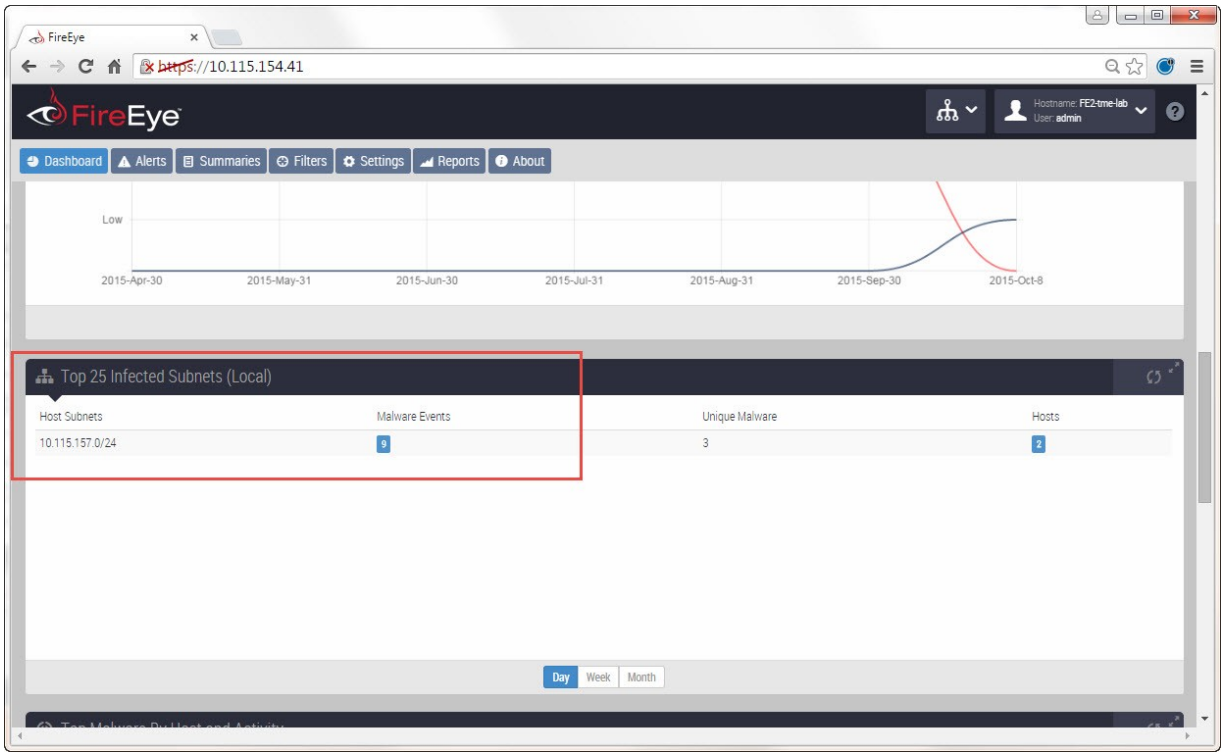


Figure 2-19: FireEye Dashboard—Top 25 Infected Sites

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.

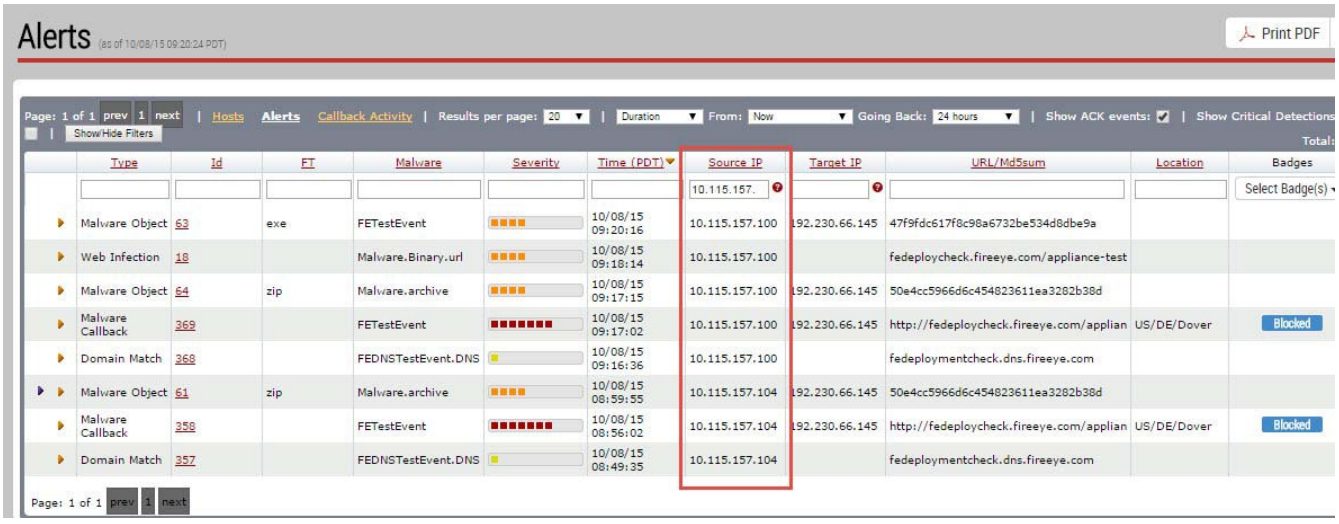


Figure 2-20: FireEye Alerts Showing Client IP Addressed in Source IP Column

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.

Blue Coat SSLVA Configuration

This chapter describes the configuration procedures for a Blue Coat SSLVA appliance and the GigaVUE-HC2. The procedures are organized as follows:

- *Configuring the Blue Coat SSLVA*
- *GigaVUE-HC2 Inline Tool Configuration for Blue Coat SSLVA*

Configuring the Blue Coat SSLVA

These procedures apply to the portion of the topology highlighted in Figure 3-1, which shows the network reference architecture.

- *Configure/Generate Resigning Certificate Authorities*
- *Creating IP Addresses and Host Configuration Lists*
- *Creating Ruleset Policy*
- *Creating Segment Policy and Assigning the Ruleset*
- *GigaVUE-HC2 Inline Tool Configuration for Blue Coat SSLVA*

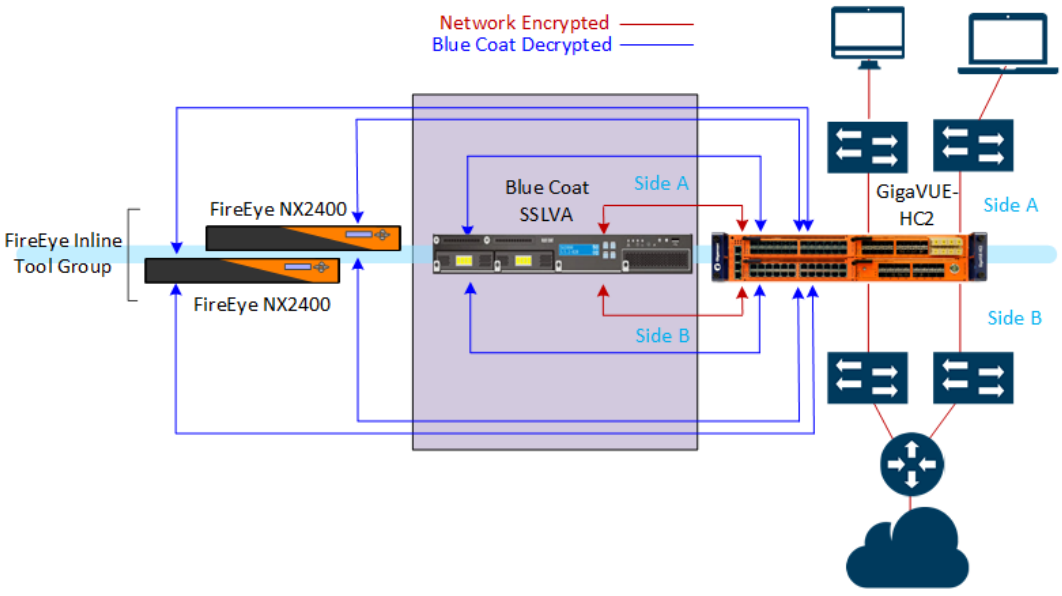


Figure 3-1: Blue Coat SSLVA

The SSLVA must have both a segment and ruleset policy configured and assigned. The ruleset policy is created first because the ruleset policy is assigned to a segment policy as it is created.

Be aware that if the aggregated links are asymmetric with VLAN tags, Blue

Coat recommends the SSLVA feature for VLAN tag mapping not be used.

Finally, in this deployment example, the configurations for the Blue Coat SSLVA will decrypt all SSL traffic, except as follows:

- IP addresses: VMWare vCenter Server and ESX Hosts
- Blue Coat Web Filter Categories: Financial Services, Brokerage/Trading, Health
- Blue Coat SSLV unsupported sites.

NOTE: This guide focuses on the easiest SSLVA configuration scenario where self-signed certificates are generated and used to get this combined deployment up and running. For a more complex PKI deployment, such as uploading external certs, setting trusted authorities, and HSM implementations, refer to the *Blue Coat SV2800, SV3800 Administration Guide*.

Configure/Generate Resigning Certificate Authorities

This section goes through the step necessary to generate self-signed RSA and Elliptical Curve certificates used for resigning certificates sent by external resources where clients request HTTPS/SSL access. These are the certificates that the SSLVA sends to the clients instead of those sent by the external HTTPS/SSL resource.

To generate SSLVA resigning certificate authorities, do the following:

1. Log into the SSLVA GUI with an admin account that has Manage PKI privileges.
2. Select **PKI > Resigning Certificate Authorities**.
3. In the Local Resigning Certificate Authorities section, click the red certificate seal symbol as shown in Figure 3-2.

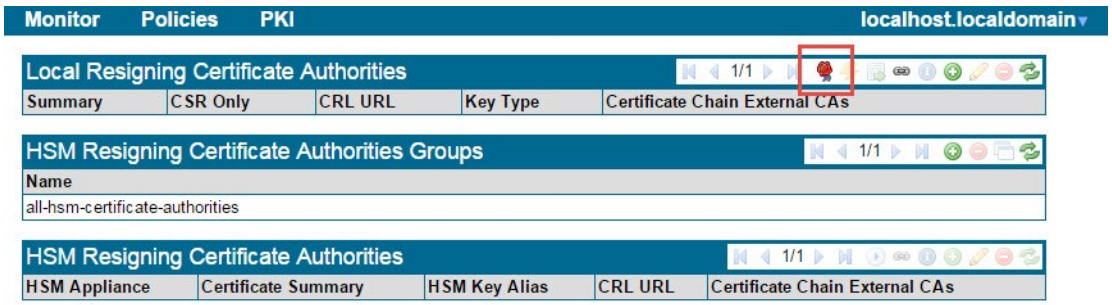


Figure 3-2: Blue Coat SLVA Self-sign Certificate Generation

4. In the Generate Certificate page that displays, fill in the appropriate information for your organization. Leave RSA for key type. The default values for valid time and key size are appropriate for most; however, change as necessary. Figure 3-3 shows an example.

Figure 3-3: Certificate Generation Form

5. Click Generate self-signed CA.
6. Repeat for an Elliptic Curve certificate if needed.
7. Click Apply at the bottom of the PKI Changes page.

Creating IP Addresses and Host Configuration Lists

This section goes through the necessary steps to create lists used to create *cut through policy* later in the policy ruleset. Certain sites are not currently supported for proper decryption by the SSLVA and are therefore listed in an unsupported-sites list provided by Blue Coat. IP address and host categorization lists are user-defined as shown in the steps in the following sections:

- *Creating the IP Address List*
- *Creating the Host Configuration List*

Creating the IP Address List

The vCenter server in the Gigamon lab used to test the deployment did not allow for self-signed certificates for the communication between it and the ESX hosts it was managing. Therefore, a list of IP addresses for both was necessary. Your organization may have similar needs.

The following are the steps used for creating the IP Address for the vCenter and ESX hosts:

1. Select **Policies > IP Address List**.
2. In the IP Addresses List section, click the green circles “+”.
3. Type an appropriate name for the IP address list in the Name dialog box.
4. Click OK. The list name will appear in IP Addresses Lists.
5. Highlight the list name and click the green circled “+” in the IP Addresses section.
6. Type the IP address in the Add IP Address Item box that pops up.

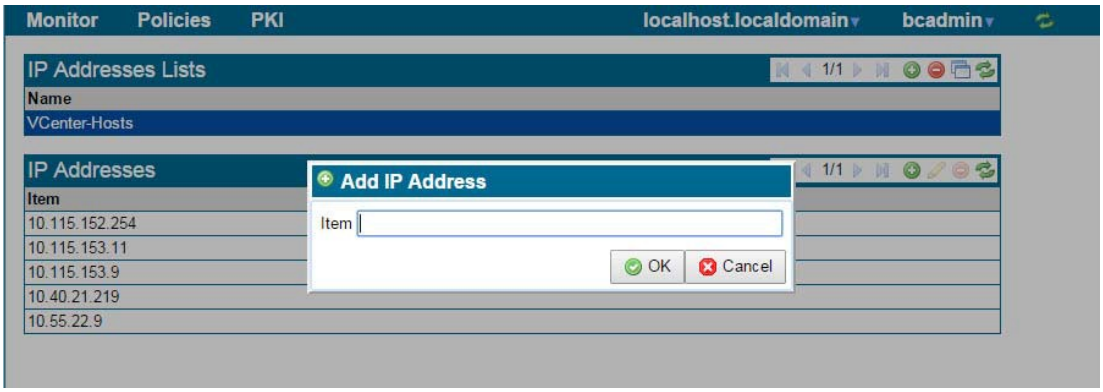


Figure 3-4: IP Address List Creating for Blue Coat SSLVA.

7. Click OK.
8. Repeat for all IP addresses.

   NOTE: SSLVA IP address lists support IPv6 and CIDR formats. For more details, refer to the *Blue Coat SV2800 and SV3800 Administration and Deployment Guide*.
9. Click Apply at the bottom of the page.

Creating the Host Configuration List

Blue Coat provides a host categorization list that can be licensed and used by the SSLVA for user-defined policy on which a site's traffic can be passed directly through without being sent to the decryption engine. Many companies use this feature to maintain employee privacy when using company resources to access health and financial websites during business hours. This assumes the company is otherwise decrypting all SSL traffic.

Another approach is to *cut through* all SSL traffic and only decrypt sites they deem to be inappropriate or a source of malicious content. Either approach uses the following steps to create host category lists for policy.

To create host category lists, do the following:

1. Select **Policies > Host Categorization List**.
2. Make sure the Host Categorization Status shows the database is loaded and available. Figure 3-5 shows an example.

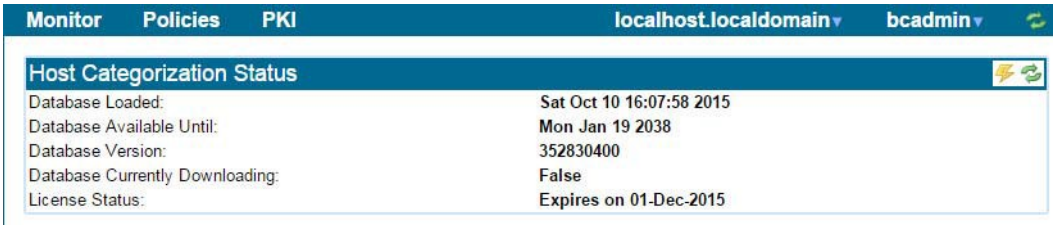


Figure 3-5: Database Status for Blue Coat Web Filter

3. In the Host Categorization Lists section click the green "+".
4. Type an appropriate name in the Add Host Categorization List dialog box and click OK.
5. Highlight the name of your new list and click the pencil icon in the Host Categorizations section.
6. Check the appropriate categories for the type of host categories for your list. Figure 3-6 shows an example of the "Don't" decrypt list.

Figure 3-6: Blue Coat Category Check List

7. Click OK.
8. Click Apply at the bottom of the page.

Creating the Blue Coat Unsupported Site List

To define the unsupported site list, you need to create a list of unsupported sites and then insert the list as a rule.

To create the list of unsupported sites, do the following:

1. Select **Policies > Subject/Domain Names List**.
2. In the Subject/Domain Names Lists section, click the green circled "+".
3. In the Add Subject/Domain Names List dialog, type `sslng-unsupported-sites`.
4. Click OK.
5. Highlight the created name and click the pencil icon in the Ruleset Options section.
6. Create a list that looks like the list shown in Figure 3-7.
7. Click Apply at the bottom of the page.

Subject/Domain Names
Item
cn=*.citrixonline.com
cn=*.data.toolbar.yahoo.com
cn=*.dropbox.com
cn=*.fedoraproject.org
cn=*.itunes.apple.com
cn=*.logmein.com
cn=*.mozilla.org
cn=*.rhn.redhat.com
cn=*.sls.microsoft.com
cn=*update.microsoft.com

Figure 3-7: List of Unsupported Sites

Creating Ruleset Policy

This section presents the process for creating a ruleset from the unsupported sites, IP address, and host lists previously created to define which SSL traffic will be decrypted and which will be *cut through.* The following example will have the last rule as "Decrypt". This means all traffic will be decrypted except for that matching the rules above the last rule of "Decrypt".

In addition to the last rule in the rule set, there is a "Catch All Action" that is set to "Cut Through" in this example. This defines what happens to an SSL session that does not trigger any of the rules within a ruleset. It seems counterintuitive to have this and the last rule in the ruleset opposite of each other. This was the Blue Coat subject matter expert's recommendation.

1. Select **Policies > Rulesets**.
2. Click the green circled "+" in the Rulesets section.
3. Type an appropriate name in the Add Ruleset dialog box.
4. Click OK.
5. Highlight the created name and click the pencil icon in the Ruleset Options section.
6. Select the Ruleset Options:

- Default RSA & EC: Match earlier PKI configurations for local or external certificates and/or certificate authorities.
- Catch All Action: Cut Through
- Host Categorization IP Exclude List: Default (Not Set)
- HSM Failure Action: As appropriate for your HSM settings.

7. Click OK.
8. Click Apply at the bottoms of the page.

Creating Ruleset Rules

This section provides the steps for creating the following ruleset rules.

- *Blue Coat Unsupported List Rule*
- *IP Address List Rule*
- *Host Categorization List Rule*
- *Decrypt Resign Last Rule*

Blue Coat Unsupported List Rule

To create a rule for unsupported sites, do the following:

1. Select **Policies > Rulesets**.
2. In the Rulesets section, highlight by selecting the ruleset to add rules.
3. In the Rules section, click the green circled "+".
4. Leave all the default settings, *except* select the radio button next to Subject/Domain Name List.
5. Select **sslng-unsupported-sites** from the drop-down list as shown in Figure 3-8. This is the list that you created in the previous procedure.

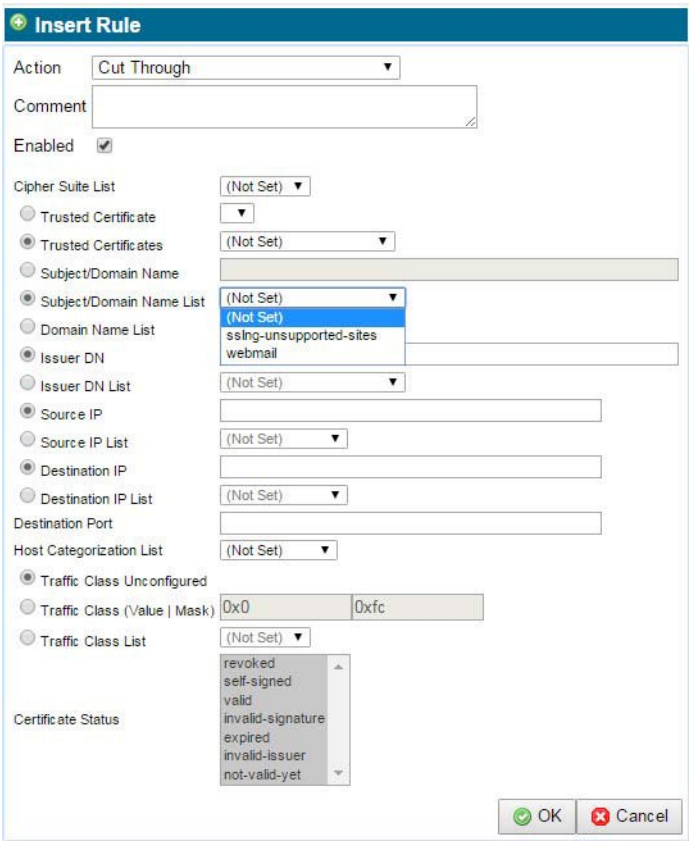


Figure 3-8: Blue Coat SSLVA Unsupported Sites Rule

6. Click OK.
7. Click Apply at the bottom of the page.

IP Address List Rule

To add a second rule for the IP address list, do the following:

1. In the Rules section, click the green circled "+".
2. Leave all the default settings, *except* select the radio button next to Source IP List.
3. Select the IP address list you created earlier in the section *Creating the IP Address List*.
4. Click **OK**.
5. Click Apply at the bottom of the page.

Host Categorization List Rule

To add a rule for the Host Categorization list, do the following:

1. In the Rules section, click the green circled "+".
2. Next to Host Categorization list,select from the pull-down list. This is the list that you created in the section *Creating the Host Configuration List* on page 35. All the other settings are left at their defaults.
3. Click **OK**.
4. Click Apply at the bottom of the page.

Decrypt Resign Certificate Last Rule

This is the important last rule that all SSL traffic should match if it does not match any of the previous rules. For this example, decrypt and resign is appropriate.

To define the decrypt resign last rule, do the following:

1. In the Rules section, click the green circled "+".
2. Select only the following and leave the rest unchanged:
   - Action: Decrypt (Resign Certificate)
   - EC Resigning CA: Your self-signed EC Certificate unless you have external or imported cert.
   - RSA resigning CA: Your self-signed RSA Certificate unless you have an external or imported cert.

   Your selections should look similar to those shown in Figure 3-9.

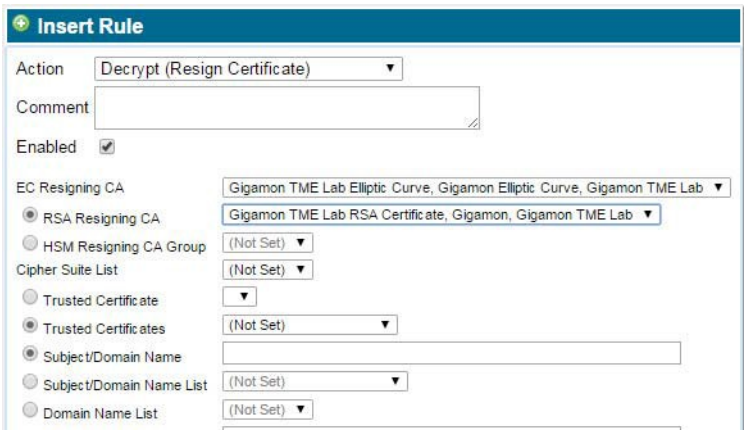


Figure 3-9: Last Rule Catch All Rule for Decrypt Action

3. Click **OK**.
4. Click Apply at the bottom of the page.

After defining Decrypt Resign Last rule, you have a rule set that looks similar to the example shown in Figure 3-9.

NOTE: Make sure that the Decrypt (Resign Certificate) Rule is at the bottom of the Ruleset list. Use the down arrow to move the rule if necessary.

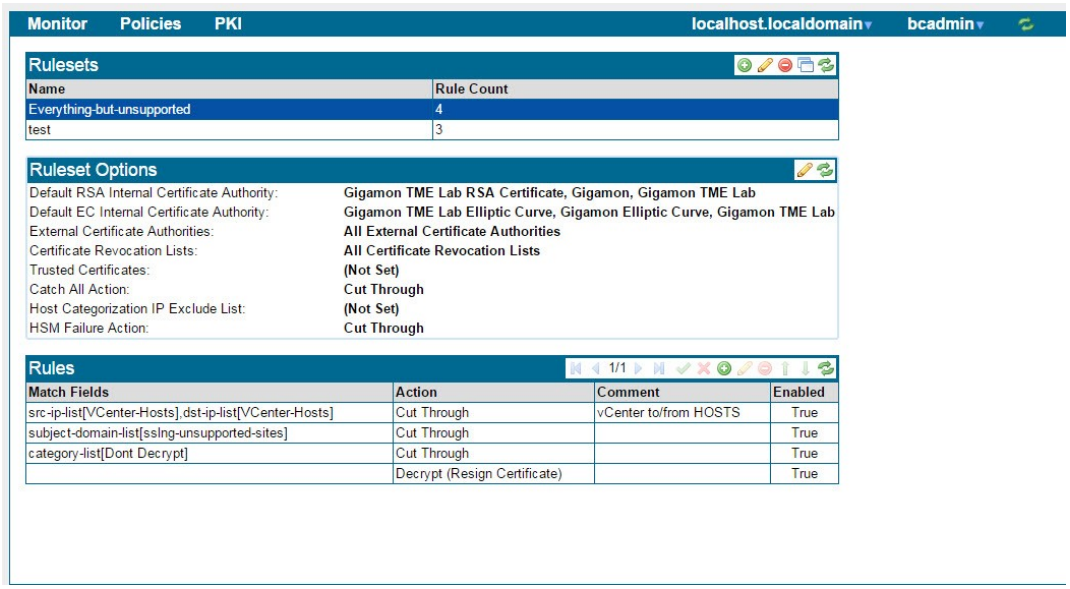


Figure 3-10: Complete SSLVA Ruleset

NOTE: This example has all SSL traffic decrypted except for the "whitelist" rules that are "cut through." The opposite approach would be to create a "blacklist" of rules set to decrypt and resign and set the last rule as "cut through.

Creating Segment Policy and Assigning the Ruleset

This section goes through the steps necessary to create a segment policy. This includes the physical bridge ports' mode of operation, the ruleset assigned to the segment, and lastly defining which physical port pairs where the policy is applied.

To create the segment policy, do the following:

1. Select **Policy > Segmen**t.
2. In the Segments section, click the green circled "+" . The Add Segment page displays.
3. In the Add Segment page, click **Edit** for the Mode of Operation.
4. Select the mode of operation that matches your physical cabling shown in the small diagram.

   For this example, cabling matches **Active Inline, Fail to Appliance** a shown in Figure 3-11.

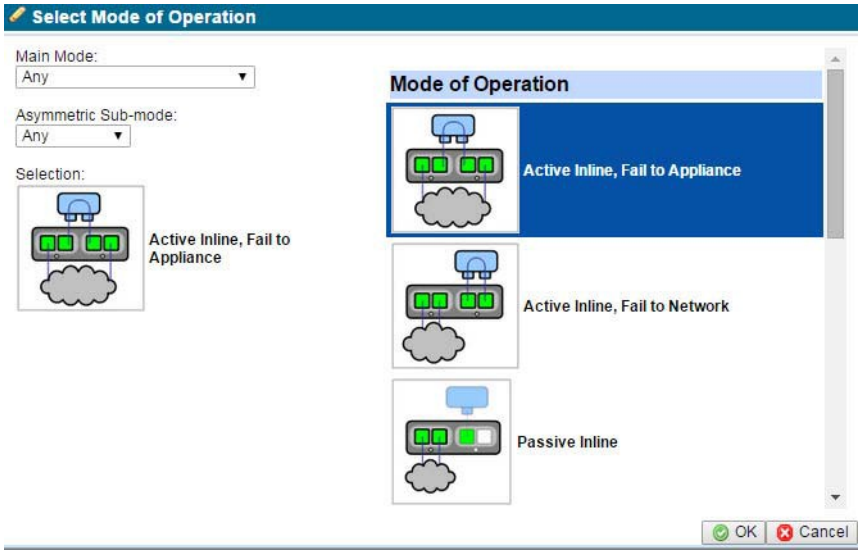


Figure 3-11: Blue Coat SSVA Segment Modes of Operation

5. Click **OK**.

   The mode of operation should now show in the Add Segment page.

6. On the Add Segment page, do the following:

   a. In the Ruleset drop-down list, select the ruleset you created in *Creating Ruleset Policy*.

   b. Leave Session Log Mode and VLAN Translation as the default. Add a comment as you see fit.

   c. Click **OK**.

7. To assign this segment and ruleset policy to physical ports, highlight the policy row, and then click the Mark for Activation icon as shown in Figure 3-12.

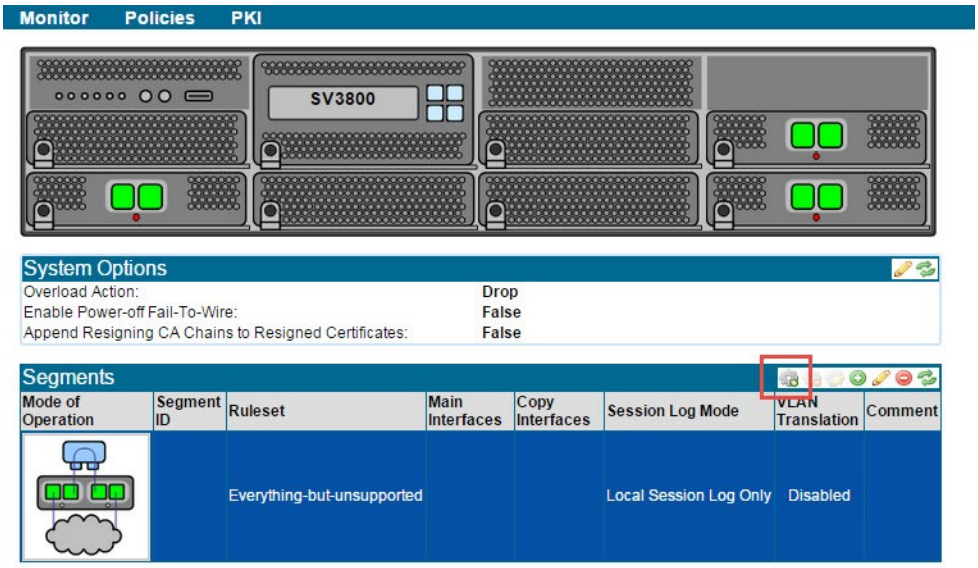


Figure 3-12: Blue Coat SSLVA Marking a Segment Policy for Activation

8. In the Segment Activation page that displays, select the ports from the segment image in the order indicated by the fuchsia colored ports, and then select **Next** as shown in Figure 3-13.

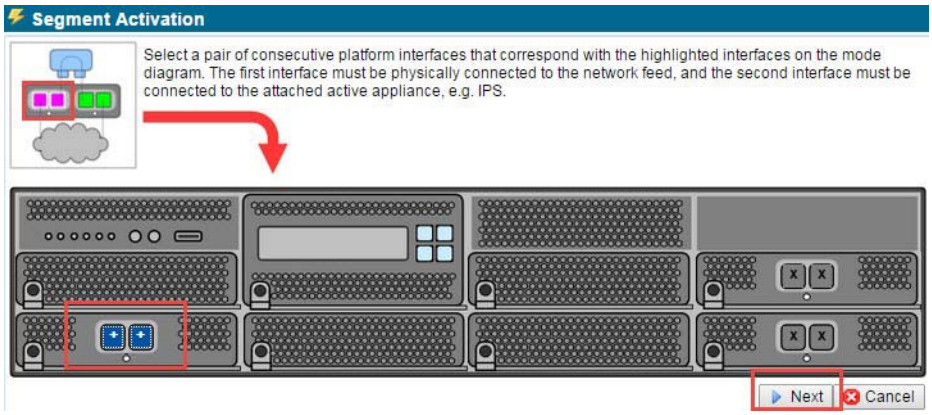


Figure 3-13: Blue Coat SSLVA Segment Activation Port Selection

9. Select the next set of port pairs, and then click **Next**.
10. On the Copies port, select **Next** without selecting a physical interface, and then Click OK.
11. Click **Apply** at the bottom of the page.

NOTE: There are several configurations that can be changed for Certificate Status Actions, Appliance Feedback Options, and VLAN Mappings. This deployment guide does not cover the details of these configurations.

GigaVUE-HC2 Inline Tool Configuration for Blue Coat SSLVA

This section covers configuring the GigaVUE-HC2 for the Blue Coat SSLVA inline tool element or elements that will be used to create new maps and change existing traffic flow maps. At a high level, the SSLVA will be placed logically inline between the GigaVUE-HC2 and the FireEye inline tool group providing SSL decryption for traffic as appropriate.

This section covers configurations for the section highlighted in the Figure 3-14.

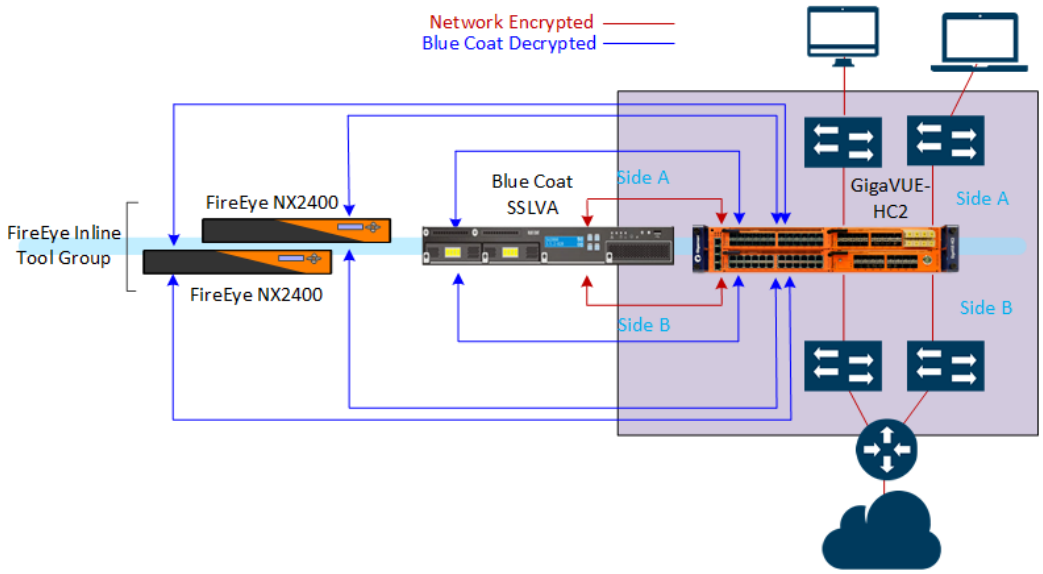


Figure 3-14: GigaVUE-HC2 Configurations

The configuration procedures are organized as follows:

- *Configuring the GigaVUE-HC2 Inline Tool Pair for the SSLVA*. From the perspective of the SSLVA, these ports are the network input ports.
- *Configuring the GigaVUE-HC2 Inline Network Port Pair for the SSLVA*. From the perspective of the SSLVA, these ports are the decrypted traffic tool output ports.
- Delete the existing traffic maps of the GigaVUE-HC2 for the inline Network Group. Create a new map so that the Inline Network Group goes to the SSLVA Inline Tool pair instead of the FireEye Inline Tool Group.
- Create the new traffic maps from the SSLVA Inline Network port pair of the GigaVUE-HC2 to the FireEye Inline Tool Group.

NOTE: Modifications of these procedures is not recommended.

Configuring Inline Tool and Inline Network Port Pairs for the SSLVA

It is necessary to create both an Inline Tool pair as well as an Inline Network port pair for the SSLVA. This is because the GigaVUE-HC2 sends traffic to the SSLVA for decryption as well as receives the decrypted traffic from the SSLVA to distribute to the FireEye Inline Tool Group as indicated in Figure 3-15. The figure also indicates the port type relativity between the GigaVUE-HC2 and the Blue Coat appliance. From the point-of-view of the GigaVUE-HC2, the Blue Coat SSLVA is an inline tool. However, from the point-of-view of the Blue Coat SSLVA, the GigaVUE-HC2 is part of an inline network.

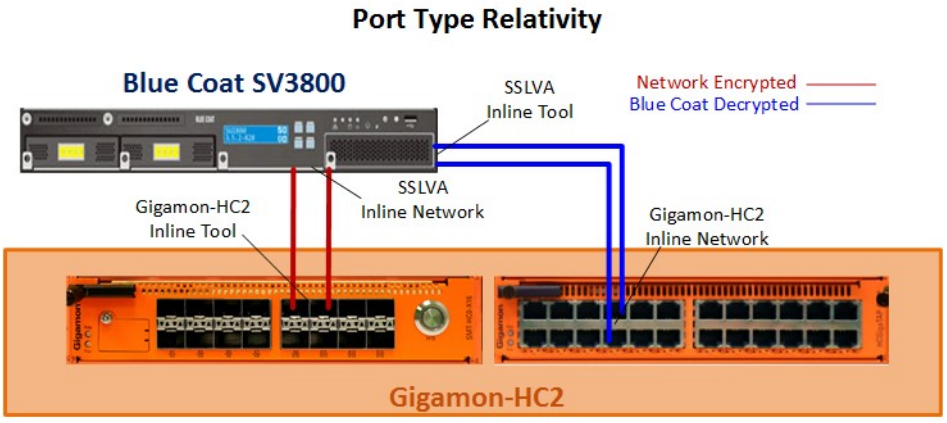


Figure 3-15: GigaVUE-HC2 Inline Tool Port Pair Connections to Blue Coat SSLVA Inline Network Port Pair

This section walks through the steps needed to configure an Inline Network (IN) bypass pair and an Inline Tool (IT) pair for the SSLVA. As the company infrastructure grows and more SSLVAs are needed to decrypt traffic, an Inline Network and Inline Tool Group can be created respectively to distribute traffic across the SSLVAs. For specific steps, refer to previous sections of this deployment guide.

NOTE: It is assumed that you have all the SSLVA connected ports shown in Figure 3-15 as Inline Network on the GigaVUE-HC2 set as Inline Network port types. Similarly, those that are indicated as Inline Tool on the GigaVUE-HC2 are configured as Inline Tool type ports. Refer to the Help Topics provided in GigaVUE-OS H-VUE for specific instructions on completing these tasks.

Configuring the GigaVUE-HC2 Inline Tool Pair for the SSLVA

This section covers the steps needed to configure the GigaVUE-HC2's inline tool port pair for the encrypted side of the SSLVA ports. Refer to the GigaVUE-HC2 red Inline Tool links to/from the SV3800 in Figure 3-15 of the previous section.

To configure the inline tool port pair:

1. In H-VUE, select **Ports > Inline Bypass > Inline Tools**.
2. Click **New**. The Inline Tool configuration page displays.
3. In the **Alias** field, type an alias that will help you remember which inline tool this Inline tool pair represents. For example, `Inline-Tool_SSLVA`.
4. In the Ports section, carefully select Port A and B ports that correspond to Side A and Side B of the network diagram.

   Important: It is essential these match Side A and B of the Inline Network port pairs.
5. Leave the default settings for the remaining configurations.
6. Click **Save**.

NOTE: The failure action for this inline tool is ToolBypass. This means the GigaVUE-HC2 will not send traffic to this inline tool if it is considered 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.

Configuring the GigaVUE-HC2 Inline Network Port Pair for the SSLVA

This section covers the steps needed to configure the GigaVUE-HC2's inline network port pair for the decrypted side of the SSLVA ports. Refer to the GigaVUE-HC2 blue Inline Tool links to and from the SV3800 in Figure 3-15.

To configure the network port pair, do the following;

1. In H-VUE, select to **Ports > Inline Bypass > Inline Networks**.
2. Click **New**. The Inline Network Info page displays.
3. In the **Alias** field, type an alias that will help you remember which network link this Inline Network bypass pair represents. For example, `Inline-Network_from_SSLVA`.
4. In the **Ports** section, for Port A either use the pull-down list or start typing the port label for the A side port as it is represented in the network topology diagram.

   Important: It is essential Side A and B of the GigaVUE-HC2 match the Side A and B of the SSLVA or traffic distribution for the Inline Tool Group will not work correctly.
5. For **Port B** either use the pull-down list or start typing the port label for the A side port as it is represented in the network topology diagram.
6. Change **Traffic Path** to **To Inline Tool**
7. Leave **Link Failure Propagation** set.
8. Click **Save**.

NOTE: If you are using BPS ports for the SSLVA inline network ports, the step will be similar to those covered in configuring in inline network bypass pair. Notably you will not be able to change the alias and port A and B are preselected.

Changing the Traffic Flow Maps

The traffic maps must now change to send the inline network group traffic first to the SSLVA for SSL traffic decryption before it is sent to the FireEye inline tool group for distribution across its members for malware inspection. The following are the high-level steps in this process:

1. Set Inline Networks to Physical Bypass. Refer to *Change the Physical Bypass Traffic Path*.

2. Delete the two existing traffic flow maps from the Inline Network to the FireEye Inline Tool Group, both the Bypass and Collector traffic flow maps. Refer to *Deleting the Existing Maps for FireEye*.
3. Create a new traffic flow maps to send all traffic from Inline Network Group to the one SSLVA inline Tool. Refer *Creating a New Inline Network Group to SSLVA Map*
4. Create a new traffic flow maps to send all traffic from the SSLVA Inline Network port pair (decrypted traffic) to the FireEye inline tool group. Refer to *Creating a New SSLVA to FireEye Maps: Bypass and Collector* and *Creating a New SSLVA to FireEye Collector Map*.

NOTE: To minimize packet loss, the steps include changing the Inline Network port pair to physical bypass while the traffic flow maps are changed. This is not required, only recommended.

Change the Physical Bypass Traffic Path

Enable physical bypass for the inline network pairs in the inline network group, by doing the following:

1. In H-VUE, select **Ports > Inline Bypass > Inline Networks**.
2. Check the box next to one of the Inline Network pair you configured in *Gigamon GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups*.
3. Click **Edit** so the properties page for that link displays.
4. Select **Physical Bypass** as shown in Figure 3-16, and then click **Save**.

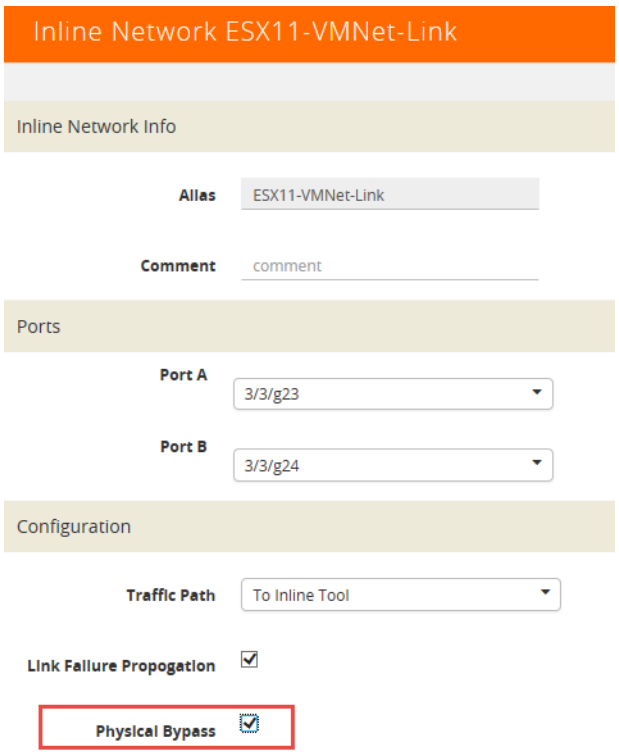


Figure 3-16: Inline Network Physical Bypass Enablement

5. Repeat steps 2 through 4 for the all other inline network pairs in the inline network group.

Configuring the Traffic Flow Maps

This section goes through the process of deleting the existing traffic flow maps and creating a new ones to logically put the Blue Coat SSLVA inline between the network links and the FireEye inline tool group.

Deleting the Existing Maps for FireEye

To delete the existing maps that you originally created for the FireEye appliance, do the following:

1. In H-VUE, **select Maps > Maps**.
2. Select the Collector traffic flow map from the Inline Network Group to the FireEye Tool Group.
3. Click **Delete**.
4. Select the Rule based Inline Network Group to FireEye Inline Tool Group.
5. Click **Delete**.

Creating a New Inline Network Group to SSLVA Map

To create a new map for the inline network tool group, do the following:

1. On the Maps page, click New.
2. Configure the new map as follows:
   - Map Alias: ING_to_SSLVA
   - Type: Inline
   - Sub Type: Pass All
   - Traffic Path: Normal
   - Traffic Type: Symmetric
   - Source: Select the Inline Network Group
   - Destination: Select the SSLVA Inline Tool

   For all other configurations, leave the defaults. The map configuration should look like the example shown in Figure 3-17.
3. Click **Save**.

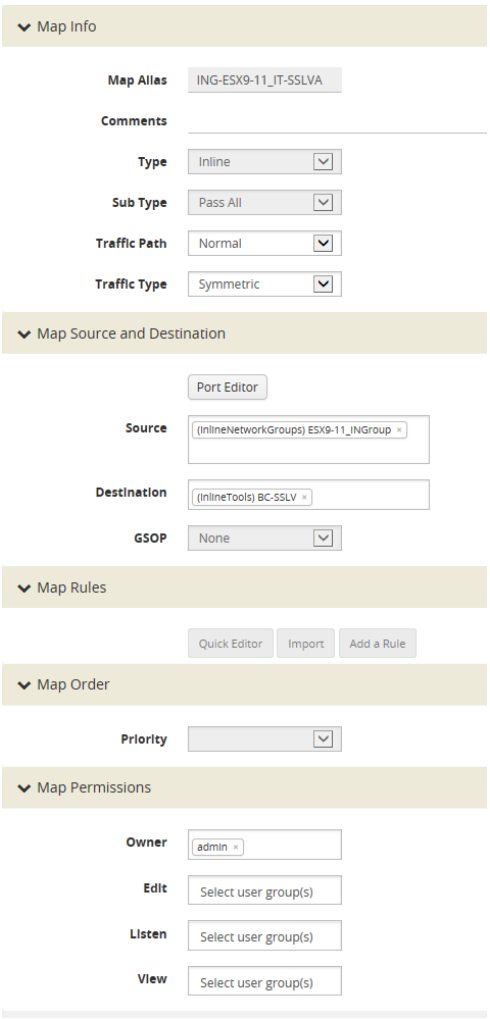


Figure 3-17: Inline Network Group to SSLVA Traffic Map

Creating a New SSLVA to FireEye Maps: Bypass and Collector

To create the bypass traffic map, do the following:

1. In the H-VUE, navigate to the Maps page, and then click **New**.
2. Configure the new map as follows:
   - Map Alias: Bypass_IN-SSLVA
   - Type: Inline
   - Sub Type: By Rule
   - Traffic Path: Bypasss
   - Source: Select the SSLVA Inline Network
   - Destination: None
   - Map Rule

     Click in the rule field, select **ip4Proto**, and then Select **Pass**, **Bi Directional**, and **IGMP** for IPv4 Protocol.

   The map configuration should look similar to the example shown in Figure 3-17.

3. Click **Save**.

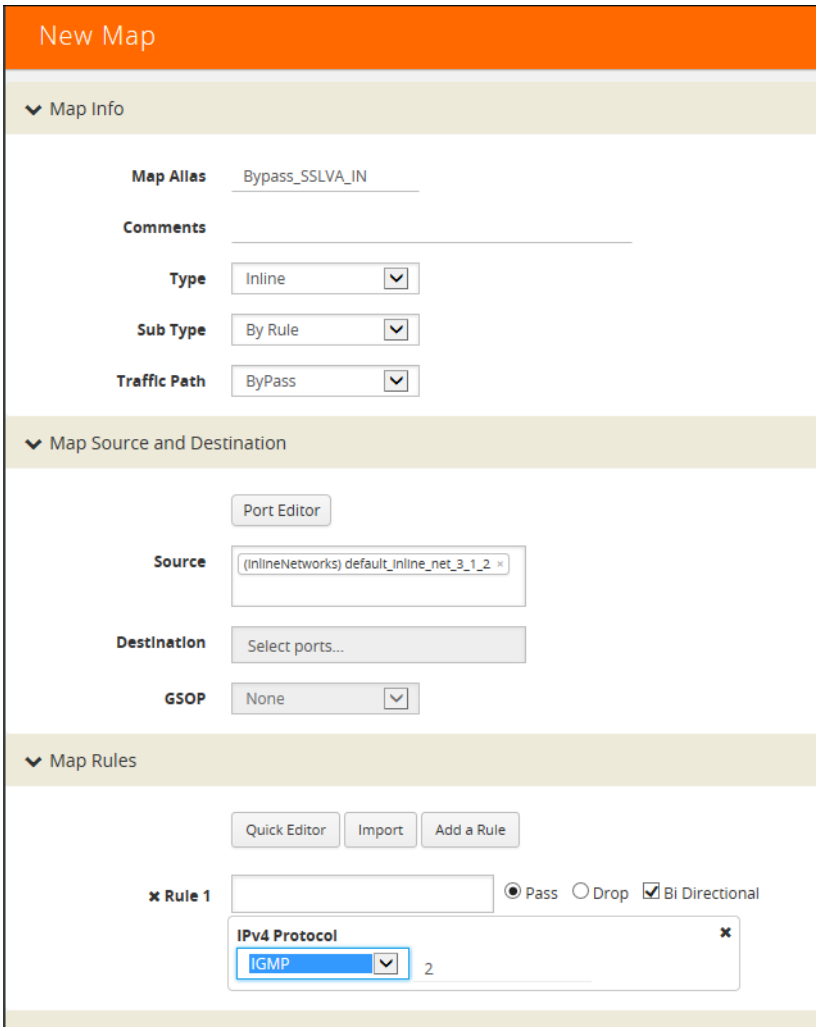


Figure 3-18: Inline Network Group to SSLVA Traffic Map

Creating a New SSLVA to FireEye Collector Map

To create a new collector map, do the following:

1. On the Maps page, click **New**.
2. Configure the map as follows:
   - Map Alias: Collector_IN-SSLVA_ITG_FE1-FE2
   - Type: Inline
   - Sub Type: Collector
   - Traffic Path: Normal
   - Source: Inline_Network_form_SSLVA (the alias for your SSLVA Inline Network)
   - Destination: ITGRP-FE1-FE2

   The map configuration should look similar to the example shown in Figure 3-19.
3. Click **Save**.

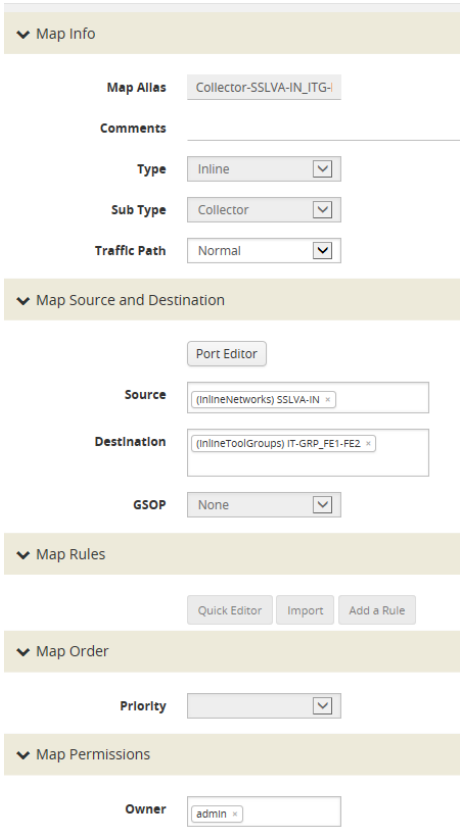


Figure 3-19: Collector SSLVA Inline Network To Fe Inline Tool Group Traffic Map

Removing Physical Bypass from the Inline Networks

To remove physical bypass from the inline networks, do the following:

1. In the H-VUE, select **Ports > Inline Bypass > Inline Networks**.
2. On the Inline Networks page, select one of the Inline Network pairs.
3. Click **Edit** so the properties page for that link displays.
4. Unselect **Physical Bypass**, and then click Save.
5. Repeat steps 2 through 4 for any other Inline Networks in the Inline Network Group.

Test SSLVA Decryption by Using FireEye SSL Test URLs

This section walks you through testing the combined solution of Blue Coat SSL decryption and FireEye malware detection by using the SSL version of FireEye's deployment test traffic.

NOTE: As of software version 3.8.5-16, Blue Coat does not support forwarding the Block/Comfort page to the requester's browser. This means that you will not see the "Access Denied" page for HTTPS blocked content.

Test SSLVA Decryption by Using FireEye SSL Test URLs

The general directions are the same as testing without the SSLVA in that you need to use approximately four workstations with sequentially increasing IP addresses. However, this time you will need to manually enter the URLs provided by FireEye because HTTPS will need to be inserted in the browser. The following are some links that you can use to make this easier:

https://fedeploycheck.fireeye.com/appliance-test/alert.html

https://fedeplycheck.fireeye.com/appliance-test/block.html

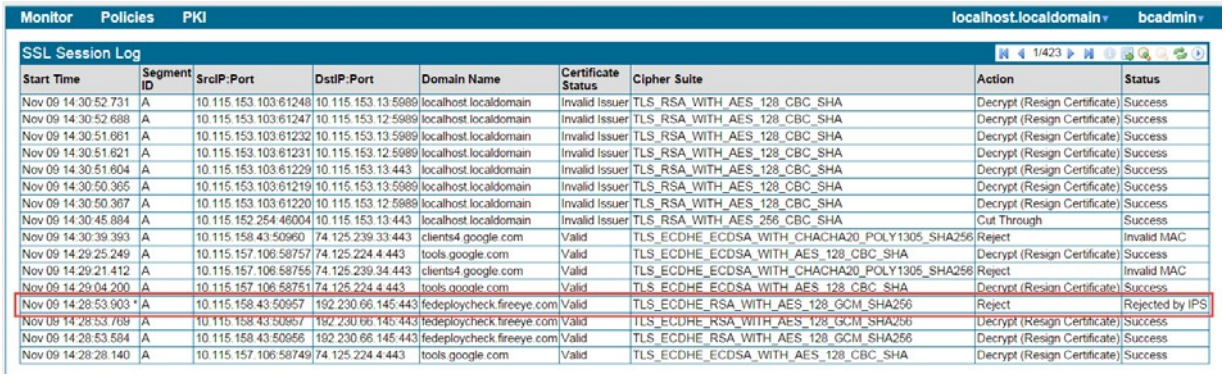
https://fedeplycheck.fireeye.com/appliance-test/test-infection.pdf https://fedeplycheck.fireeye.com/appliance-test/test-infection.exe

https://fedeploymentcheck.dns.fireeye.com

https://fedeplycheck.fireeye.com/appliance-test/test-infection.zip

You should have the same results as the earlier section where the traffic was not SSL traffic. This means that all the traffic from any given client IP address should go to only one of the members of the FireEye inline tool group.

To verify that SSL is being decrypted, log into the SSLVA and go to Monitor > SSL Session Log. You should be able to find the FireEye deployment test domain listed in the Domain Name column, Reject in the Action column, and Rejected by IPS in the Status column as shown in Figure 3-20.



Start Time	Segment ID	SrcIP:Port	DstIP:Port	Domain Name	Certificate Status	Cipher Suite	Action	Status
Nov 09 14:30:52.731	A	10.115.153.103:61248	10.115.153.13:5989	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:30:52.688	A	10.115.153.103:61247	10.115.153.12:5989	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:30:51.661	A	10.115.153.103:61232	10.115.153.13:5989	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:30:51.621	A	10.115.153.103:61231	10.115.153.12:5989	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:30:51.604	A	10.115.153.103:61229	10.115.153.13:443	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:30:50.365	A	10.115.153.103:61219	10.115.153.13:5989	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:30:50.367	A	10.115.153.103:61220	10.115.153.12:5989	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:30:45.884	A	10.115.152.254:46004	10.115.153.13:443	localhost.localdomain	Invalid Issuer	TLS_RSA_WITH_AES_256_CBC_SHA	Cut Through	Success
Nov 09 14:30:39.393	A	10.115.158.43:50960	74.125.239.33:443	clients4.google.com	Valid	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Reject	Invalid MAC
Nov 09 14:29:25.249	A	10.115.157.106:58757	74.125.224.4:443	tools.google.com	Valid	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:29:21.412	A	10.115.157.106:58755	74.125.239.34:443	clients4.google.com	Valid	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	Reject	Invalid MAC
Nov 09 14:29:04.200	A	10.115.157.106:58751	74.125.224.4:443	tools.google.com	Valid	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success
Nov 09 14:28:53.903 *	A	10.115.158.43:50957	192.230.66.145:443	fedeploycheck.fireeye.com	Valid	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Reject	Rejected by IPS
Nov 09 14:28:53.769	A	10.115.158.43:50957	192.230.66.145:443	fedeploycheck.fireeye.com	Valid	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Decrypt (Resign Certificate)	Success
Nov 09 14:28:53.584	A	10.115.158.43:50956	192.230.66.145:443	fedeploycheck.fireeye.com	Valid	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Decrypt (Resign Certificate)	Success
Nov 09 14:28:28.140	A	10.115.157.106:58749	74.125.224.4:443	tools.google.com	Valid	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success

Figure 3-20: Blue Coat SSLVA Session Log

Test Non-SSL Traffic Again

It is good practice to make sure non-SSL traffic is also going through the SSLVA to the FireEye inline tool group and being analyzed correctly. Repeat the same set of deployment tests, using the deployment test links provided by FireEye and described in the *Testing the Functionality of the FireEye Inline Tool*. You should see the alert counters reflect both the HTTPS and HTTP test you sent through.

Summary and Conclusions

The previous chapters showed how to deploy Gigavue-HC2 bypass protection with Blue Coat SSL decryption and 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 both Blue Coat SSL decryption and FireEye malware protection 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.

For issues related to Blue Coat products, visit http://www.bluecoat.com/techical-support to download the latest documentation and software, access the knowledgebase, or log a support ticket.

Appendix A

Configuration Sample

The following is an example of a configuration based on the instructions in the sections of this deployment guide.

```
HC2-C03-13 (config) # show run
##
## Running database "initial"
## Generated at 2015/11/10 23:29:20 +0000
## Hostname: HC2-C03-13
##
## Note: If you are not an admin user some command invocations may be
omitted
## because you do not have permissions to see them.
##

##
## Network interface configuration
##
interface eth0
create comment ""
no dhcp display
duplex auto
ip address 192.168.0.53 /21 mtu 1500
no shutdown speed
auto no zeroconf
exit

##
## Network interface IPv6 configuration
##
interface eth0
no ipv6 address autoconfig ipv6 address
autoconfig default
no ipv6 address autoconfig privacy no ipv6
dhcp client enable
ipv6 enable exit

##
## Routing configuration
##
ip default-gateway 192.162.0.1 eth0
##


## Other IP configuration
##
hostname HC2-C03-13
ip domain-list 192.168.0.22
ip name-server 192.168.0.20

##
## Other IPv6 configuration
##
no ipv6 enable

##
## AAA remote server configuration
##
```

```
# ldap bind-password ********
# radius-server key ********
# tacacs-server key ********

##
## Chassis level configurations
##
chassis box-id 1 serial-num C0036 type hc2

##
## Card level configurations
##
card slot 1/1 product-code 132-00BD
card slot 1/2 product-code 132-00BE
card slot 1/3 product-code 132-00B3
card slot 1/4 product-code 132-00BK
card slot 1/5 product-code 132-00AT
card slot 1/cc1 product-code 132-
00AN

##
## Port level configurations
##
port 1/1/x1    type inline-tool
port 1/1/x1 params admin enable autoneg
enable port 1/1/x10      type network
port 1/1/x11    type
inline-net port 1/1/x12
                type
inline-net port 1/1/x13
                type
network port 1/1/x14
                type
network port 1/1/x15
                type
network port 1/1/x16
                type
network port 1/1/x17
                type
network port 1/1/x18
                type
network port 1/1/x19
                type
network port 1/1/x2
                type
inline-tool
port 1/1/x2 params admin enable autoneg
enable port 1/1/x20      type network
port 1/1/x21    type
network port 1/1/x22
                 type
network port 1/1/x23
                 type
network port 1/1/x24
                 type
network port 1/1/x3
                type
network port 1/1/x4
                type
tool
port 1/1/x4 params admin
enable port 1/1/x5
                type network
port 1/1/x6    type network
port 1/1/x7  type network
port 1/1/x8  type network
port 1/1/x9  type network
port 1/2/q1  type network
port 1/2/q2  type network
port 1/2/q3  type network
```

```
port 1/2/q4  type network
port 1/2/q5  type network
port 1/2/q6  type network
port 1/3/g1  type network
port 1/3/g1 params taptx passive
port 1/3/g10    type network
port 1/3/g10 params taptx passive
port 1/3/g11    type network
port 1/3/g11 params taptx passive
port 1/3/g12    type network
port 1/3/g12 params taptx passive
port 1/3/g13    type network
port 1/3/g13 params taptx passive
port 1/3/g14    type network
port 1/3/g14 params taptx passive
port 1/3/g15    type network
port 1/3/g15 params taptx passive
port 1/3/g16    type network
port 1/3/g16 params taptx passive
port 1/3/g17    type network
port 1/3/g17 params taptx passive
port 1/3/g18    type network
port 1/3/g18 params taptx passive
port 1/3/g19    type network
port 1/3/g19 params taptx passive
port 1/3/g2   type network
port 1/3/g2 params taptx passive
port 1/3/g20    type network
port 1/3/g20 params taptx passive
port 1/3/g21    type inline-net
port 1/3/g21 params admin enable
port 1/3/g22    type inline-net
port 1/3/g22 params admin enable
port 1/3/g23    type inline-net
port 1/3/g23 params admin enable
port 1/3/g24    type inline-net
port 1/3/g24 params admin enable
port 1/3/g3   type network
port 1/3/g3 params taptx passive
port 1/3/g4   type network
port 1/3/g4 params taptx passive
port 1/3/g5   type network
port 1/3/g5 params taptx passive
port 1/3/g6   type network
port 1/3/g6 params taptx passive
port 1/3/g7   type network
port 1/3/g7 params taptx passive
port 1/3/g8   type network
port 1/3/g8 params taptx passive
port 1/3/g9   type network
port 1/3/g9 params taptx passive
port 1/4/x1   type network
port 1/4/x10   type network
port 1/4/x11   type inline-
tool
port 1/4/x11 params admin
enable port 1/4/x12
               type inline-
tool port 1/4/x12 params
admin enable port 1/4/x13
               type inline-
tool
port 1/4/x13 params admin enable autoneg
enable port 1/4/x14      type inline-tool
port 1/4/x14 params admin enable autoneg
enable port 1/4/x15      type inline-tool
port 1/4/x15 params admin enable autoneg
enable port 1/4/x16      type inline-tool
port 1/4/x16 params admin enable autoneg
enable port 1/4/x2type network
port 1/4/x3   type
network port 1/4/x4
```

```
              type
network port 1/4/x5
              type
network port 1/4/x6
              type
network port 1/4/x7
              type
inline-net
port 1/4/x7 params admin
enable port 1/4/x8
              type inline-
net port 1/4/x8 params
admin enable port 1/4/x9
              type network

##
## Gigastream configurations
##
gigastream advanced-hash slot 1/cc1 default

##
## Gsgroup configurations
##
gsgroup alias gsgrp-1_4_e1 port-list 1/4/e1

##
## Gs params configurations
##
gsparams gsgroup gsgrp-1_4_e1
  cpu utilization type total rising
  80 dedup-action drop
  dedup-ip-tclass
  include dedup-ip-
  tos include dedup-
  tcp-seq include
  dedup-timer 500000
  dedup-vlan ignore
  flow-sampling-rate 5
  flow-sampling-timeout 1
  flow-sampling-type
  device-ip gtp-flow
  timeout 48
  gtp-persistence disable
  gtp-persistence file-age-timeout 30
  gtp-persistence interval 10
  gtp-persistence restart-age-time
  30 gtp-whitelist add MyIMSIs
  ip-frag forward
  enable ip-frag
  frag-timeout 10
  ip-frag head-session-timeout
  30 lb failover disable
  lb failover-thres lt-bw 80
  lb failover-thres lt-pkt-rate
  1000 lb replicate-gtp-c disable
  lb use-link-spd-wt disable
  resource buffer-asf disable
  ssl-decrypt decrypt-fail-action drop
  ssl-decrypt enable
  ssl-decrypt key-cache-timeout 10800
  ssl-decrypt non-ssl-traffic drop
  ssl-decrypt pending-session-timeout 60
  ssl-decrypt session-timeout 300
  ssl-decrypt tcp-syn-timeout 20
  ssl-decrypt ticket-cache-timeout 10800  exit

##
## Gsop configurations
##
```

```
gsop alias GTP-Flowsample flow-ops gtp-flowsample lb app gtp metric  hashing
key imsi port-list gsgrp-1_4_e1
gsop alias gtp-whitelist flow-ops gtp-whitelist lb app gtp metric hashing
key imsi port-list gsgrp-1_4_e1

##
## Vport configurations
##
vport alias vport1 gsgroup gsgrp-1_4_e1

##
## Inline-network configurations
##
inline-network alias InLineNetwo  lfp
  enable
  physical-bypass disable
  traffic-path to-inline-tool
  exit
inline-network alias InLineNetworkPair1
  pair net-a 1/3/g21 and net-b 1/3/g22  lfp
  enable
  physical-bypass disable
  traffic-path to-inline-tool
  exit
inline-network alias InlineNetwork4BC
  pair net-a 1/4/x7 and net-b 1/4/x8  lfp
  enable
  physical-bypass disable
  traffic-path to-inline-tool
  exit
inline-network alias InlineNetworkPair2
  pair net-a 1/3/g23 and net-b 1/3/g24  lfp
  enable
  physical-bypass disable
  traffic-path to-inline-tool
  exit

##
## Inline-network-group configurations
##
inline-network-group alias ESX12_INGroup
  network-list InLineNetworkPair1,InlineNetworkPair2  exit

##
## Inline-tool configurations
##
inline-tool alias ITFireEye1
  pair tool-a 1/4/x13 and tool-b 1/4/x14
  enable
  exit
inline-tool alias ITFireEye2
  pair tool-a 1/4/x15 and tool-b 1/4/x16
  enable
  exit
inline-tool alias InlineToolBC
  pair tool-a 1/4/x11 and tool-b 1/4/x12
  enable
  exit

##
## Inline-tool-group configurations
##
inline-tool-group alias ITG-Fe1-
  fe2 tool-list
  ITFireEye1,ITFireEye2  enable
  hash a-srcip-b-
  dstip  exit

##
```

```
## Traffic map connection configurations
##
map alias
  PassAll2FEs type
  inline byRule
  roles replace admin to owner_roles
  rule add pass macsrc 00:00:00:00:00:00 00:00:00:00:00:00 bidir
  to ITG-Fe1-fe2
  from
  InlineNetwork4BC
  exit
map-passall alias ING_to_SSLVA
  roles replace admin to
  owner_roles to InlineToolBC
  from
  ESX12_INGroup
  exit

##
## X.509 certificates configuration
##
#
# Certificate name system-self-signed, ID
316ea8f8a0b6980795515b55d2d377477379aeb2
# (public-cert config omitted since private-key config is hidden)


##
## Web configuration
##
# web proxy auth basic password ********
web auto-logout 30

##
## E-mail configuration
##
# email auth password ********
# email autosupport auth password ********
```

See Inside Your Network™

4051-02 12/15