Deployment Guide:
Flexible Inline Arrangements
GigaVUE-OS 5.3

Document Revision - 06/05/2018

Table of Contents

Overview

Flexible Inline framework guides various inline traffic flows in an inline network or among different inline networks through a user-defined sequence of inline tools and/or inline tool groups. It overcomes the limitation with classic inline wherein a sequence of inline tools / inline tool groups used for inspecting traffic on a given inline network / inline network group cannot be reused for inspecting traffic on another inline network / inline network group.

Traffic matching a flexible inline flow map is tagged with a unique VLAN ID as opposed to the classic inline flow map that tags traffic based on the member port receiving traffic in an inline network group. This key differentiator allows users to pick and choose traffic from various inline networks using flow maps and guide them through a sequence of tools that are of interest. Each inline flow map can be configured to guide traffic to arbitrary sequence of tools and the tools can be shared among multiple flow maps. The GigaVUE-OS lets user to either automatically or manually assign VLAN ID to a flexible inline flow map.

Inline network group and inline tool serial are not applicable for the Flexible Inline Arrangements. Multiple flexible inline flow maps associated with inline networks achieve the inline network group functionality. Inline tool serial is not needed as the flexible inline arrangements allow for the same configuration without the inline serial construct.

Flexible Inline Solution Highlights

- Flexible inline flow map assigns a unique VLAN ID for the matching traffic.
- Flexible inline flow map guides traffic through arbitrary sequence of inline tools and inline tool groups.
- Unlike the classic inline flow maps, flexible inline flow maps do not require a separate map for guiding traffic to out-of-band tools.
- Flexible inline flow maps are of two types, by rule and collector. Unlike the classic inline flow maps, there is no passall map. The collector map acts as a passall map in the absence of a rule based map.
- Flexible inline flow maps enable traffic in each direction to be bypassed or inspected by identical or different set of inline tools in the same or reverse order.

Deployment Checklist

Before deploying the Flexible Inline arrangements, it is strongly recommended

- To familiarize the feature by reviewing the latest ***Flexible Inline Arrangements Guide.***
- To review ***GigaVUE-OS Release Notes*** for any known issues that may impact your use case.
- To review the following checklist

Pre-deployment checklist

- Gigamon device must be upgraded to GigaVUE-OS 5.3 or later.
- GigaVUE-FM supports workflow based configuration to ease deploying Flexible Inline Arrangements. Install or upgrade GigaVUE-FM to 5.3 or later.
- Analyze traffic flow by capturing pcaps with existing setup to identify the required flow maps and the associated packet attributes for filtering in appropriate traffic.
- When the network traffic is VLAN tagged, ensure the inline tools support Q-in-Q tagged frames with outer and inner TPIDs carrying 0x8100.
- Prioritize and deploy Flexible Inline Solution in phases for each traffic flow by interleaving a pre-defined monitoring period before proceeding with the next phase.
- It is recommended to deploy inline solution in fail open mode (i.e. for the network connectivity to remain up in case of Gigamon device failures) using protected inline network links.
- For optimal use of the internal resources, we recommended you have minimal flexible inline flow maps.
- Addition or deletion of inline-tools / inline-tool-groups in a tool sequence is supported.
- Verify that email notifications are configured for at least the following events. Refer to **Notifications** section in **GigaVUE-FM Users Guide**.

systemreset:	System Reset
modulechange:	Module Change
linkspeedstatuschange:	Link Status or Speed Change
watchdogreset:	Watchdog Reset
processcrash:	A process in the system has crashed
processexit:	A process in the system unexpectedly exited
livenessfailure:	A process in the system was detected as hung
cpuutilhigh:	CPU utilization has risen too high
cpuutilok:	CPU utilization has fallen back to normal levels
memusagehigh:	Memory usage has risen too high
memusageok:	Memory usage has fallen back to acceptable levels
interfaceup:	An interface's link state has changed to up
interfacedown:	An interface's link state has changed to down
switchcputemp:	Switch CPU temperature notification
cputemp:	CPU temperature notification

- As a best practice, take backup of the existing configuration to make sure that the configuration can be restored in case any untoward issues were to be encountered while deploying the solution.

Deployment checklist

- At the outset, protected inline network(s) must have Physical Bypass enabled. After deploying the Flexible Inline Solution, it is strongly recommended to set the Traffic Path to bypass (i.e. logical bypass) and to disable the Physical Bypass of inline network(s) to make sure that the map rules are configured appropriately; the Traffic Path can be set to to-inline-tool thereafter.
- When a network port is shared among different maps, traffic is redirected based on the order in which the maps are configured or prioritized. As a rule of thumb, it is recommended to configure maps with more specific rules first before configuring maps with less specific or generic rules.
- Review priority of the configured flow maps while updating the rule sets or while creating new maps and adjust them as required.
- Shared mode must be enabled for inline tool(s) to be used in flexible inline flow maps.
- Inline tools must be configured in transparent mode to seamlessly work with Flexible Inline Solution.

  NOTE: Heartbeat should be enabled for inline tools to trigger failover actions. If an inline tool is deployed in a non-transparent mode, the heartbeat messages would not be received. Hence, the inline tool will be deemed as operationally down.
- Make sure that inline network and inline tool links do not report any link errors or discards.
- Plan to have a laptop connected to a tool port on the Gigamon device. If inline network traffic must be analyzed, inline network out-of-band map can be configured with the tool port as the destination.

Post-deployment checklist

- As a best practice, take backup of the configuration after the deployment for reference.
- If inline tools' sequence or if map rules must be modified, it is strongly recommended to enable Physical Bypass on protected inline network(s) before proceeding, and to enable the Physical Bypass after modifying the config.
- Monitor for a pre-defined period before proceeding with the next batch of deployment.

Unsupported

- Editing the tools in an inline tool group is restricted in GigaVUE-OS 5.3.
- Flexible inline flow maps cannot use Inline tool / inline-tool-group that are already in use by classic inline or inline-SSL flow maps.
- Inline SSL GigaSMART Operation (GSOP) cannot be used in flexible inline maps in GigaVUE-OS 5.3.
- Asymmetrical hashing to an inline tool group is not supported in which one direction to hash is based on source IP and the other direction to hash is based on destination IP address.

Use Cases

Selectively guiding and load balancing traffic flows to inline tools

This use case illustrates Flexible Inline Solution's ability to enable enterprises to selectively guide web (i.e. HTTP and HTTPS) and non-web traffic, and load balance them among multiple Advance Persistent Threat (APT) Systems and multiple Web Application Firewalls (WAF) for inspection as illustrated below.

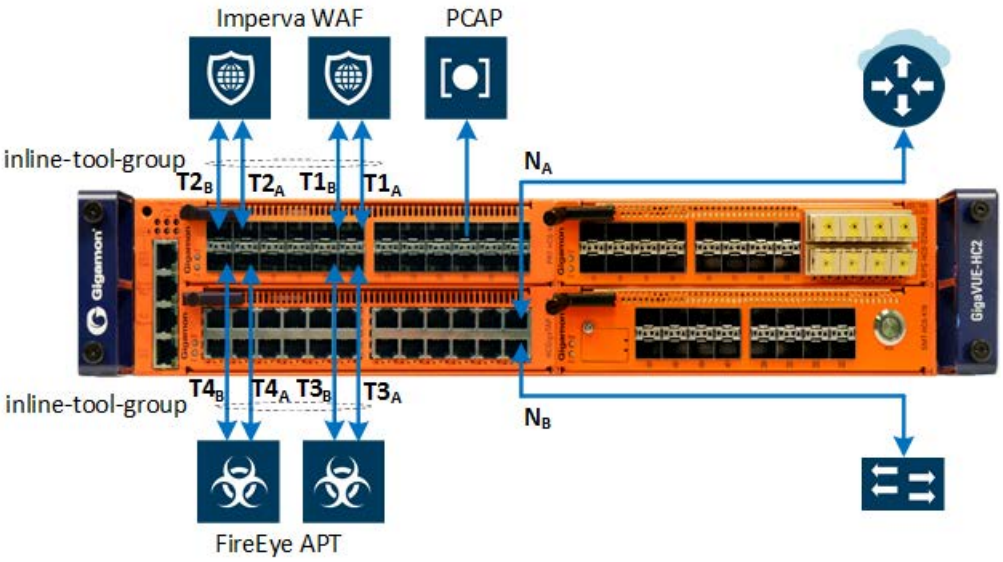


Figure 1: Flexible Inline Solution deployment for selectively guiding and load balancing different traffic flows among multiple inline tools

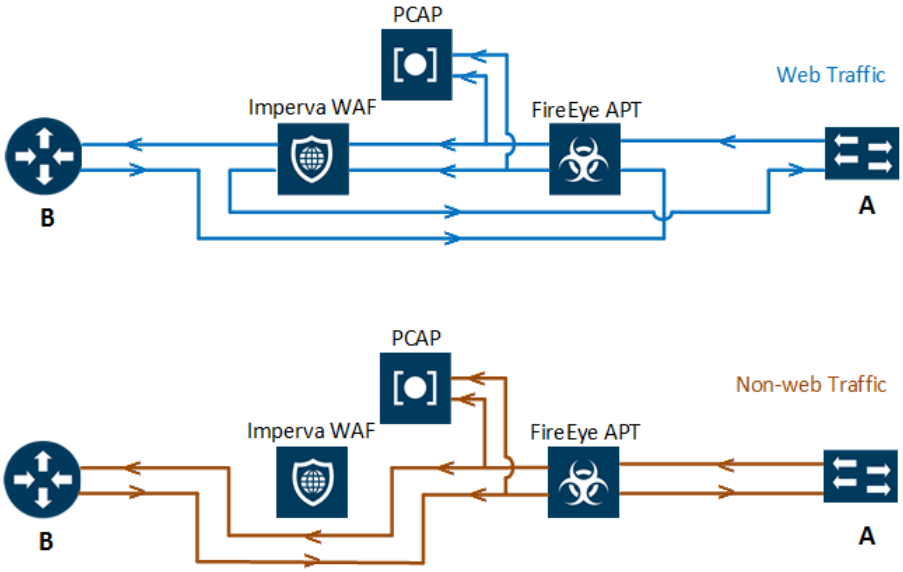


Figure 2: Traffic flow enabled by the Flexible Inline Solution

Requirements

Traffic flow: Web traffic must be inspected by both FireEye APT and Imperva WAF and the traffic must also be load balanced among the inline tools. Non-web traffic must be inspected by FireEye APT alone and the traffic must be load balanced among the APTs. Traffic traversing the FireEye APTs must be captured for verification.

Inline Network requirements: A protected inline network link is required. The network traffic will be tagged. Until the flow maps are configured, Physical Bypass must be enabled on the inline network to make sure that the network traffic is not affected.

Inline Tool requirements: Both FireEye APTs and Imperva WAFs must be configured as inline tool group respectively. By default, the flexible inline flow maps will insert additional VLAN tag for the matching traffic. Hence, the inline tools must be capable of handling Q-in-Q (with outer and inner TPIDs carrying 0x8100).

Out-of-band tool *requirements*: The traffic traversing FireEye APTs must be verified using packet capture. The out-of-band traffic must carry the same tag as that of the inline network traffic. A VM with Wireshark installed must be connected to a tool port for monitoring.

Configuration

The following prerequisite tasks must be completed before deploying the Flexible Inline Solution.

Prerequisites:

1. Configure the type as inline network for ports N_{A-B}.
2. Configure the type as inline tool for ports $T1_{A-B}$, $T2_{A-B}$, $T3_{A-B}$ and $T4_{A-B}$.
3. Configure the type as tool for port connecting to the VM.

Refer to **Configuring Ports** in the **Configuration Tasks** section of this document for the detailed steps.

To deploy Flexible Inline Solution:

1. Create protected inline network link using ports N_{A-B}.

   NOTE: Physical Bypass should be enabled for the inline network links until the flow maps are configured to ensure that the network traffic is not affected.

2. Create inline tool links corresponding to the inline tool ports connecting to each of the Imperva WAFs ($T1_{A-B}$ and $T2_{A-B}$) and the FireEye APTs ($T3_{A-B}$ and $T4_{A-B}$).

   NOTE: Shared mode must be set to True, and **Regular heartbeat** should be enabled for dynamically detecting inline tool failures and triggering the failover action.

3. Create inline tool groups, one corresponding to the FireEye APTs and the other to the Imperva WAFs.
4. Create a flexible inline by rule map with two rules, one corresponding to filtering in bidirectional HTTP traffic (protocol TCP with destination port 80) and the other to filtering in bidirectional HTTPS traffic (protocol TCP with destination port 443), and to send them from A-to-B via each of the inline tool groups corresponding to the FireEye APTs and the Imperva WAFs.
5. Configure out-of-band copy to feed the traffic egressing the FireEye APT inline tool group to the VM.

   Traffic in the other direction, B-to-A, should be configured to traverse the same path as A-to-B as illustrated by the traffic flows.

6. Create a flexible inline collector map to filter in all other traffic and to send them from direction A-to-B (and B-to-A) to the FireEye APT inline tool group.

Flexible Inline Arrangements Workflow in GigaVUE-FM provides intuitive drag and drop option for deploying the Flexible Inline Solution.

To launch the workflow:

1. Select the device from **FM Navigation Pane > Physical Nodes**.
2. Select device **Navigation Pane > Workflows > Flexible Inline Arrangements**. Refer to **Using Flexible Inline Flow Configuration Workflow** in the **Configuration Tasks** section for the detailed steps.
3. After configuring the flow maps, the inline network should have **Physical Bypass** disabled and its **Traffic Path** must be set to to-inline-tool for allowing the traffic to flow through the Gigamon device. Refer to **Updating Inline Network Settings** in the **Configuration Tasks** section of this document for the detailed steps.

Gigamon device's CLI configuration:

flexInline-useCase01-config.txt

DOWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify the Flexible Inline Solution

1. Ports' health and statistics
2. Inline network health
3. Inline tool health
4. Inline tool group health
5. Map health and statistics

Refer to **Verification Tasks** section of this guide for the detailed steps.

Selectively decrypting inline SSL traffic and guiding traffic to inline tools

Gigamon devices support profile based inline SSL decryption/encryption of both inbound and outbound SSL sessions. This use case describes guiding decrypted outbound traffic among inline tools for inspection as illustrated below.

Inline SSL GigaSMART Operation (GSOP) cannot be used in flexible inline maps in GigaVUE-OS 5.3. The decrypted traffic must be physically looped back in to the Gigamon device to apply flexible inline maps for guiding the decrypted traffic.

Refer to the latest *Inline SSL Decryption Guide* and *Inline SSL Deployment Guide* for additional information about GigaSECURE® Inline SSL Solution.

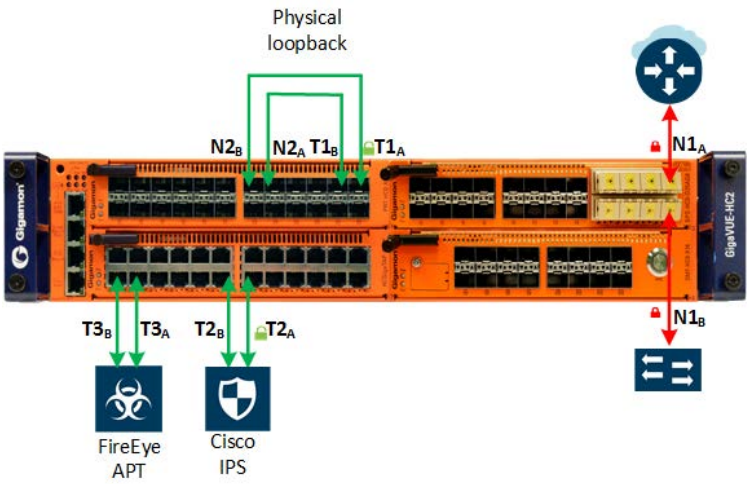
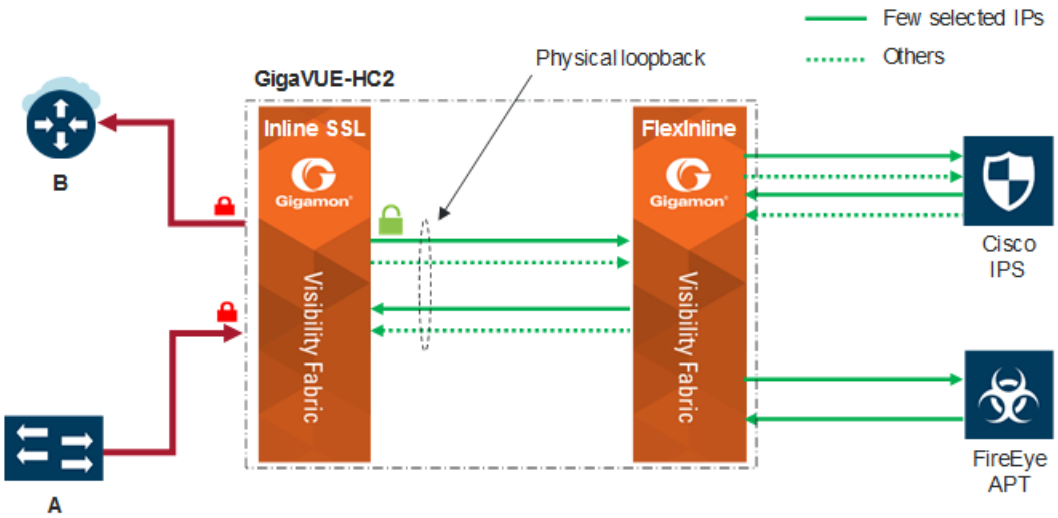


Figure 3: Gigamon Inline SSL and Flexible Inline Solution



Note: Traffic in the opposite direction flows in the same order as illustrated.

Figure 4: Traffic flow illustrating inline SSL inspection

Requirements

Traffic flow: Traffic destined to few selected applications must be inspected by Cisco IPS and FireEye APT in both directions, A-to-B and B-to-A. Rest of the traffic must be inspected by Cisco IPS alone.

Inline Network requirements: A protected inline network link is required. The network traffic will be tagged. Until the flow maps are configured, Physical Bypass must be enabled on the inline network to make sure that the network traffic is not affected.

Inline Tool requirements: By default, the flexible inline flow maps will insert additional VLAN tag for the matching traffic. Since the network traffic is tagged, the inline tools must be capable of handling Q-in-Q traffic (with outer and inner TPIDs carrying 0x8100).

Signing CA requirements: Servers with only the valid certificates must be accepted for decryption.

Configuration

Below steps illustrate deploying Inline SSL Solution followed by the Flexible Inline Solution.

Configuration pre-requisites for deploying Inline SSL Solution:

1. Unlock the Keychain Password.
2. Install a key pair in the Key Store.

   NOTE: A self-signed key pair can also be generated on the Gigamon device for the purpose. However, it is recommended to use the one provided by the InfoSec team.

3. Configure the Signing CA.
   a. Map the installed key pair to the Primary Signing CA.

      NOTE: If the Primary Signing CA is not configured, the Gigamon device will operate as a TCP proxy. The Primary Signing CA certificate must also be installed in clients' browser so that it can validate the certificate without reporting any warning.

4. Create the inline SSL policy profile.
   a. Since only the valid server certificates must be accepted for decryption, retain the Security Exceptions with the default values (i.e. drop).

      NOTE: Should any Security Exception must be changed to decrypt, it is strongly recommended to install another key pair in the inline SSL key store and map it to the Secondary Signing CA.

   b. Since traffic destined to few selected applications must be inspected, the default action should be retained as no decrypt and Policy Rules must be defined corresponding to the IP address of the applications for decryption.

The **Inline SSL Configuration workflow** in GigaVUE-FM walks through each of the above tasks.

To launch the workflow:

1. Select the device from **FM Navigation Pane > Physical Nodes**.
2. Select device **Navigation Pane > Workflows > Inline GigaSMART Operations**.
3. Refer to **Using Inline SSL Configuration Workflow** in the **Configuration Tasks** section for the detailed steps.

Steps for deploying the Inline SSL Solution:

1. Configure protected inline network link using ports $N1_{A-B}$.

   NOTE: Physical Bypass should be enabled for the inline network links until the flow maps are configured to ensure that the network traffic is not affected.

2. Configure inline tool link using ports $T1_{A-B}$.

   NOTE: The inline tool should be a physical fiber loopback as illustrated in the above physical topology. **Shared mode** for the inline tool must be set to False so inline ssl does not append an extra tag. Ensure all network traffic is directed to the GigaSMART engine. Steps corresponding to deploying the flexible inline solution provides instruction for guiding traffic through the other inline tools.

3. Configure GS Group

4. Configure Virtual Port
5. Configure Inline SSL GS Operation
6. Configure flow maps: Based on the earlier observations, below flow maps must be configured.
   a. *Inline First Level Map*: To filter in all traffic from the inline network and send it to the virtual port for decryption.
   b. *Inline Second Level Map*: To decrypt traffic received on the virtual port by using Inline SSL GSOP, and send both the decrypt traffic and the no decrypt traffic to the inline tool.

Inline SSL Map workflow in GigaVUE-FM walks through each of the above steps. Select any flow from the workflow and skip steps corresponding to configuring the classic inline map and the shared collector map.

To launch the workflow:

1. Select the device from **FM Navigation Pane > Physical Nodes**.
2. Select device **Navigation Pane > Workflows > Inline GigaSMART Operations**.
3. Refer to **Using Inline SSL Map Workflow** in the **Configuration Tasks** section for the detailed steps.

Configuration pre-requisites for deploying Flexible Inline Solution:

1. Configure the type as inline network for ports $N2_{A-B}$.
2. Configure the type as inline tool for ports for $T2_{A-B}$ and $T3_{A-B}$.

Refer to **Configuring Ports** in the **Configuration Tasks** section of this document for the detailed steps.

To deploy Flexible Inline Solution:

1. Create inline network link using ports $N2_{A-B}$.
2. Create inline tools corresponding to the inline tool ports connecting to IPS ($T2_{A-B}$) and APT ($T3_{A-B}$).

   NOTE: Shared mode must be set to True, and **Regular heartbeat** should be enabled for dynamically detecting inline tool failures and triggering the failover action.
3. Create a flexible inline by rule map with rules to filter in bidirectional traffic corresponding to the IP address of the applications and to send them from direction A-to-B via IPS and APT.

   Traffic in the other direction, B-to-A, should be configured to traverse the same path as A-to-B as illustrated by the traffic flow.
4. Create a flexible inline collector map to filter in all other traffic and to send them from direction A-to-B (and B-to-A) to the Cisco IPS.

Flexible Inline Arrangements Workflow in GigaVUE-FM provides intuitive drag and drop option for deploying the Flexible Inline Solution.

To launch the workflow:

1. Select the device from **FM Navigation Pane > Physical Nodes**.
2. Select device **Navigation Pane > Workflows > Flexible Inline Arrangements**. Refer to **Using Flexible Inline Flow Configuration Workflow** in the **Configuration Tasks** section for the detailed steps.

3. After configuring the flow maps, the inline network should have **Physical Bypass** disabled and its **Traffic Path** must be set to to-inline-tool for allowing the traffic to flow through the Gigamon device. Refer to **Updating Inline Network Settings** in the **Configuration Tasks** section of this document for the detailed steps.

Gigamon device's CLI configuration:

flexInline-useCase02-config.txt

DOWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify the Flexible Inline Solution

1. Ports' health and statistics
1. Inline network health
2. Inline tool health
3. Inline tool group health
4. Map health and statistics
5. Virtual port or GSOP statistics
6. InlineSSL session summary
7. InlineSSL session runtime statistics

Refer to **Verification Tasks** section of this guide for the detailed steps.

Deploying external inline SSL interception and guiding traffic to inline tools

Flexible Inline Solution can help in deploying external inline SSL interception and in guiding traffic to more than one tool as illustrated below.

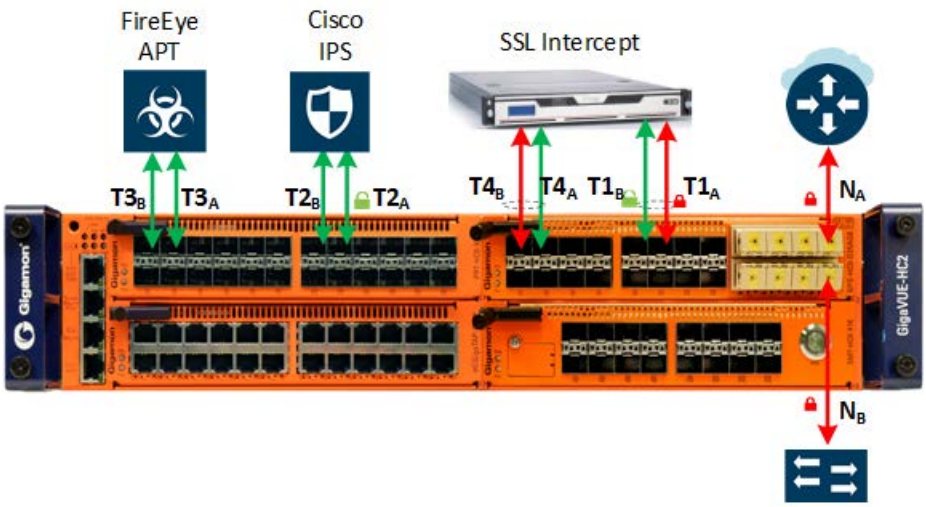


Figure 5: Enabling inline SSL inspection

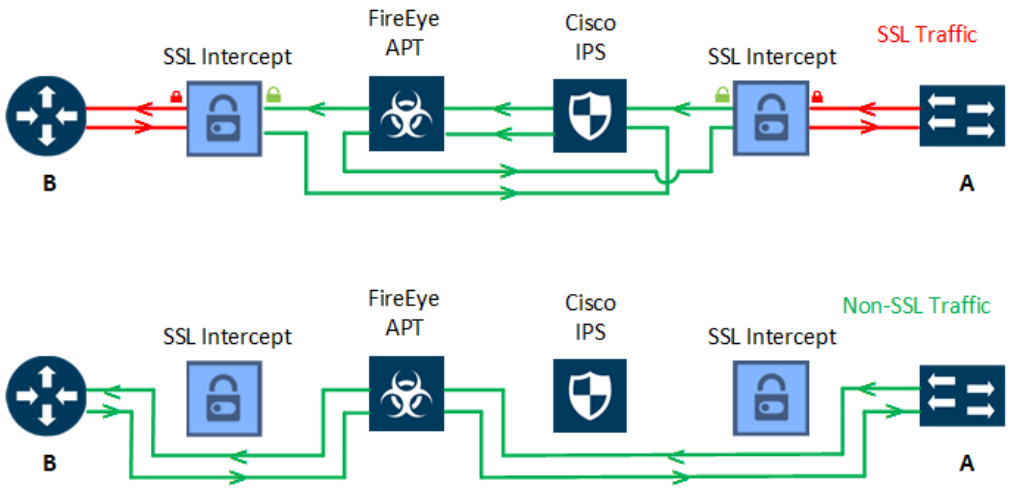


Figure 6: Traffic flow illustrating inline SSL inspection

Requirements

Traffic flow: HTTPS network traffic in both directions, A-to-B and B-to-A, must first be forwarded to an external SSL intercept device. Thereafter, the decrypted traffic must be forwarded to Cisco IPS and FireEye APT for inspection. All other traffic must be forwarded to the FireEye APT.

Inline Network requirements: A protected inline network link is required. The network traffic will be tagged. Until the flow maps are configured, Physical Bypass must be enabled on the inline network to make sure that the network traffic is not affected.

Inline Tool requirements: By default, the flexible inline flow maps will insert additional VLAN tag for the matching traffic. Since the network traffic is tagged, all inline tools (i.e. SSL Intercept, Cisco IPS and FireEye APT) must be capable of handling Q-in-Q traffic.

Configuration

The following prerequisite tasks must be completed before deploying the Flexible Inline Solution.

Prerequisites:

1. Configure the type as inline network for ports $N_{A\text{-}B}$.
2. Configure the type as inline tool for ports $T1_{A\text{-}B}$ (SSL Intercept), $T2_{A\text{-}B}$ (Cisco IPS), $T3_{A\text{-}B}$ (FireEye APT) and $T4_{A\text{-}B}$ (SSL Intercept).

Refer to **Configuring Ports** in the **Configuration Tasks** section of this document for the detailed steps.

To deploy Flexible Inline Solution:

1. Create protected inline network link using ports $N_{A\text{-}B}$.

   NOTE: Physical Bypass should be enabled for the inline network links until the flow maps are configured to ensure that the network traffic is not affected.

2. Create inline tools links corresponding to $T1_{A\text{-}B}$ (SSL Intercept), $T2_{A\text{-}B}$ (Cisco IPS), $T3_{A\text{-}B}$ (FireEye APT) and $T4_{A\text{-}B}$ (SSL Intercept) inline tool port pairs.

   NOTE: Shared mode must be set to True, and **Regular heartbeat** should be enabled for dynamically detecting inline tool failures and triggering the failover action.

3. Create a flexible inline by rule map to guide network traffic from direction A-to-B via $T1_{A-B}$ (SSL Intercept), $T2_{A-B}$ (Cisco IPS), $T3_{A-B}$ (FireEye APT) and $T4_{A-B}$ (SSL Intercept), and that from direction B-to-A to traverse $T4_{A-B}$ (SSL Intercept), $T2_{A-B}$ (Cisco IPS), $T3_{A-B}$ (FireEye APT) and $T1_{A-B}$ (SSL Intercept) as illustrated by the traffic flows.
4. Create a flexible inline collector map to filter in all other traffic and to send them from direction A-to-B (and B-to-A) to the FireEye APT.

Flexible Inline Arrangements Workflow in GigaVUE-FM provides intuitive drag and drop option for deploying the Flexible Inline Solution.

To launch the workflow:

1. Select the device from **FM Navigation Pane > Physical Nodes**.
2. Select device **Navigation Pane > Workflows > Flexible Inline Arrangements**. Refer to **Using Flexible Inline Flow Configuration Workflow** in the **Configuration Tasks** section for the detailed steps.
3. After configuring the flow maps, the inline network should have **Physical Bypass** disabled and its **Traffic Path** must be set to to-inline-tool for allowing the traffic to flow through the Gigamon device. Refer to **Updating Inline Network Settings** in the **Configuration Tasks** section of this document for the detailed steps.

Gigamon device's CLI configuration:

flexInline-useCase03-config.txt **DOWNLOAD from PDF Attachments**

Monitoring

Monitor the following to verify the Flexible Inline Solution

1. Ports' health and statistics
2. Inline network health
3. Inline tool health
4. Inline tool group health
5. Map health and statistics

Refer to **Verification Tasks** section of this guide for the detailed steps.

Configuration Tasks

This section provides steps for the following tasks

- Configuring Ports
- Using Flexible Inline Flow Configuration Workflow
- Using Inline SSL Configuration Workflow
- Using Inline SSL Map Workflow
- Updating Inline Network Settings

Configuring Ports

a. Go to device **Navigation Pane > Traffic > Ports**.

b. Select port(s) that must be configured as type inline network.

c. Click **Edit** from the **Ports** menu.

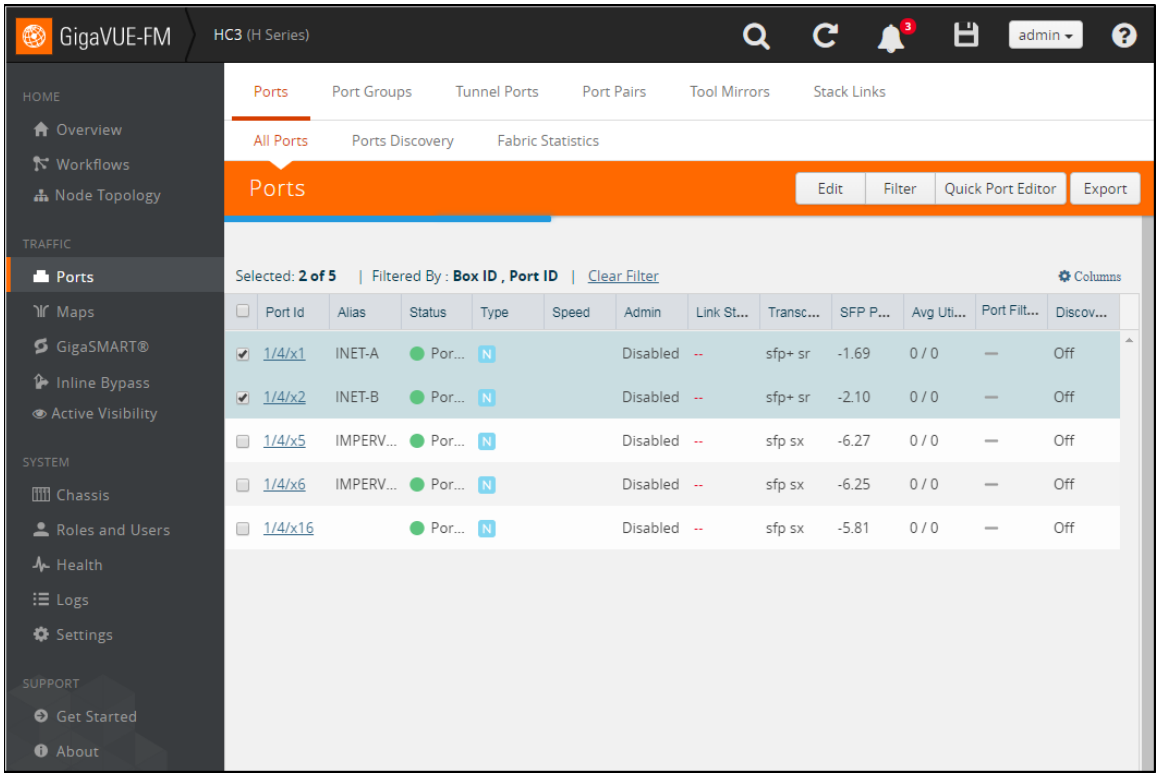


Figure 7 Configure Ports

d. Provide details as illustrated below and click **OK**.

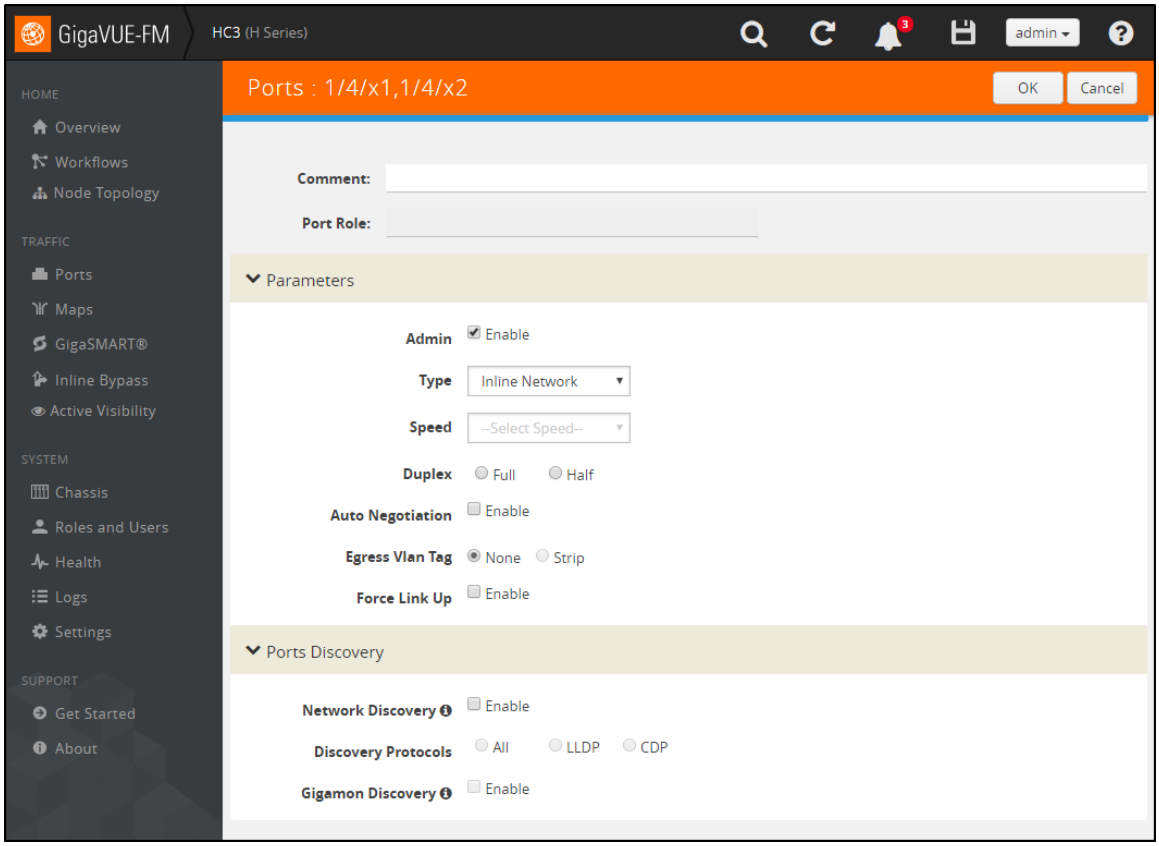


Figure 8 Port Paramters

e. Click **Floppy-Disk** icon in the top Right-hand corner to save the device configuration to the nonvolatile memory.

NOTE: Similar steps as described above should be followed for configuring ports with type inline tool, tool or hybrid.

Using Flexible Inline Flow Configuration Workflow

To launch the workflow:

1. Select the device from **FM Navigation Pane > Physical Nodes**.
2. Select device **Navigation Pane > Workflows > Flexible Inline Arrangements**.

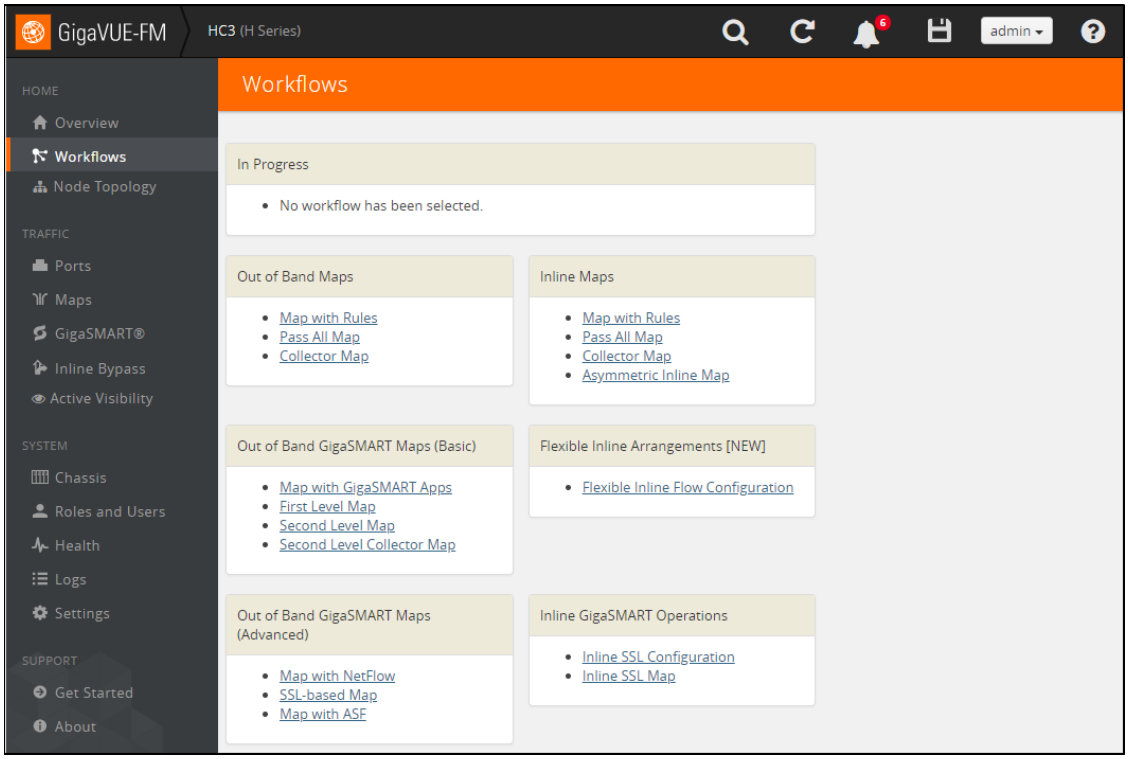


Figure 9 Workflows

3. Configure new inline network

   a. Drag and drop new inline network on to the canvas.

   b. Click on the inline network icon to view and update its properties as illustrated below and click OK.

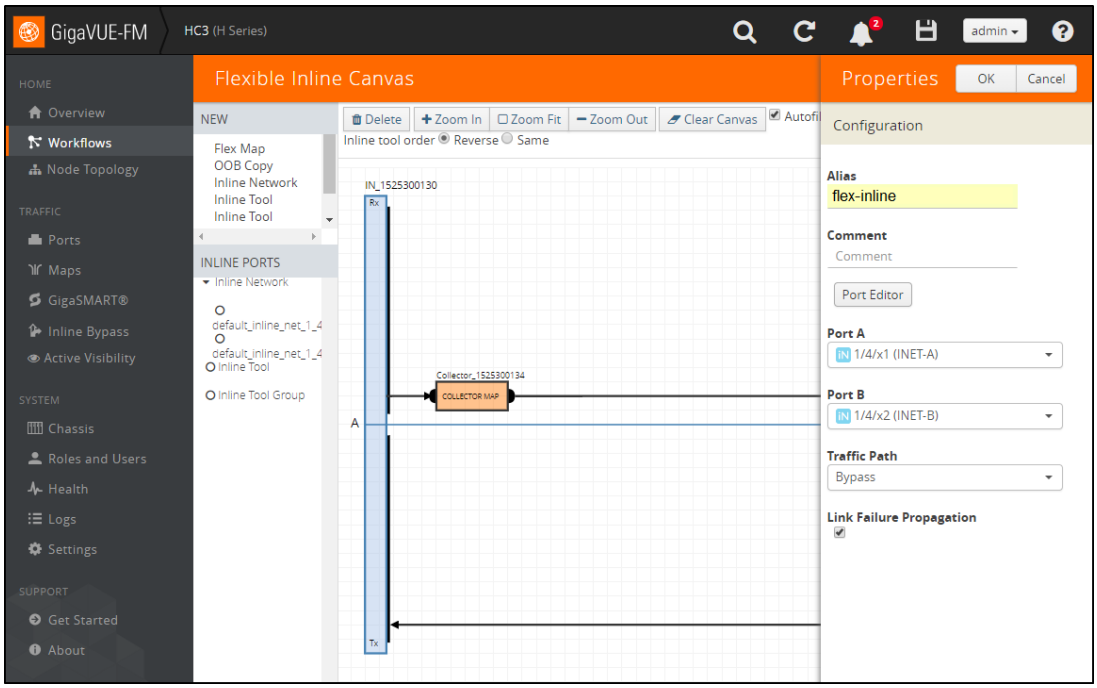


Figure 10 Flexible Inline Canvas

4. Configure new inline tool
   a. Drag and drop new inline tool on to the canvas.
   b. Click on the inline tool icon to view and update its properties as illustrated below and click OK.
   c. Repeat the above steps for configuring additional inline tools.

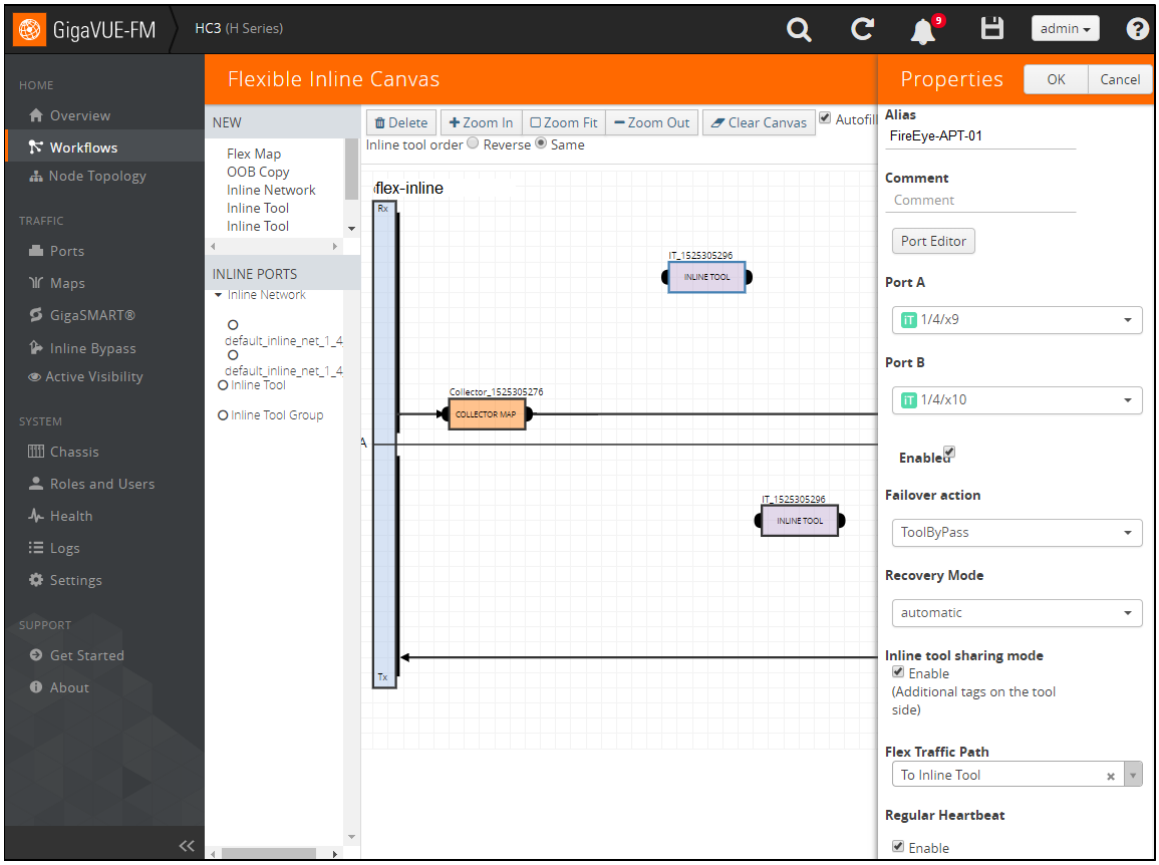


Figure 11 New Line Tool Group

5. Configure new inline tool group
   a. Drag and drop new inline tool group on to the canvas.
   b. Click on the inline tool group icon to view and update its properties as illustrated below and click OK.
   c. Repeat the above steps for configuring additional inline tool groups.

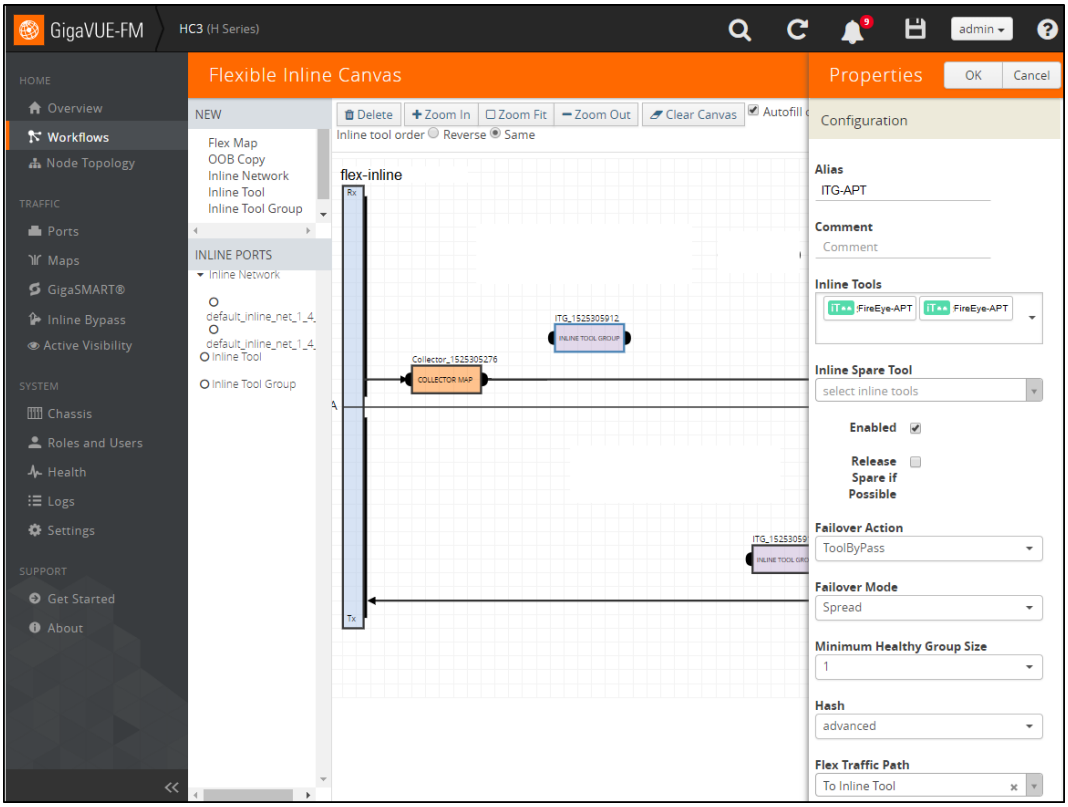


Figure 12 Line Tool – Rule Map

6. Configure new flexible inline by rule map

   a. Drag and drop new inline map on to the canvas.

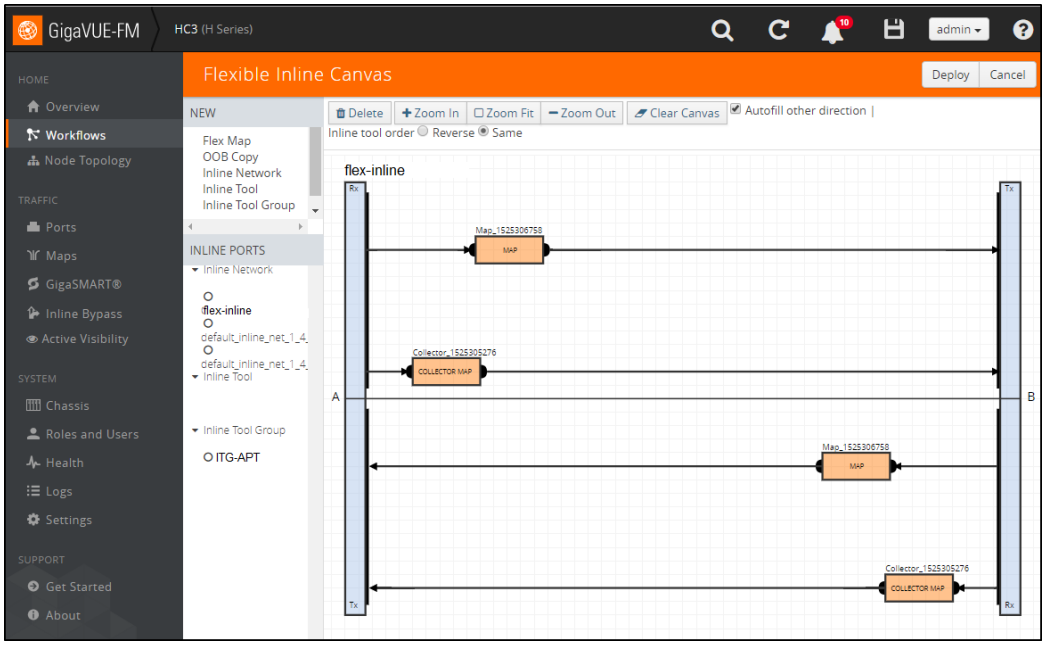


Figure 13: Line Tool Group

   b. Drag and drop inline tool and/or inline tool group created in the previous steps on to the canvas as illustrated below to define the traffic path from A-to-B.

c. Select autofill other direction (i.e. B-to-A) as Same.

NOTE: Autofill other direction can be set to reverse or it can be disabled to define another sequence of inline tools.

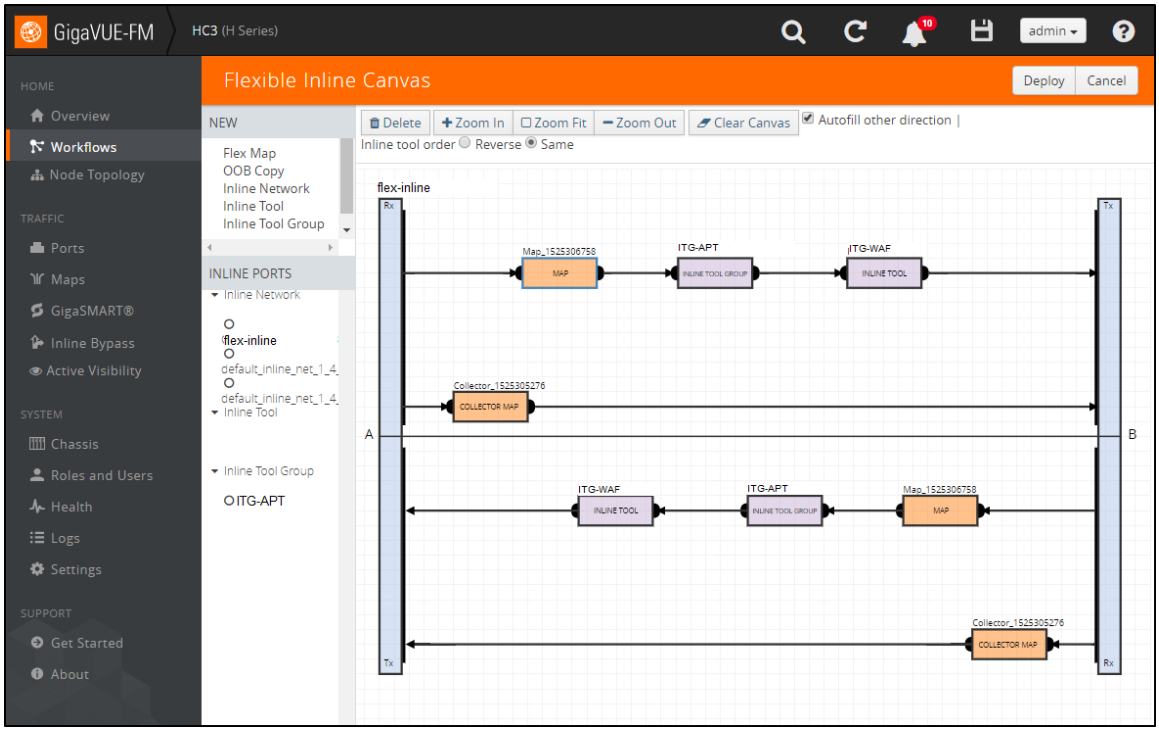


Figure 14: Map Rules

d. Define map rules for filtering in the intended traffic by clicking on the map icon and update its properties as illustrated below and click OK.

NOTE: Packet attributes such as Protocol and Port Destination can be grouped together by selecting them from the same rule's drop-down menu. More than one rule can be defined by clicking the Add a Rule option.

e. Above steps can be repeated to create more than one flexible inline by rule map.

f. By default, a flexible inline collector map is created for each inline network. It can be edited by clicking on the icon as described in the previous steps.

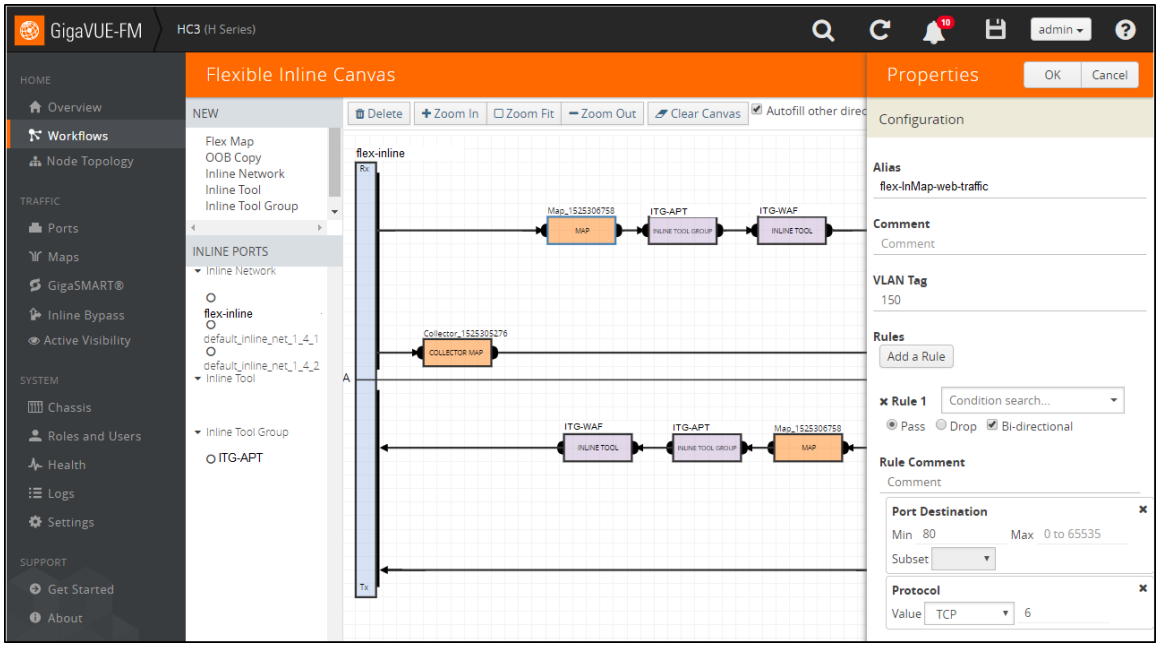


Figure 15: Inline Canvas Properties

g. [optional] Drag and drop new OOB Copy on to the canvas. Click on the icon and update its properties as illustrated below.

NOTE: Out-of-band traffic can carry the same VLAN tag as that of the inline network traffic or it can be untagged. The VLAN tagging must be identical if the same port is used as the out-of-band destination port for more than one source (i.e. inline network(s), inline tool(s) or inline tool group(s)). The source port must be unique for each out-of-band copy in a flexible inline map.

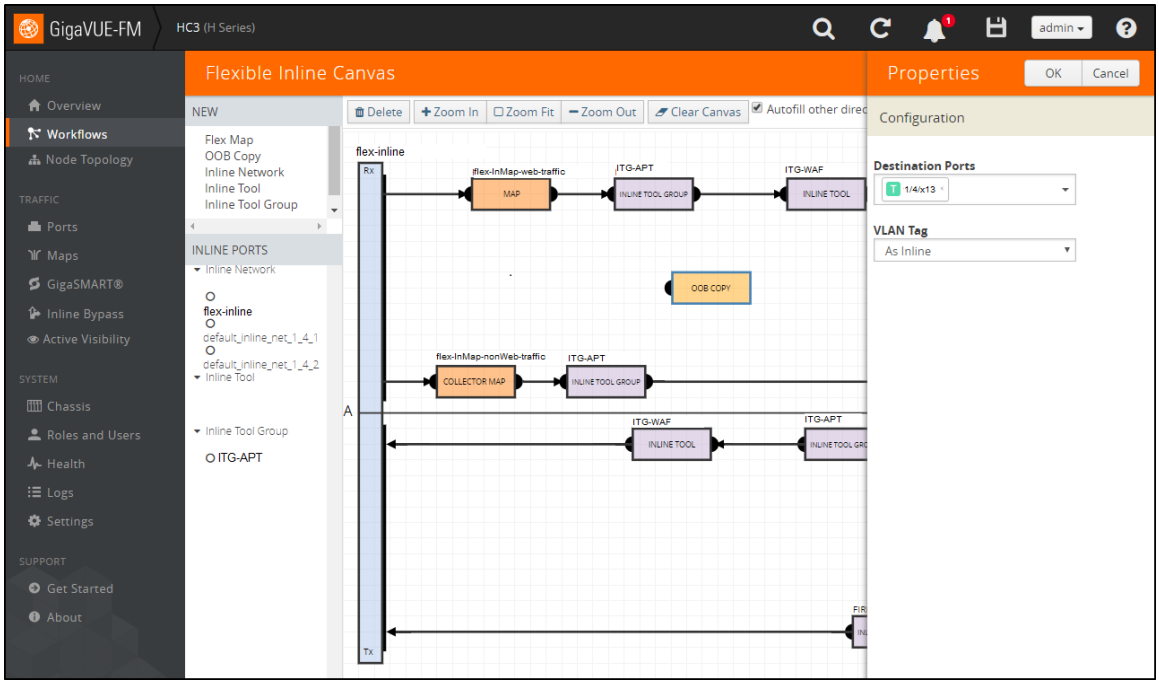


Figure 16: Inline Canvas Properties – Destination Ports

h. [optional] Associate the OOB Copy to the inline tool(s) and/or inline tool group(s) as illustrated below.

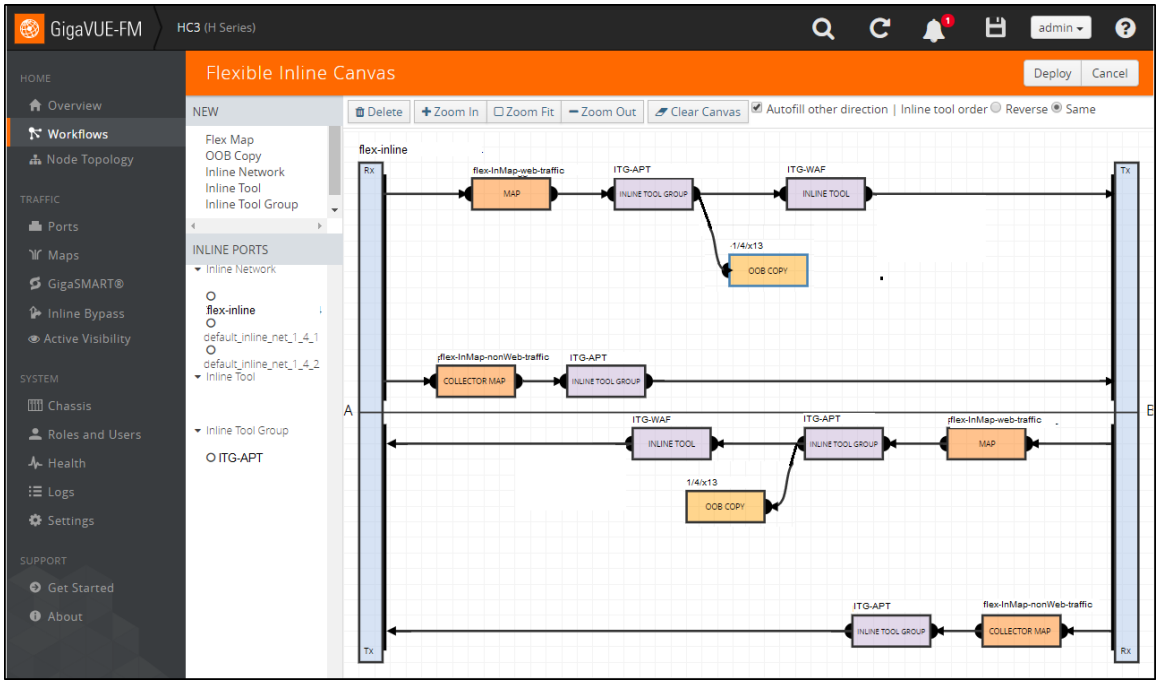


Figure 17: Inline Canvas Deploy Page

7. Deploy the configuration.
8. Click **Floppy-Disk** icon in the top Right-hand corner to save the device configuration to the nonvolatile memory.

Using Inline SSL Configuration Workflow

Inline SSL Configuration workflow walks through the mandatory prerequisite steps before configuring the forwarding paths between inline network and inline tool for Inline SSL decryption.

To use the Inline SSL Configuration Workflow:

1. Configure the Keychain Password

   NOTE: Keychain Password must be configured to enable the Inline SSL Solution. Otherwise, the Gigamon device will behave as a TCP Proxy.

   a. Click **Setup Keychain Password**.

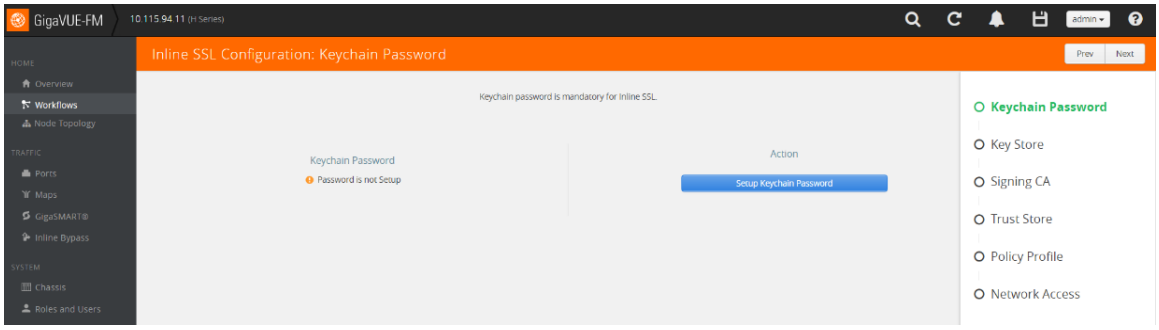


Figure 18 Inline SSL Configuration Workflow: Keychain Password

   b. Set the password and click **Submit** from the top menu.

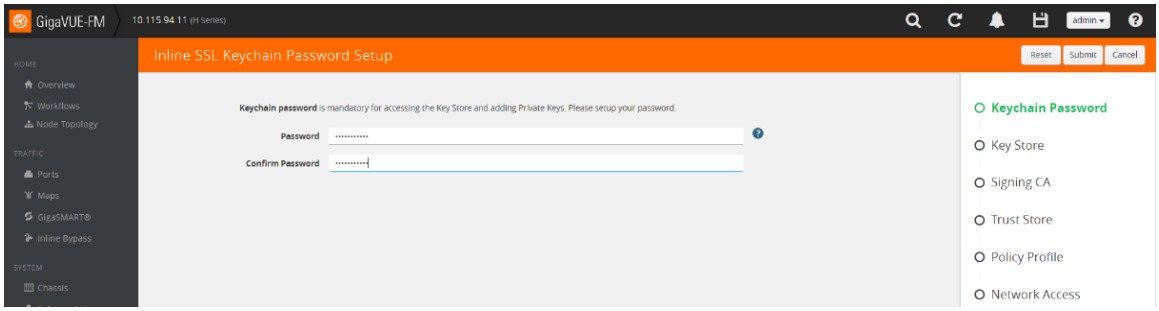


Figure 19 Inline SSL Configuration Workflow: Configuring Keychain Password

2. Update the Key Store

NOTE: The following steps illustrate uploading keypairs for configuring the Primary and the Secondary Root CAs. However, the same steps can be followed for uploading a server's keypair for decrypting inbound SSL sessions.

a. Click **Add Key Pair**.

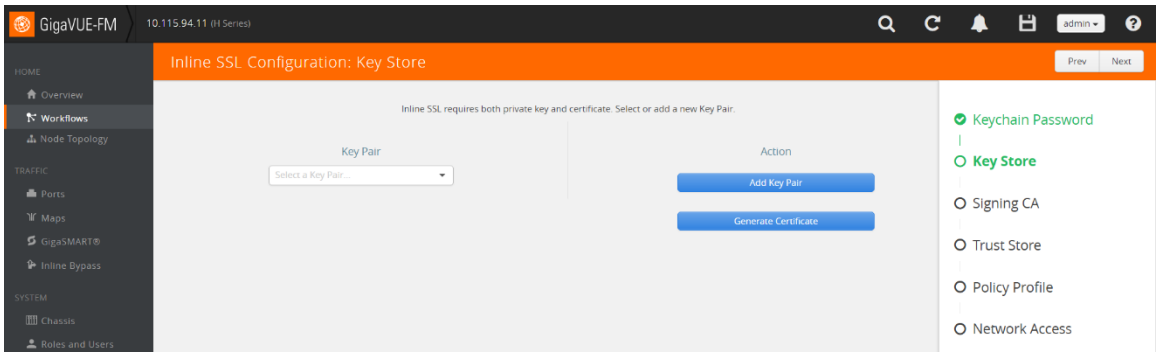


Figure 20 Inline SSL Configuration Workflow: Key Store

b. Provide relevant details as illustrated below.

c. Click **OK** from the top menu to install the key pair.

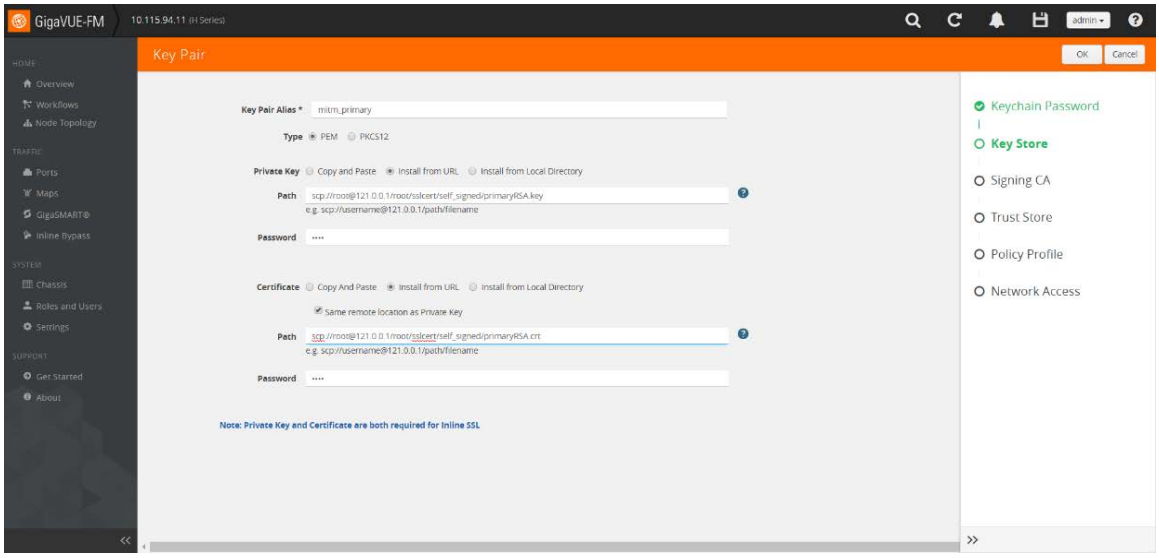


Figure 21 Inline SSL Configuration Workflow: Updating the Key Store

3. Configure the Signing CA

   NOTE: Skip this step if the Inline SSL Solution were to be deployed for decrypting inbound SSL sessions. Starting from GigaVUE-OS 5.2.00.3, Primary Root CA configuration is not enforced for decrypting inbound SSL sessions.

   a. Click **Configure Signing CA**.

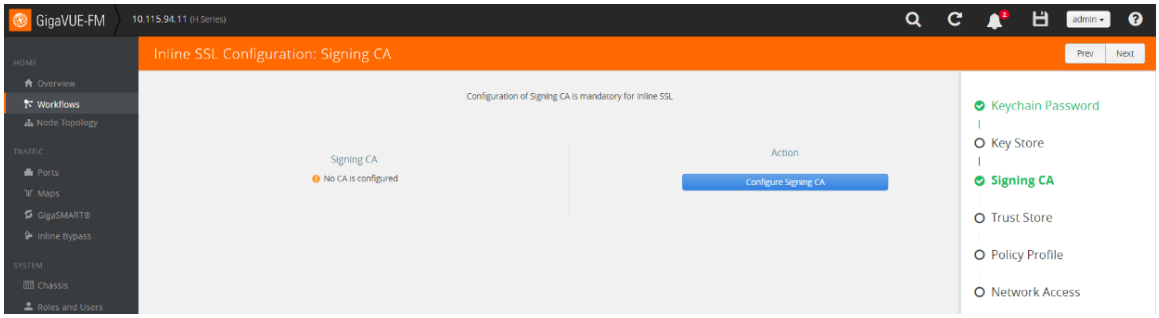


Figure 22 Inline SSL Configuration Workflow: Signing CA

   b. Select key pairs for Primary Root CA and Secondary Root CA.

   c. Click **OK** from the top menu to configure the mapping.

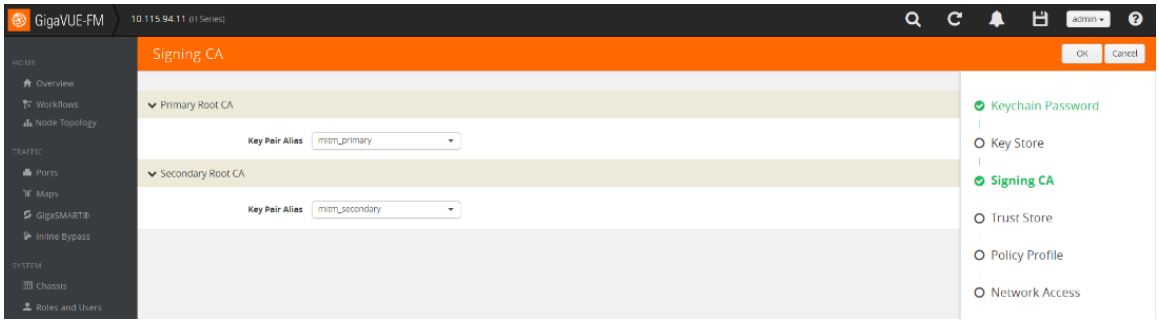


Figure 23 Inline SSL Configuration Workflow: Configuring Signing CA

4. Update the Trust Store:

   NOTE: Skip the test if the default Trust Store has the required certificates. If the Trust Store does not have a root CA certificate, follow the following steps to update the Trust Store.

   a. Download the Trust Store from the device **Navigation Pane > GigaSMART > Inline SSL > Trust Store > Actions**.

   b. Append the missing certificate in the file.

   c. Click **Replace Trust Store** and update the Trust Store.

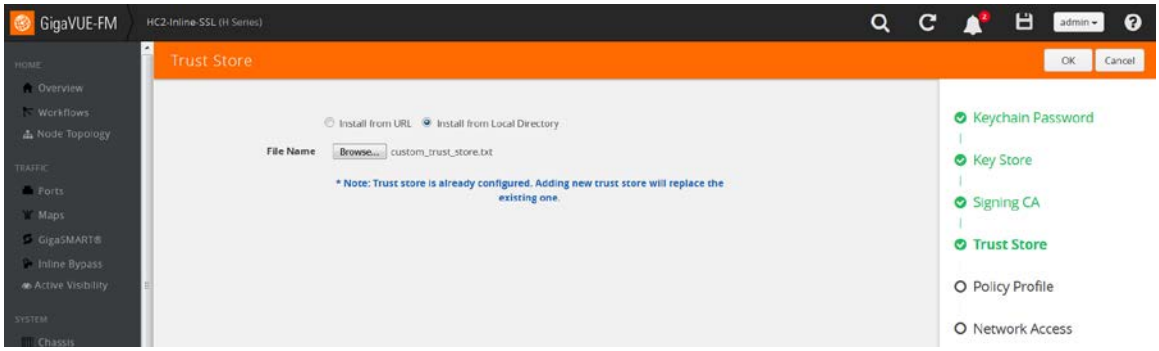


Figure 24 Inline SSL Configuration Workflow: Updating the Trust Store

5. Configure the Inline SSL profile

   a. Click **Create**.

Figure 25 InlineSSL Configuration Workflow: Policy Profile

   b. Select the **Policy Configuration** and the **Security Exceptions** as illustrated below.

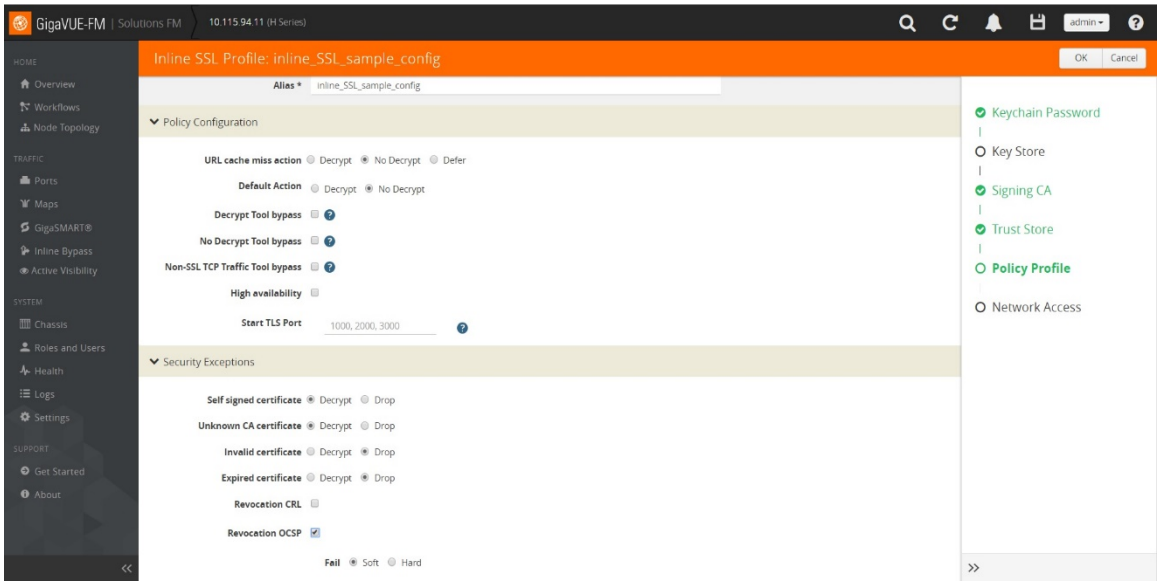


Figure 26 InlineSSL Configuration Workflow: Configuring Policy configuration & Security Exceptions in the Policy Profile

   c. Upload Whitelist and/or Blacklist as illustrated below

   NOTE: Skip this step if it is not applicable.

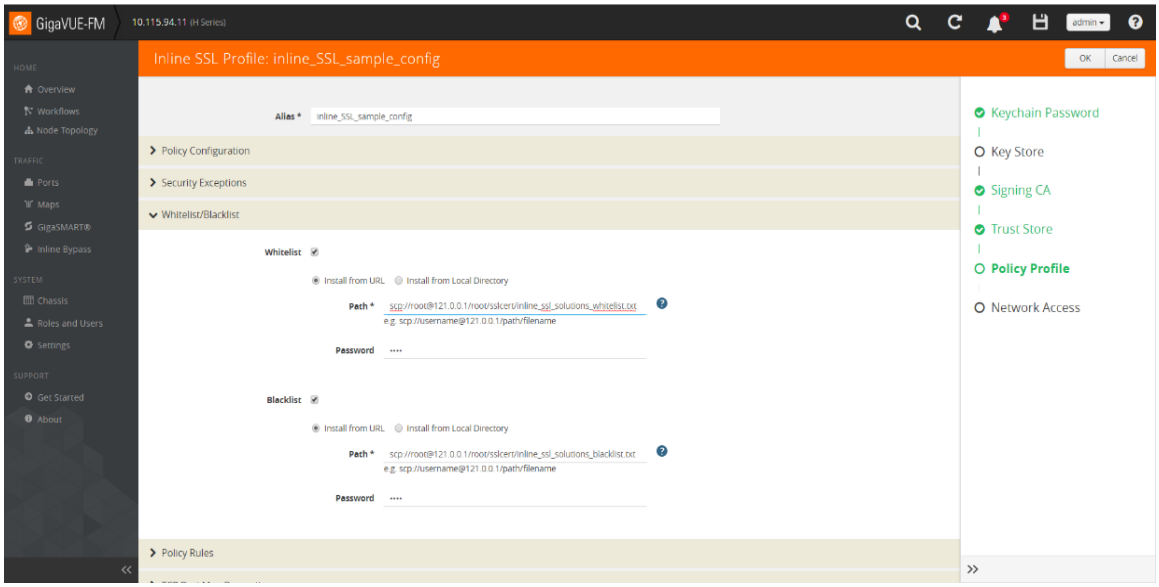


Figure 27 InlineSSL Configuration Workflow: Configuring Whitelist/Blacklist in the Policy Profile

f. Configure Policy Rules

- Click **Add a Rule**.
- Enable **Decrypt** option for the rule.
- Select **Category** from the drop-down menu.
- Select the **bot_nets** category.
- Repeat the above steps for adding the other categories as illustrated below.

NOTE: Rules can be defined based on other criteria as listed under the rule's drop-down menu.

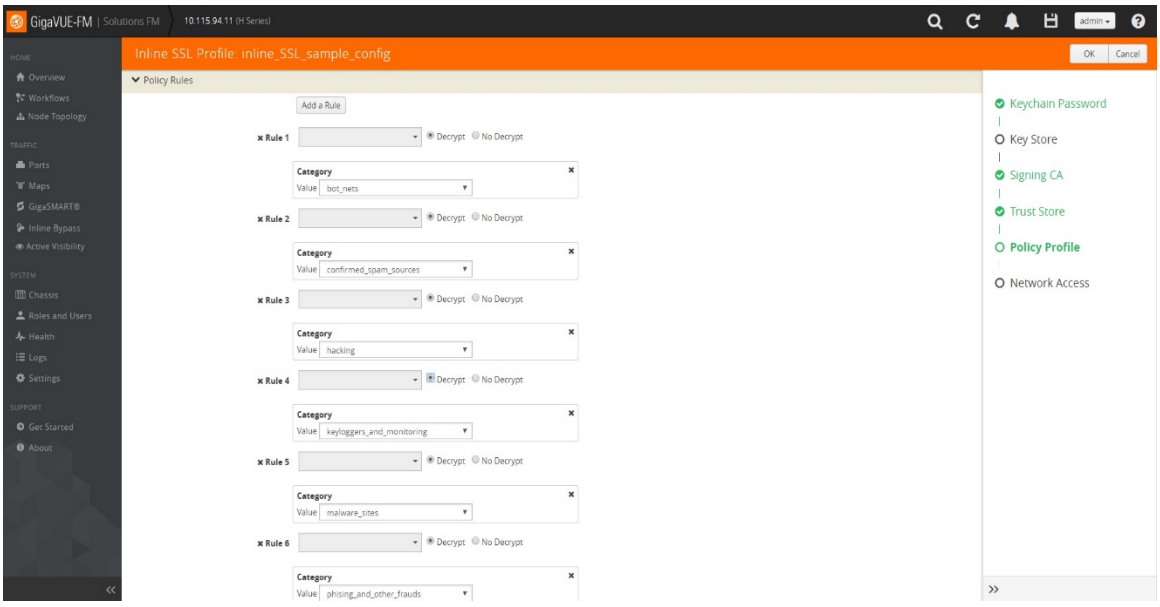


Figure 28 InlineSSL Configuration Workflow: Configuring Policy Rules in the Policy Profile

g. Configure Server Key Map

NOTE: Skip this step if inline SSL Solution were to be deployed for decrypting outbound sessions.

- Click **Add Server Key Map**.
- Enter the IP address or domain name of the server.
- Select the key pair.

h. Click **OK** from the top menu to configure the inline SSL profile.

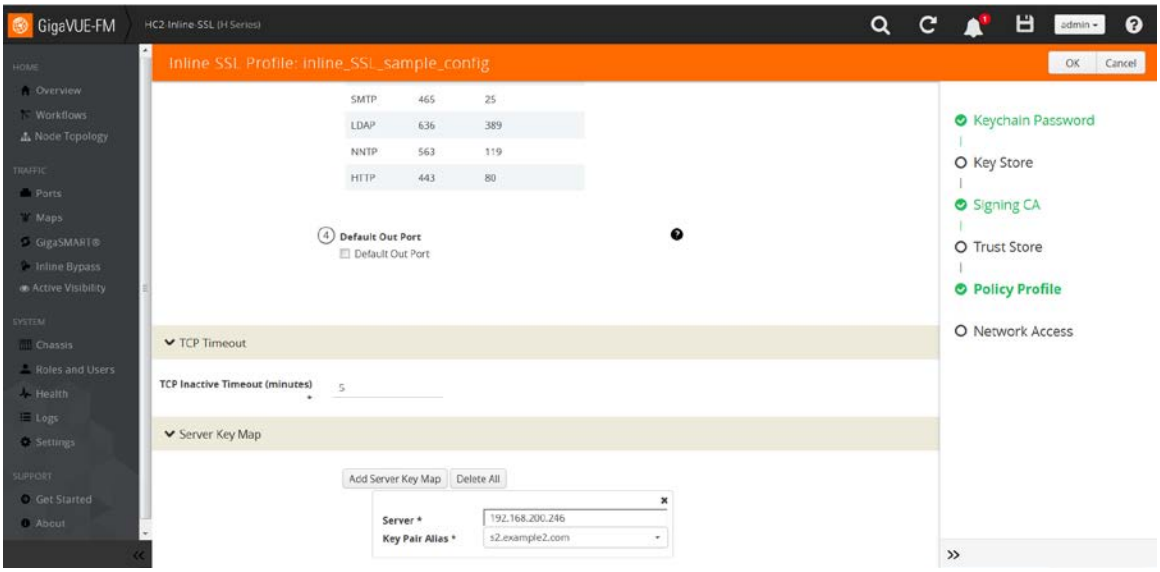


Figure 29 InlineSSL Configuration Workflow: Configuring Key Map in the Policy Profile

6. Configure Network Access:

   i. GigaSMART® module must have connectivity to the Internet for URL categorization and Certificate Revocation checks.

   NOTE: Skip this step if the InlineSSL Solution were to be deployed for decrypting inbound SSL sessions.

   j. Click **Configure Network Access**.

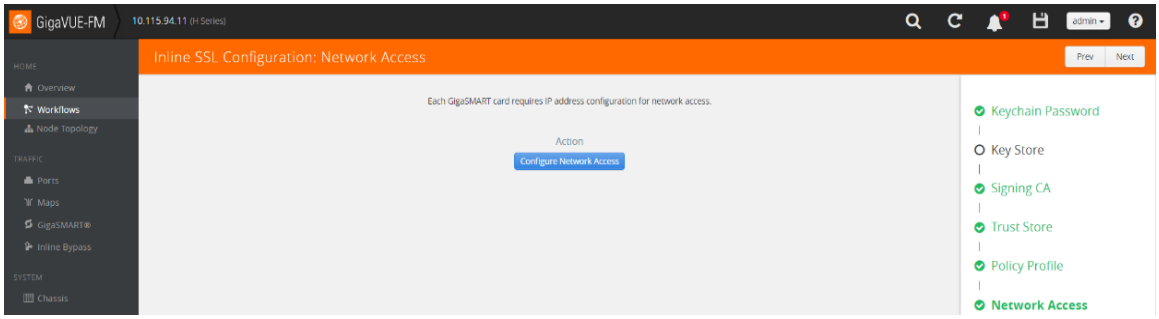


Figure 30 InlineSSL Configuration Workflow: Network Access step

   k. **Enable DHCP** or manually configure the IP address.

      i. Click **OK** from the top menu; exit the workflow.

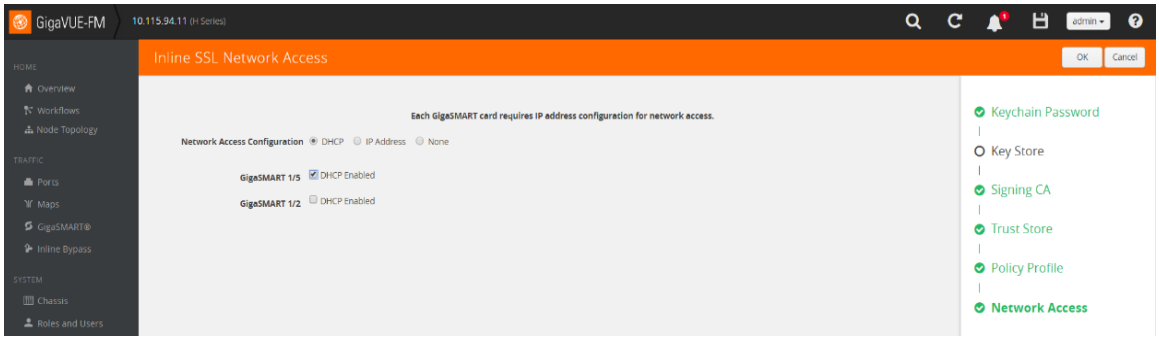


Figure 31 InlineSSL Configuration Workflow: Configuring Network Access

ii. Open the **Quick View** window for the GigaSMART engine interface from the device **Navigation Pane > Ports**. Verify that the IP address is assigned to the GigaSMART engine interface. Ping the default GW to make sure that the connectivity exists.

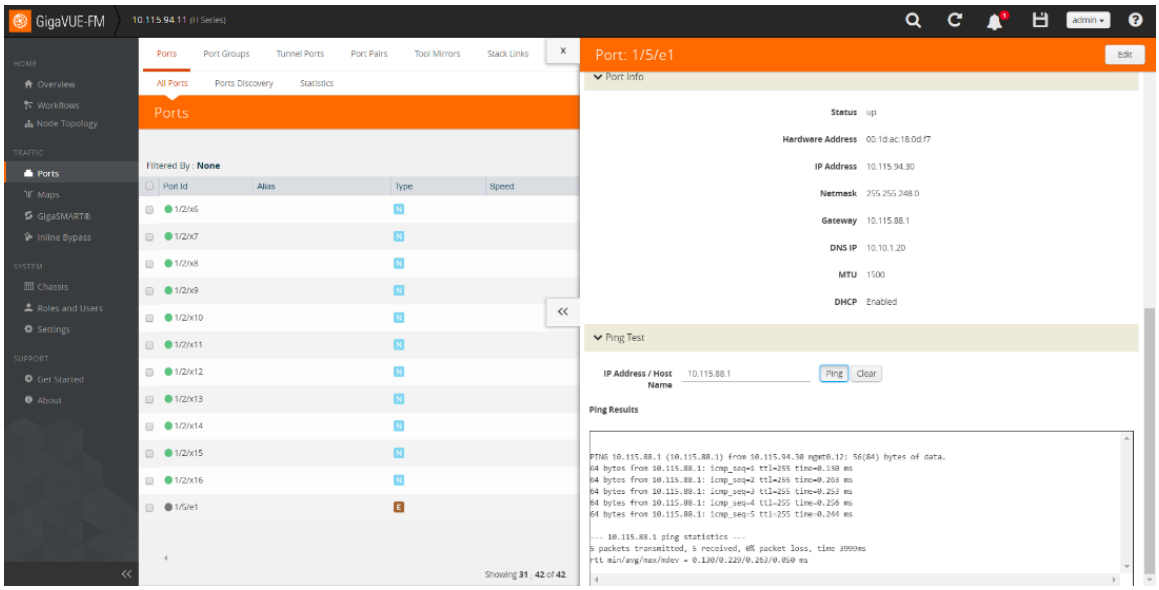


Figure 32 GigaSMART engine interface Quick View window

NOTE: Click **Floppy-Disk** icon in the top Right-hand corner to save the device configuration to the nonvolatile memory.

Using Inline SSL Map Workflow

InlineSSL Map workflow guides user in configuring flow maps for setting up the forwarding paths. Before proceeding, please review the traffic flow in the absence of the Gigamon device, identify the packet attributes for filtering-in the intended traffic for decryption and identify the traffic path for the un-intended traffic.

Depending on the required traffic flows, user can select one of the pre-defined traffic flows in the InlineSSL Map workflow. For illustration purposes, **Flow B** is selected to send HTTP traffic to inline tools, to send the intended traffic to the GigaSMART engine and to send the rest of the traffic along the bypass path.

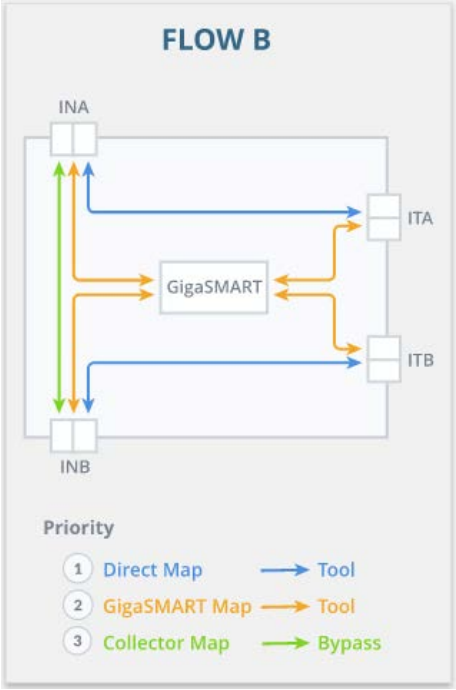


Figure 33 InlineSSL Map Workflow: Flow B

To use the InlineSSL Map Workflow:

6. Configure Inline Networks:

   a. Click **Create Inline Network**.

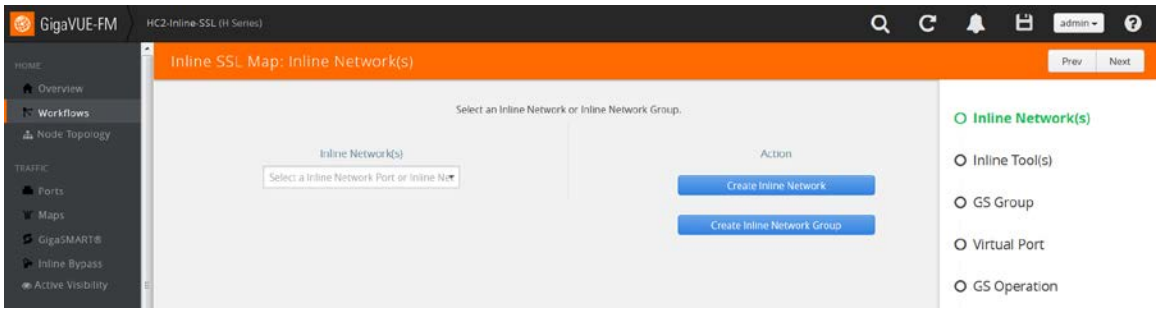


Figure 34 InlineSSL Map Workflow: Inline Network

   b. Provide details as illustrated below and Click **OK**.

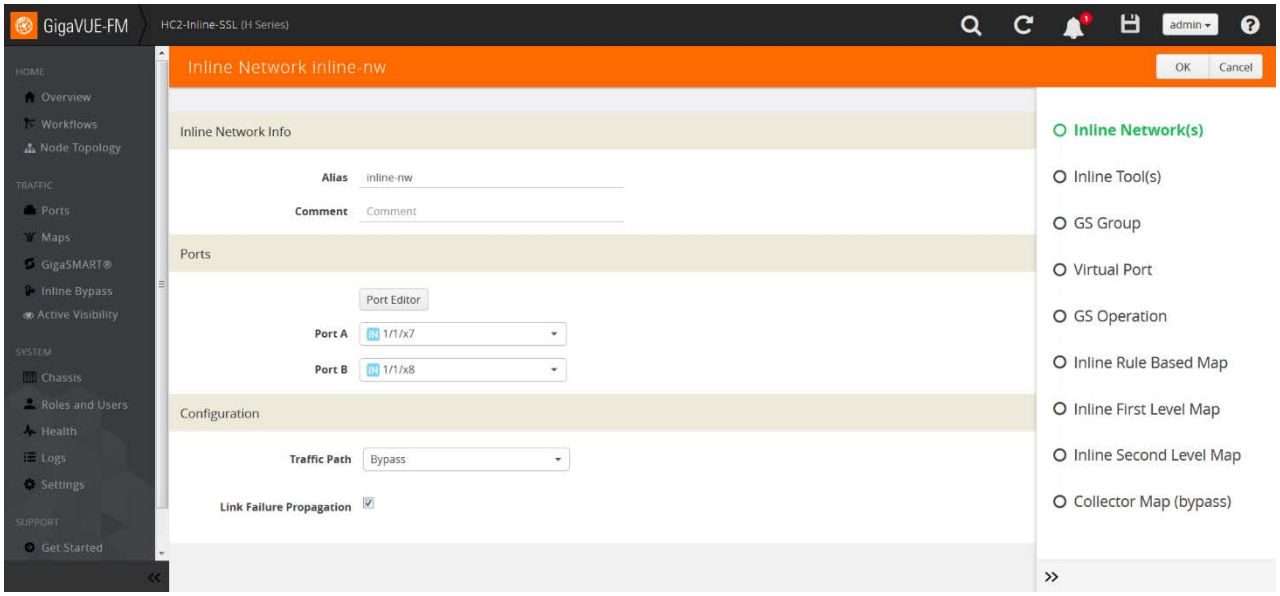


Figure 35 InlineSSL Map Workflow: Creating inline network

7. Configure Inline Tool

   a. Click **Create Inline Tool**.

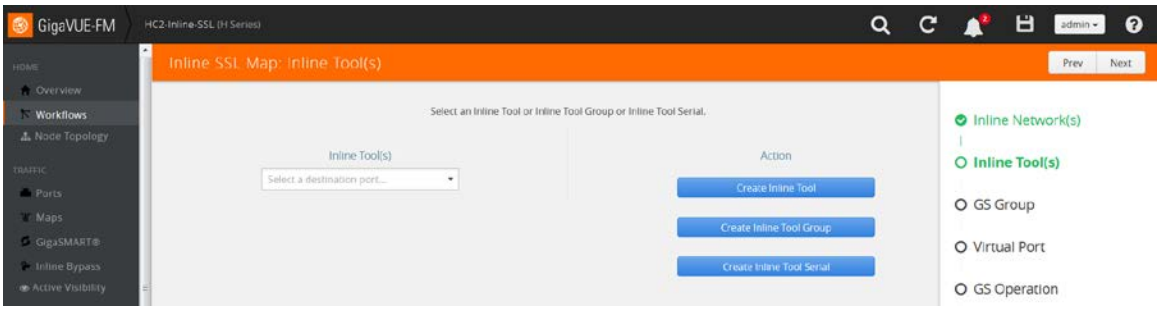


Figure 36 InlineSSL Map Workflow: Creating inline tool

   b. Configure the inline tool as illustrated below.

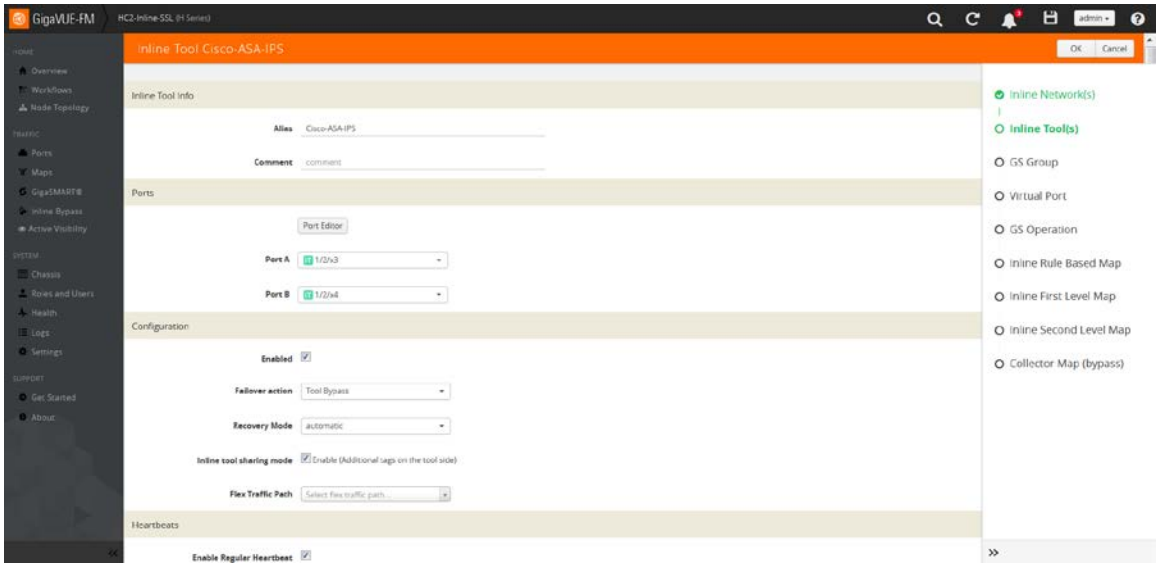


Figure 37 InlineSSL Map Workflow: Configuring inline tool

8. Configure the GigaSMART Group:

   a. Click **Create**.

   b. Provide details as illustrated below and click **OK** from the top menu.

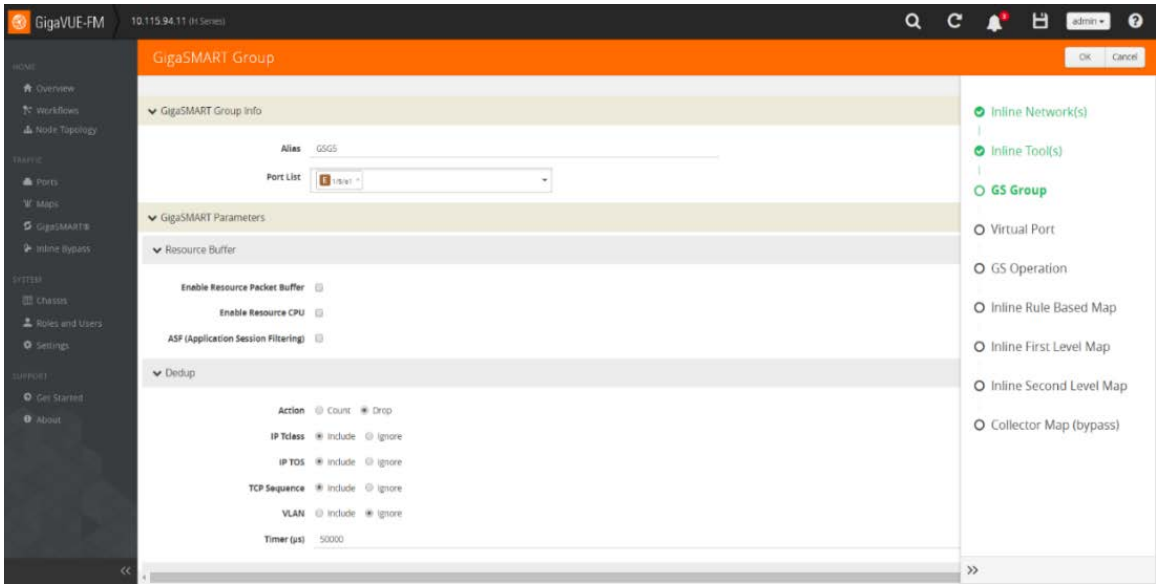


Figure 38 InlineSSL Map workflow: Creating new GigaSMART Group

9. Configure Virtual Port:

   a. Select **Create**.

   b. Enter an alias name and click **OK** from the top menu.

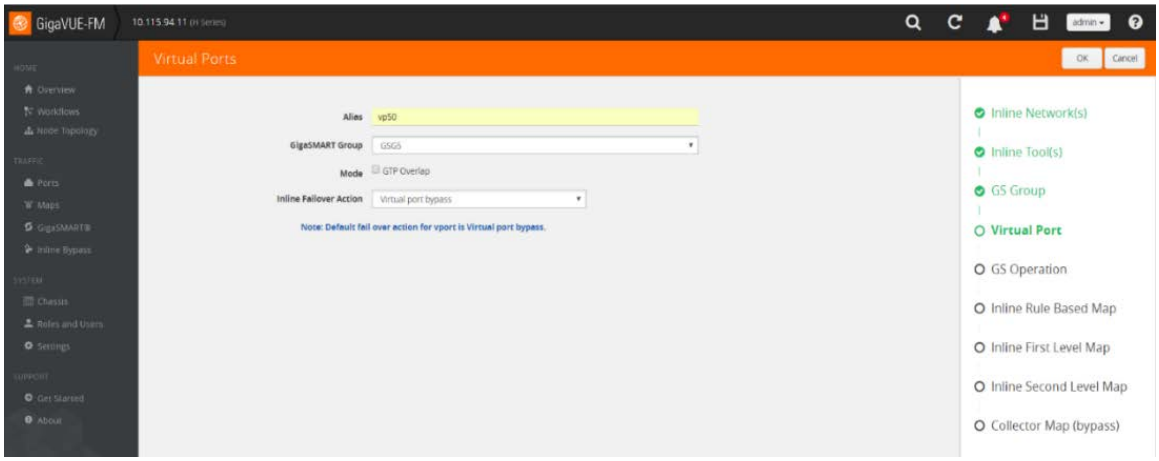


Figure 39 InlineSSL Map workflow: Creating new Virtual Port

10. Configure the GigaSMART operation

    a. Click **Create**.

    b. Enter an alias name, select the inline SSL profile and click **OK** from the top menu.

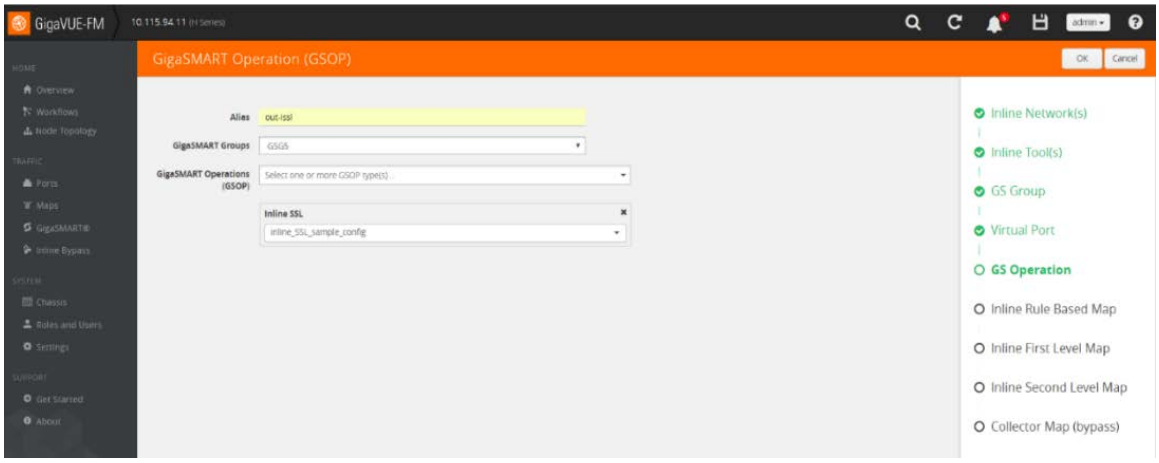


Figure 40 InlineSSL Map workflow: Creating GigaSMART Operation

11. Configure the Inline Rule Based Map

    a. Provide details as illustrated below and click **OK**.

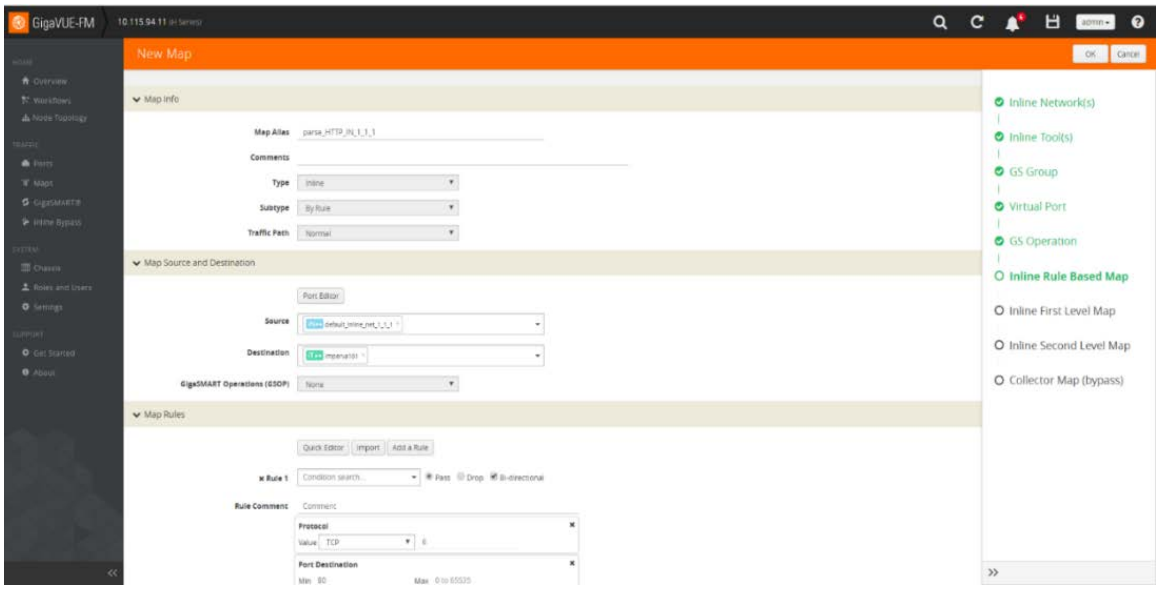


Figure 41 InlineSSL Map workflow: Creating Classic Inline Map

12. Configure the Inline First Level Map:

    a. Provide details as illustrated below and click **OK**.

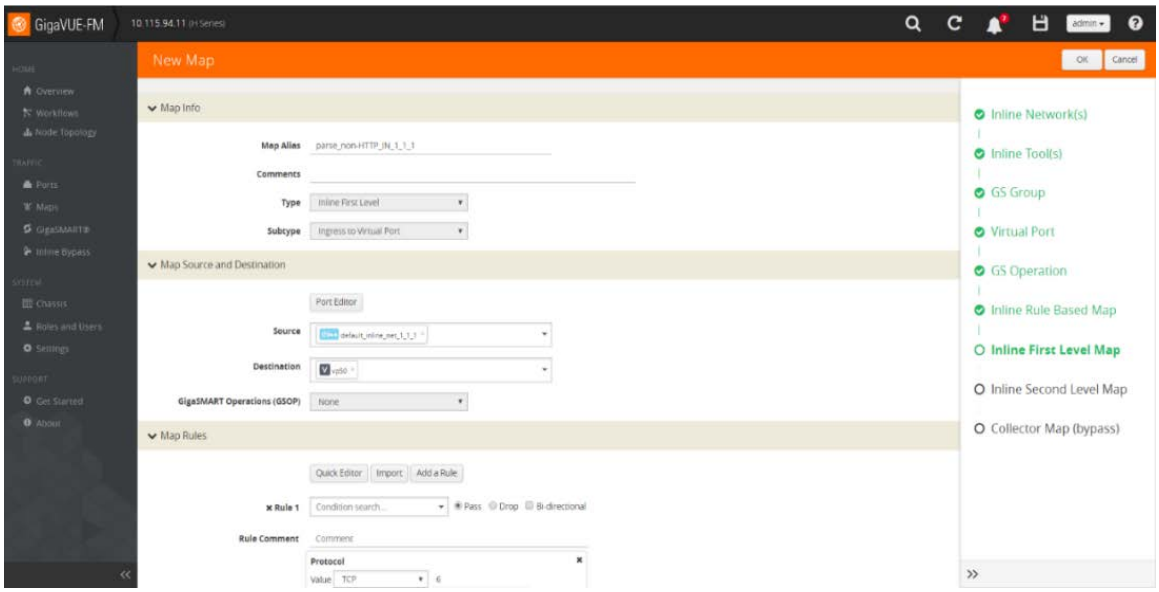


Figure 42 InlineSSL Map workflow: Creating Inline First Level Map

13. Configure the Inline Second Level Map:

    a. Enter an alias name and click **OK**.

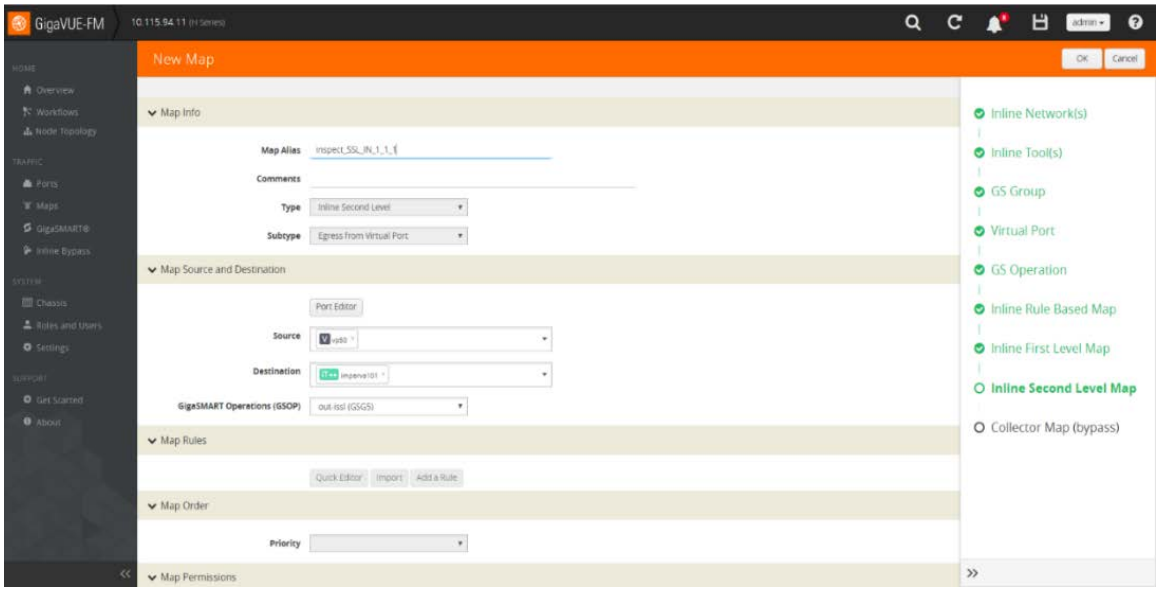


Figure 43 InlineSSL Map workflow: Creating Inline Second Level Map

14. Configure the Collector Map:

    a. Enter an alias name and click **OK**.

    b. Click **To Maps** after completing the workflow.

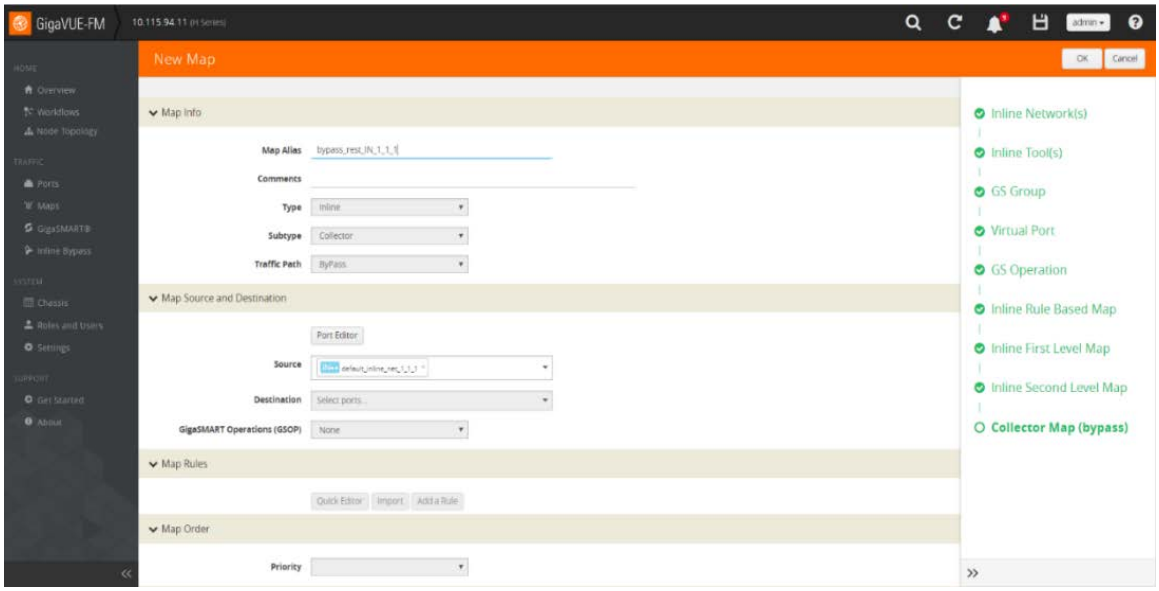


Figure 44 InlineSSL Map workflow: Creating the Shared Collector Map

    c. Review the maps created by the workflow.

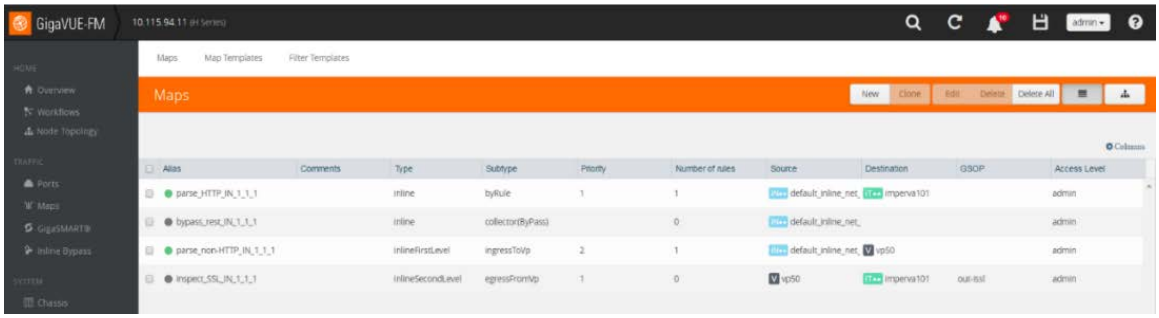


Figure 45 Verifying the Maps

NOTE: Click **Floppy-Disk** icon in the top Right-hand corner to save the device configuration to the nonvolatile memory.

Updating Inline Network Settings

Use the following steps to allow traffic to flow through the Gigamon device. Before proceeding, make sure that flow maps are properly configured.

To update the Inline Network Settings:

1. Go to Physical Nodes and select the device.
   a. Select **Inline Bypass > Inline Networks**.
   b. Select the intended inline network.
   c. Click **Edit** from the **Inline Networks** menu.
   d. Select Traffic Path as To Inline Tool.
   e. Disable **Physical Bypass** and click **OK** from the top menu.

   NOTE: When the Physical Bypass is disabled, the optical protection switch is opened and the associated links are made up. Any traffic coming in on these fibers is subject to the traffic forwarding rules imposed by the current configuration as well as the current state of the inline tools. Depending on how fast the neighboring devices react to the Link Up event, there may be a slight glitch in the traffic flow.

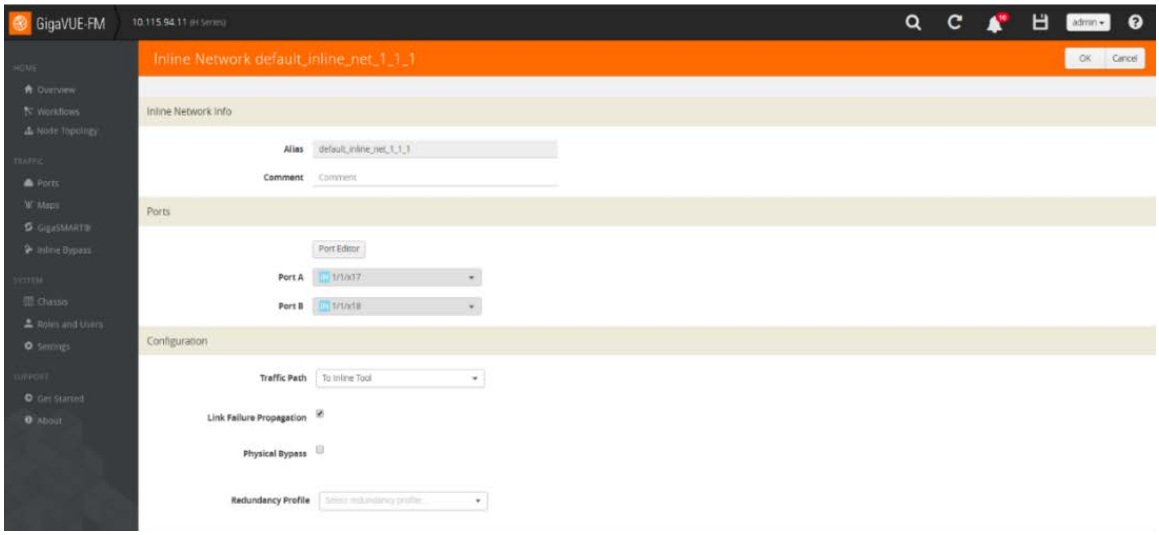


Figure 46 Updating Inline Network

NOTE: Click **Floppy-Disk** icon in the top Right-hand corner to save the device configuration to the nonvolatile memory.

Verification Tasks

Verifying Port Status

To verify port status:

1. Go to device **Navigation Pane > Traffic > Ports > All Ports**.
2. Filter in the ports under consideration.
3. All ports should be **Enabled** and their **Link Status** must be **Up**.

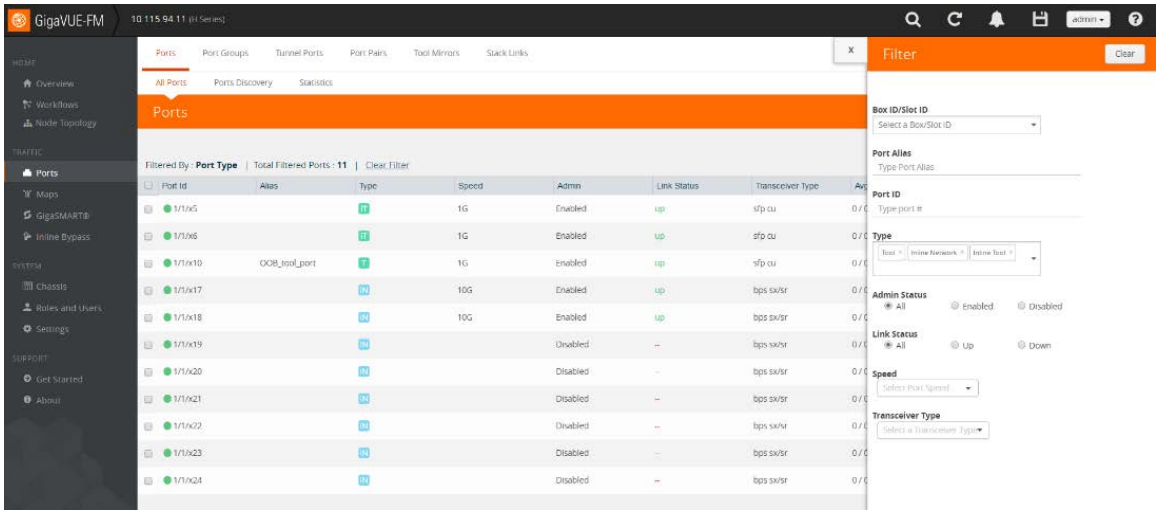


Figure 47 Viewing Ports status

Verifying Inline Network Status

To verify Inline Network status:

1. Go to device **Navigation Pane > Traffic > Inline Bypass > Inline Networks**.
2. Inline network links should have **Forwarding State** as Normal, **Physical Bypass** as Disabled and **Traffic Path** as To Inline Tool.

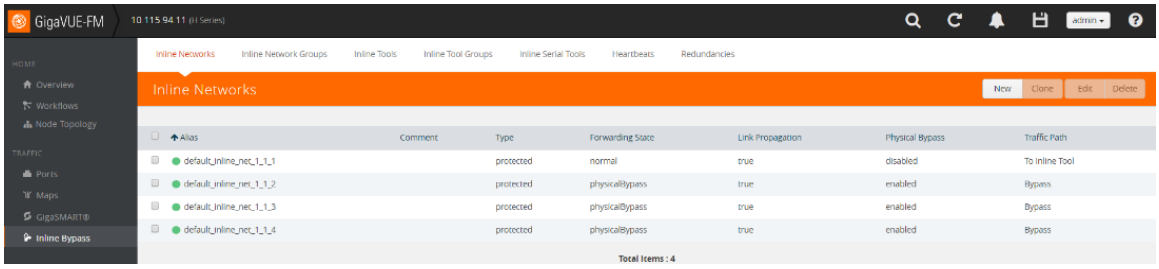


Figure 48 Viewing Inline Network status

3. Inline tool status:
   a. Go to device **Navigation Pane > Traffic > Inline Bypass > Inline Tools**.
   b. Select **Inline Tools** and verify that the inline tool has the following status:
      - **Inline Tool Status**: Enabled
      - **Combined Heartbeat Status**: Up
      - **Heartbeat Profile Health Status**: Green
      - **Inline Tool Health Status**: Green

      NOTE: Health Status depends on the member link status. If the Health Status is Red, the Tool Tip displays the reason when the user scrolls the mouse over the legend.

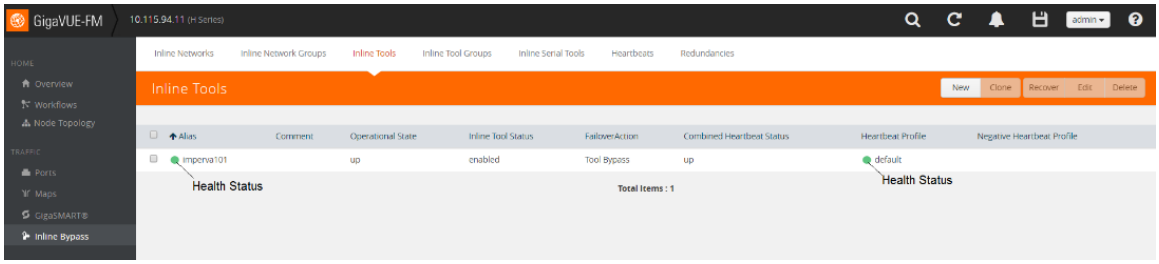


Figure 49 Viewing Inline Tool status

Verifying Map Status

To verify map status:

1. Go to device **Navigation Pane > Traffic > Maps**
2. In the Maps tab, verify that the Health Status of all the maps is Green.

   NOTE: Health Status depends on the associated ports' (from and to ports) link status. If the Health Status is Red, the Tool Tip displays the reason when user scrolls the mouse over the legend.

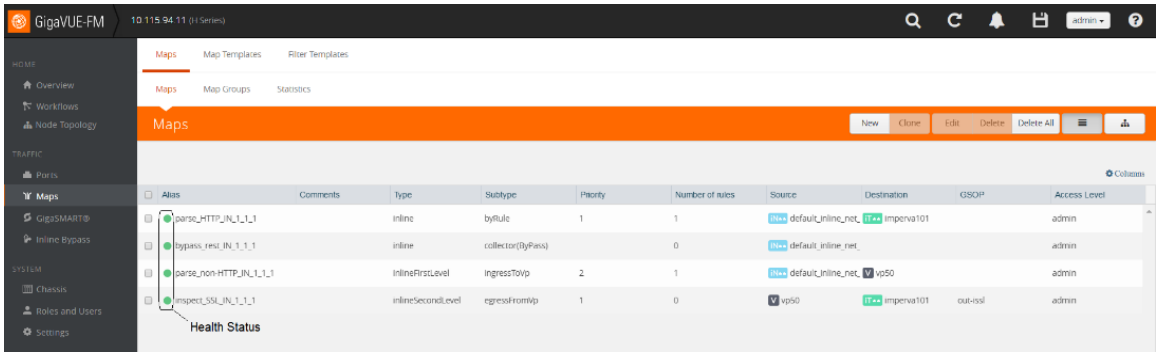


Figure 50 Viewing Maps status

Verifying Port Statistics

To verify port statistics:

1. Go to device **Navigation Pane > Traffic > Ports > Filter**.

Filter in inline network, inline tool, tool and/or hybrid ports (if any), and verify that the ports are receiving traffic.

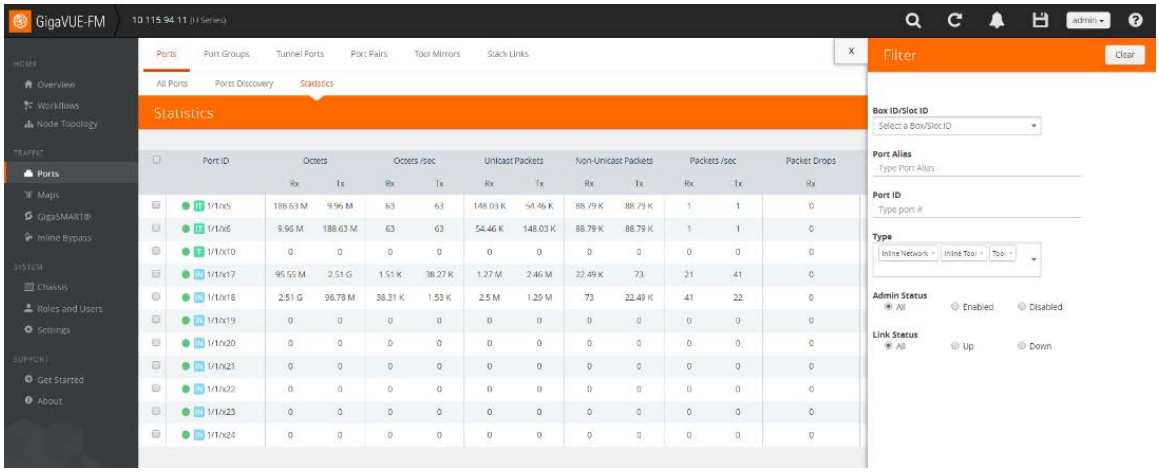


Figure 51 Viewing Ports statistics

Verifying Map Statistics

To verify map statistics:

1. Verify stats reported under device **Navigation Pane > Traffic > Maps > Maps > Statistics**.

> **NOTE:** Statistics are not reported for second level inline-SSL map since they have no rules defined.

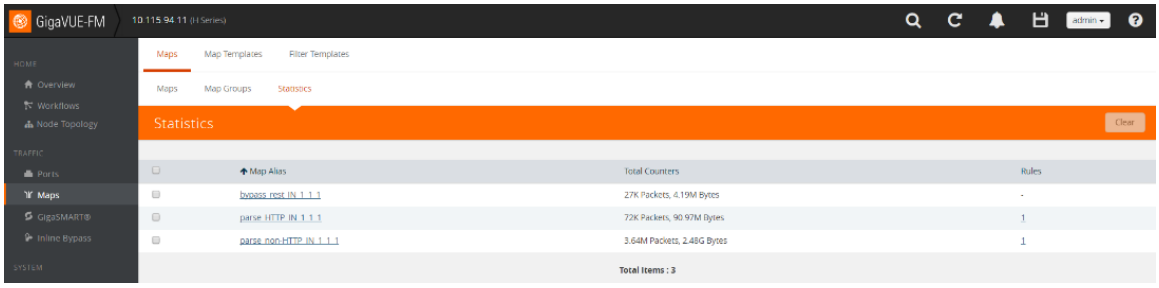


Figure 52 Viewing Maps statistics

2. Click on a map to check its trending statistics.

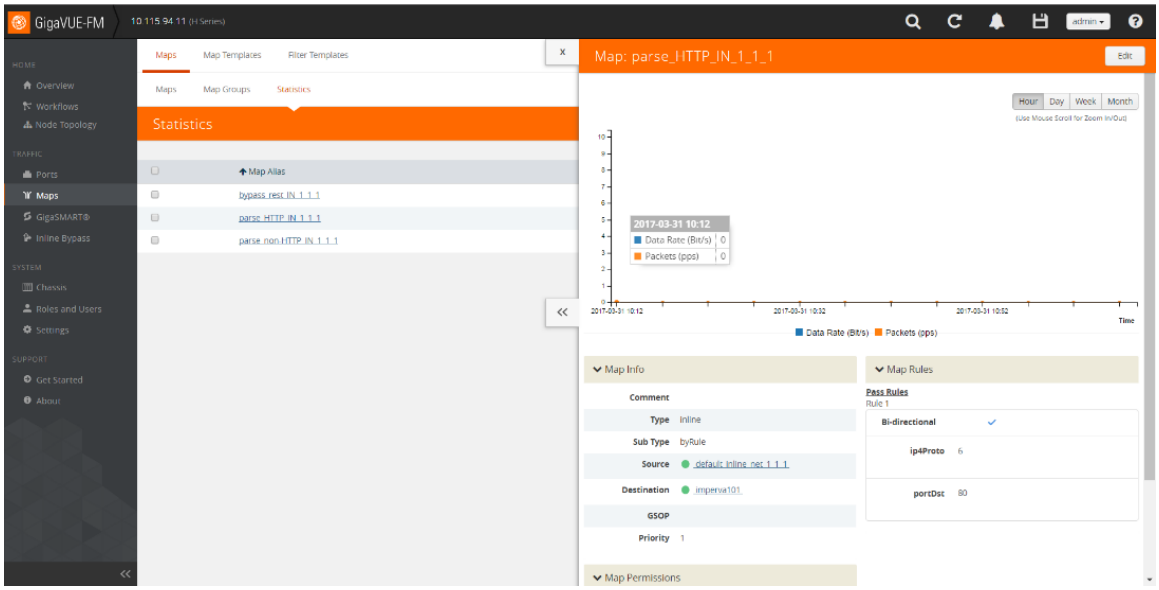


Figure 53 Viewing statistics for Classic Inline Map

Verifying GigaSMART Group Statistics

To verify GigaSMART group statistics:

3. Verify stats reported under device **Navigation Pane > Traffic > GigaSMART > GigaSMART Groups > Statistics**.

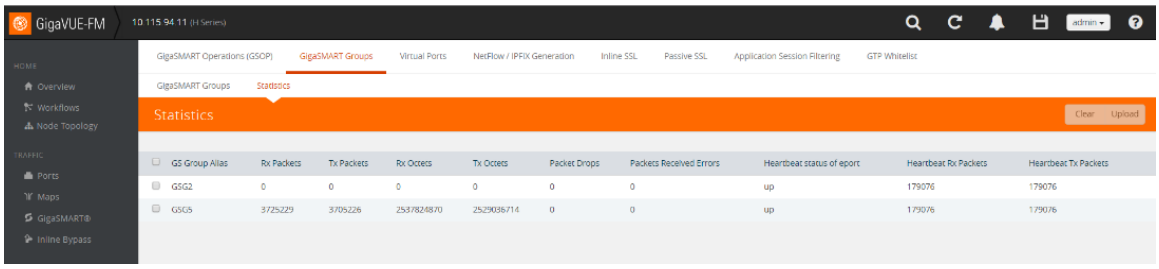


Figure 54 Viewing GigaSMART Group statistics

4. Click the GigaSMART Group Alias name to view the historical statistics.

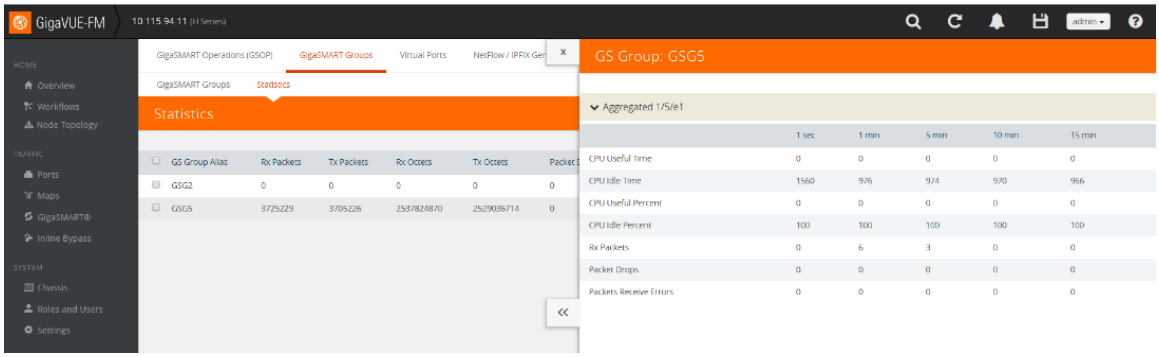


Figure 55 Viewing historical statistics of GigaSMART Group

Verifying GigaSMART Operation Statistics

To verify GigaSMART operations statistics:

5. Verify stats reported under **Navigation Pane > Traffic > GigaSMART > GigaSMART Operations (GSOP) > Statistics**.

6. Click the GigaSMART Operation alias name to view the historical statistics.

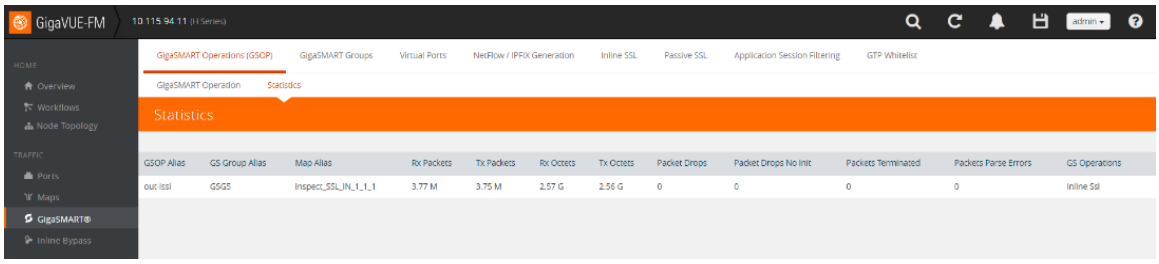


Figure 56 Viewing GigaSMART Operation statistics

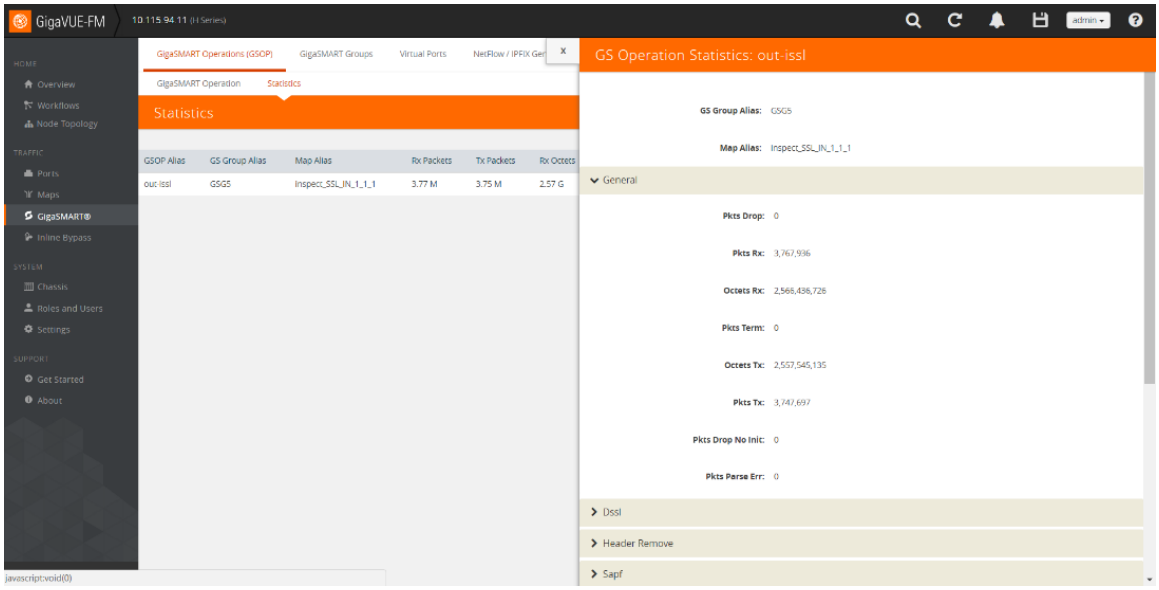


Figure 57 Viewing historical statistics of GigaSMART Group

Verifying InlineSSL Session Statistics

To verify InlineSSL session statistics:

7. Verify stats reported device **Navigation Pane > Traffic > GigaSMART > InlineSSL > Statistics**.

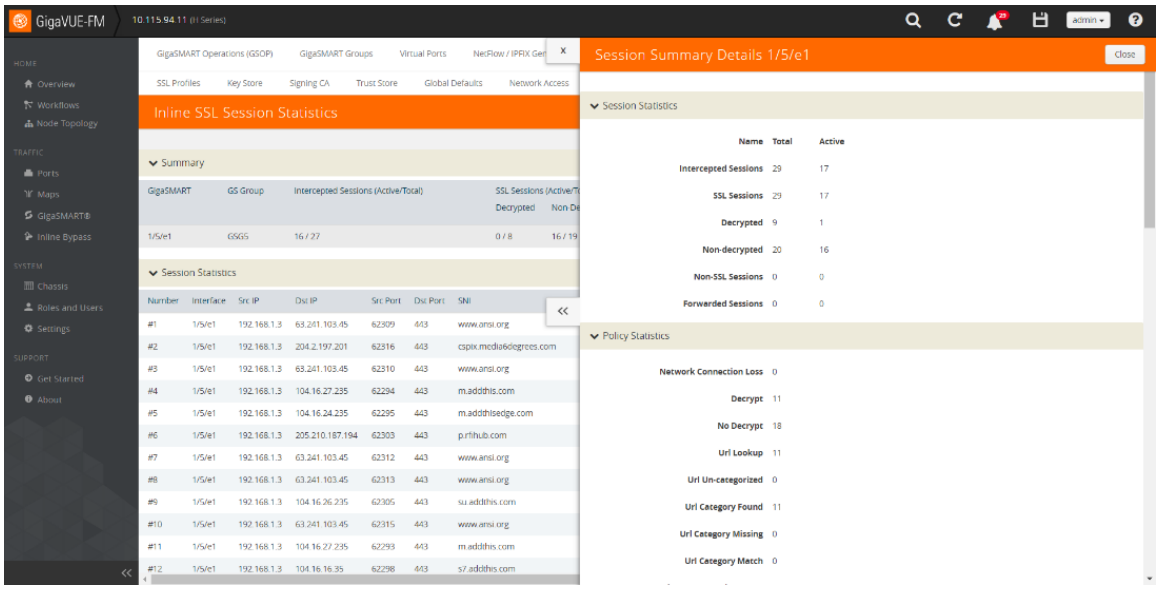


Figure 58 Viewing InlineSSL session summary

8. Click **Show Details** to view more details.

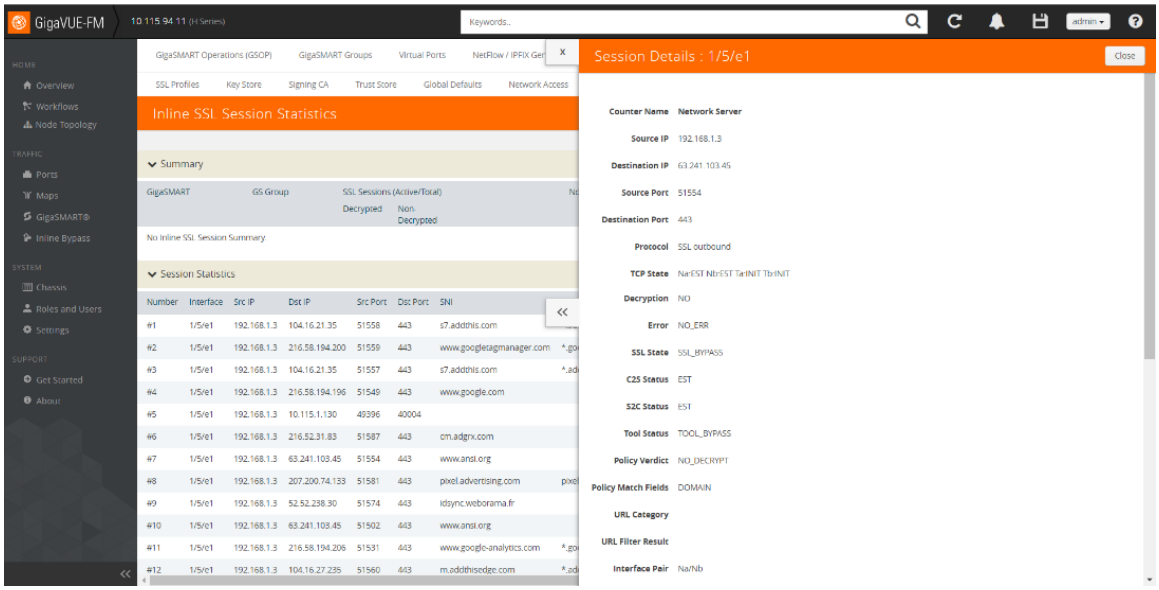


Figure 59 Viewing InlineSSL session detail statistics