

Deployment Guide: Flexible Inline Arrangements GigaVUE-OS 5.3

COPYRIGHT

Copyright © 2018 Gigamon. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without Gigamon's written permission.

TRADEMARK ATTRIBUTIONS

Copyright © 2018 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal- trademarks. All other trademarks are the trademarks of their respective owners.

Document Revision - 06/05/2018

Table of Contents

OVERVIEW4
Flexible Inline Solution Highlights 4
DEPLOYMENT CHECKLIST
Pre-deployment checklist
Deployment checklist
Post-deployment checklist
Unsupported 6
USE CASES7
Selectively guiding and load balancing traffic flows to inline tools
Selectively decrypting inline SSL traffic and guiding traffic to inline tools
Deploying external inline SSL interception and guiding traffic to inline tools
CONFIGURATION TASKS
Configuring Ports
Using Flexible Inline Flow Configuration Workflow
Using Inline SSL Configuration Workflow
Using Inline SSL Map Workflow
Updating Inline Network Settings
VERIFICATION TASKS
Verifying Port Status
Verifying Inline Network Status
Verifying Map Status
Verifying Port Statistics
Verifying Map Statistics
Verifying GigaSMART Group Statistics
Verifying GigaSMART Operation Statistics
Verifying InlineSSL Session Statistics

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 Giga VUE-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.
- 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.
- 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-useCase01config.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.







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 Ato-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.
- 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.

 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:



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-B}.
- Configure the type as inline tool for ports T1_{A-B} (SSL Intercept), T2_{A-B} (Cisco IPS), T3_{A-B} (FireEye APT) and T4_{A-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 NA-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.

Create inline tools links corresponding to T1_{A-B} (SSL Intercept), T2_{A-B} (Cisco IPS), T3_{A-B} (FireEye APT) and T4_{A-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.

- 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 Ato-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.
- 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.
- 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:



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.

🞯 GigaVUE-FM	HC3 (H Series)						C	ג כ	2 🌲	Ľ	adm	in 🗸	?
НОМЕ		Ports	Port Grou	ps Tu	innel Ports	Port	Pairs	Tool Mirro	rs St	ack Links				
A Overview		All Ports	Ports D	iscovery	Fabric	Statistics								
🔥 Worknows		Ports							E	dit Fil	ter Quid	k Port Edito	or Expo	rt
TRAFFIC														
Ports	Se	lected: 2 o	f 5 Filte	red By : Bo	x ID , Port	ID <u>Clea</u>	r Filter						Columns	5
ነ በ Maps		Port Id	Alias	Status	Туре	Speed	Admin	Link St	Transc	SFP P	Avg Uti	Port Filt	Discov	
💋 GigaSMART®		<u>1/4/x1</u>	INET-A	Por			Disabled		sfp+ sr	-1.69	0/0	-	Off	*
Inline Bypass Active Visibility		<u>1/4/x2</u>	INET-B	Por			Disabled		sfp+ sr	-2.10	0/0	_	Off	
SVSTEM		<u>1/4/x5</u>	IMPERV	Por	N		Disabled		sfp sx	-6.27	0/0	-	Off	
Chassis		<u>1/4/x6</u>	IMPERV	Por	N		Disabled		sfp sx	-6.25	0/0	_	Off	
Roles and Users		<u>1/4/x16</u>		Por	N		Disabled		sfp sx	-5.81	0/0	_	Off	
小 − Health														
i≣ Logs														
🔅 Settings														
SUPPORT														
Get Started														
About														

Figure 7 Configure Ports

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

🎯 GigaVUE-FM	HC3 (H Series)	Q	C	4	B	admin -	•
НОМЕ	Ports : 1/4/x1,1/4/x2					ОК	Cancel
🔒 Overview							
💦 Workflows	Comment						
📥 Node Topology	comment.						
TRAFFIC	Port Role:						
📥 Ports	✓ Parameters						
ነ በ Maps							
💋 GigaSMART®	Admin 🖉 Enable						
🏠 Inline Bypass	Type Inline Network 🔻						
Active Visibility	Smand Select Second at						
CVCTEM	SpeedSelect Speed- *						
m Chassis	Duplex O Full O Half						
	Auto Negotiation Enable						
	Egress Vlan Tag 💿 None 💿 Strip						
	Farmer Link Un Enable						
:= Logs	Porce Link Op — Lindole						
Settings	✓ Ports Discovery						
SUPPORT							
Get Started	Network Discovery						
About	Discovery Protocols All OLLDP OCDP						
	Gigamon Discovery 🛛 🗎 Enable						

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.

🚳 GigaVUE-FM	HC3 (H Series)		Q (℃ 🔎	B	admin -	•
	Flexible Inlin	e Canvas		Prope	rties	OK	Cancel
A Overview	NEW	Delete + Zoom In □ Zoom Fit - Zoom Out Clear	r Canvas 🗹 Au	^{tofil} Configura	tion		
 Nodervnew Node Topology TRAFFIC Ports Maps GigaSMART® Inline Bypass Active Visibility SYSTEM Chassis Roles and Users Health Logs Settings SUPPORT Get Started 	NEW Flex Map OOB Copy Inline Network Inline Tool Inline Tool Inline Network O default_inline_net_1_4 O inline Tool Group	Collector, 1525300134 Collector, 1525300134	r <u>Canvas</u>	tofii Configura Alias flex-inline Comment Comment Port Edito Port Edito Port 8 № 1/4/x1 (Port 8 № 1/4/x2 (Traffic Path Bypass	r INET-A) INET-B) Propaga	tion	•
 Get Started About 		TX					

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.

🧐 GigaVUE-FM	10.115.94.11 (H Series)		Q	С		Ë 🖪	idmin 👻	8
номе	Inline SSL Configuration: Keychain Password						Prev	Next
Overview Workflows	Keych	ain password is mandatory for Inline SSL			O Kevch	ain Pass	word	
A Node Topology	Vaulacia Decenard	Action		(D Key St	ore		
🚔 Ports `W Maps	Reschain Fassword Password is not Setup	Setup Keychain Password		(O Signing	g CA		
ර GigaSMART® වී Inline Bypass				(O Trust S	store		
SYSTEM				(D Policy	Profile		
Roles and Users				(O Netwo	ork Access	S	

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.

🎯 GigaVUE-FM	10.115.94.11 (H Series)	Q	C		B	admin 👻	8
HOME	Inline SSL Configuration: Key Store					Prev	Next
A Overview N Workflows	Inline SSL requires both private key and certificate. Select or add a new Key Pair.			Kevc	hain Pas	sword	
A Node Topology	Key Pair Action			 O Key S	Store		
🖷 Ports भि Maps	Add Key Pair Generate Certificate			O Signi	ng CA		
🗳 GigaSMART®		-		O Trust	Store		
SYSTEM				O Polic	y Profile		
IIII Chassis				O Netw	ork Acc	ess	

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.

oigaVUE-FM				Q C 🌲 💾 admin- 😯
номе	Key Pair			OK Cancel
A Overview				
🏷 Workflows 🚠 Node Topology	Key Pair Alias *	mitm_primary		Keychain Password I
TRAFFIC	Туре	PEM PKC512		O Key Store
A Ports	Private Key	Copy and Paste Install from URL Install from Local Directory		O Signing CA
W Maps	Path	scp://root@121.0.0.1/root/sslcert/self_signed/primaryRSA.key	0	o signing at
S GIgaSMART®		e.g. scp://username@121.0.0.1/path/filename		O Trust Store
🖗 inline Bypass	Password			
SYSTEM				O Policy Profile
III Chassis	Costilizato	Constant from the install from 101 - Constall from Local Directory		
Roles and Users	Ceruncate	Copyrepase a insummer of insummer of costantion costantine		O Network Access
G Carrinac		Same remote location as Private Key		
- Seconda	Path	scp.//root@121.0.0.1/root/ssicert/self_signed/primaryRSA.crt	0	
20PPORT		e.g. scp://username@121.0.0.1/path/lifename		
Ø Get Started	Password			
About				
	Note: Private Key and	Certificate are both required for Inline SSL		
3	«			>>

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**.

3 GigaVUE-FM			Q	C 🕇	admin 🗸	8
	Inline SSL Configuration: Signing CA				Prev N	ext
	Configuration of	of Signing CA is mandatory for Inline SSL				
Kvortlovs Mode Topology TRAFTC Ports GigGSMART@ GigGSMART@ SYSTEM Chassis hotes and Users	Signing CA No CA is configured	Action Configure Signing CA		Keys Keys Keys Signi Trust O Polic O Netw	iain Password tore ing CA .Store y Profile rork Access	

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.

🎯 GigaVUE-FM	10.115.94.11 (il Series) Q	C 🜲 💾 admin 🔹 😯
номе	Signing CA	OK Cancel
A Overview		
Vorkflows	✓ Primary Root CA	Keychain Password
A Node Topology	Key Pair Allies man_primary	O Key Store
🖨 Ports	✓ Secondary Root CA	Signing CA
ገኛ Maps 🗳 GigaSMARTΦ	Key Pair Alles mitm_secondary	O Trust Store
Inline Bypass SYSTEM		O Policy Profile
IIII Chassis		O Network Access

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.

🞯 GigaVUE-FM	10.115.94.11 (H. Senieri) Q Q	C 📌 🗄 admin- 😯
номе	Inline SSL Configuration: Policy Profile	Prev Next
A Overview		
N Workflows	Select or create an mine SSL Prome	Keychain Password
A Node Topology	Policy Profile Action	O Key Store
Ports	Note Journal	 Signing CA
₩ Maps Ø GigaSMART®		l O Trust Store
🗭 Inline Bypass		 O Policy Profile
SYSTEM		O Policy Prome
Chassis Chassis Roles and Users		O Network Access

Figure 25 InlineSSL Configuration Workflow: Policy Profile

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

🚳 GigaVUE-FM Solu	ons FM 01.115 94.11 (H Series) Q	C 🖡 💾 admin- ?
		OK Cancel
	Alias* Inline_SSL_sample_config	
	✓ Policy Configuration	 Keychain Password I
	URL cache miss action () Decrypt () No Decrypt () Defer	O Key Store
Ports	Default Action 🔘 Decrypt 🖲 No Decrypt	Signing CA
G GigaSMART®	Decrypt Tool bypass 🛛 🚱	Trust Store
Inline Bypass	No Decrypt Tool bypass 🛛 🕢	l Indicisione
	Non-SSL TCP Traffic Tool bypass 🛛 🔞	O Policy Profile
	High availability 🔲	O Network Access
	Start TLS Port 1000, 2000, 3000	O Network Access
Roles and Users Health	✓ Security Exceptions	
	Self signed certificate 🛞 Decrypt 🛛 Drop	
	Unknown CA certificate	
	Invalid certificate Decrypt Drop	
	Expired certificate Decrypt Drop	
About	Revocation CRL	
	Revocation OCSP 🕜	
	Fail @ Soft ① Hard	»



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.

🔞 GigaVUE-FM	10.115.94.11 (H Series) Q (C 📌 💾 admin - 🛛
номе	Inline SSL Profile: inline_SSL_sample_config	OK Cancel
A Overview N Workflows ▲ Node Topology	Alies*	Keychain Password
TRAFFIC	Policy Configuration	O Key Store
Ports	> Security Exceptions	 Signing CA
Ƴ Maps ⋬ GigaSMART® ❥ Inline Bypass	✓ Whitelist/Blackist Whitelist	I Trust Store
SYSTEM ET Chassis A Roles and Users O Setrings SUPPORT O Get Started O About		O Policy Profile O Network Access
		»

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.

🚳 GigaVUE-FM Solu		Q	C		Ë	admin -	
HOME	Inline SSL Profile: inline_SSL_sample_config					OK Cance	
A Overview	✓ Policy Rules						
🏷 Workflows 🥼 Node Topology	Add a Rule			 Keyc 	hain Pass	sword	
TRAFFIC	* Rule 1			O Key S	Store		
E Ports	Category X						
₩ Maps	Value bot,nets Y			Signi	ng CA		
GigaSMART Ø GigaSMART Ø	No Derner			O Trust	t Store		
🗭 Inline Bypass	R Rule Z			1			
Active Visibility	Category ×			O Polic	y Profile	•	
SYSTEM	Value confirmed_spam_sources			O Netw	work Acce	ec.	
III Chassis	🗙 Rule 3 🔹 🖲 Decrypt			Oncen	IOIR ACCC	.33	
Roles and Users							
🎝 Health	Category X						
i≣ Logs							
Settings	x Rule 4 - 🖲 Decrypt 🔍 No Decrypt						
SUPPORT	Category ×						
Get Started	Value keyloggers_and_monitoring						
About	x Rule 5						
	Cotagory X Value malanze_sites Y						
	* Rule 6						
«	Category X Value phong and , other, founds		>	»			

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.

🞯 GigaVUE-FM	HC2 Inline SSL (H Series)				Q C	: 🕂 💾 admin- 🖓
	Inline SSI. Profile: inline_SSI					OK Cancel
Overview Workflows Node Topology THMFHC Parts GigaSMART® Inline Bypass Active Visibility	SMT LDAY NVTI HTTP (4) Default E Defa	> 465 > 636 > 563 > 443 c Out Port	25 339 119 80	ø		 Keychain Password Key Store Signing CA O Trust Store Policy Profile
SYSTEM III Chassis A Roles and Users Health	TCP Timeout TCP Inactive Timeout (minutes) 5					O Network Access
Logs Settings Support Get Started About	✓ Server Key Map	ierver Key Map Del Server * Key Pair Alias *	ete All 192.168.200.246 s2.example2.com	×		
4	c.					»

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.

oigaVUE-FM		Q	C	4 ⁹	Ë	admin +	8
номе	Inline SSL Configuration: Network Access					Prev 1	Next
A Overview 🕅 Workflows	Each GlgaSMART card requires IP address configuration for network access.			🛛 Keycł	hain Pa:	ssword	
A Node Topology	Action Configure Network Access			I O Key S	tore		
🚔 Ports भी Maps				 Signir 	ng CA		
ធ GigaSMART® អ Inline Bypass				Trust	Store		
SYSTEM				 Policy I Netw 	vork Ac	cess	

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.

Ports Ports Port Groups Turnel Ports Port Pairs Tool Mirrors Stadk Links X Port: 1/5/e1	Edit	dit
Procession All roles Ports Status up 75 Workflows Ports Status up		
III HARE HAPANES		
TALTTIC Filtered By: None IP Address 10:115.91.30		
Vi Maps Path Id Alass Type Speed Netmask 255 255 248 0 Vi Maps © 1/2/n6 ©		
Image: state way		
Strifter © 1/2/AB Image: Character Strifter Mmtu 1500 © © 1/2/AB Image: Character Strifter Image: Character Strift		
Ables and Users Original Origin		
SUPPORT D O Cet SMatted 0 1/2/x12		
About O		
■ 1/2/x15 THE 10.115.88.1 (10.115.88.1 (10.115.88.1) from 10.115.94.38 mgmth.12: 55(84) hytres of data. (4) hytres (rom 10.115.88.1 : 10m sage4 tt)=255 ttme=0.138 ms	~	*
• 1/2/x16 14 bytes from 30.115.8.11.1002, spa2-t12.35 t1:ene-3.26 m • 1/2/x16 a4 bytes from 30.115.8.11.1002, spa2-t12.35 t1:ene-3.26 m • 1/5/e1 14 bytes from 10.115.8.11.1002, spa2-t12.55 t1:ene-3.26 m • 1/5/e1 14 bytes from 10.115.8.11.1002, spa2-t12.55 t1:ene-3.26 m		
Storing B1 42:0142	+	÷

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 unintended 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.

🞯 GigaVUE-FM	HC2-Inline-SSL (H Series)		Q	C		в	admin -	0
	Inline SSL Map: Inline Network(s)						Prev	Next
Overview								
Workflows	Select an Inline Network or Inline Network	rk Group.			O Inlin	ne Net	work(s)	
	tnline Network(s)	Action			O Inlin	e Tool	s)	
Ports	Select a Inline Network Port or Inline Net	Create Inline Network						
W Maps					OGSO	Group		
GigaSMART®		Create Inline Network Group			O Mirt	In Dor		
Inline Bypass					O virtu			
Active Visibility	5				O GS (Operati	on	

Figure 34 InlineSSL Map Workflow: Inline Network

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

🞯 GigaVUE-FM) H	C2-Inline-SSL (H Series)							Q	C	1	Ш	admin	0
	*												ОК	Cancel
♠ Overview N Workflows ♣ Node Topology	Inline Network Info									O Inlin	e Netv	vork(s)		
		Alias	inline-nw								O Inlin	e Tool(s	;)	
Ports		Comment Comment	Comment								O GS G	Froup		
GigaSMART®					O Virtual Port									
 Inline Bypass Active Visibility system Chassis 		Port A	Port Editor	Ŧ							O GS C	peratic	n	
		Port B	1/1/x8	٠	•]						O Inlin	e Rule E	Based M	lap
Roles and Users		Configuration									O Inlin	e First L	evel Ma	ар
A Health		Traffic Path	Bypass	÷	•						O Inlin	e Secor	id Level	Мар
SUPPORT	ľ	Link Failure Propagation	V								O Colle	ector Ma	ap (bypa	ass)
Get Started	•										>>			

Figure 35 InlineSSL Map Workflow: Creating inline network

7. Configure Inline Tool

a. Click Create Inline Tool.

🚳 GigaVUE-FM	HC2-Inline-SSL (H Series)	Q	C		в	admin •	0
HOME	Inline SSL Map: inline Tool(s)					Prev	Next
Overview							
Workflows	Select an Inline Tool or Inline Tool Group or Inline Tool Serial.				Netw	ork(s)	
🛦 Node Topology	Inline Tool(s) Action			1			
TRAFFIC	Select a destination port.	-9		O Inlin	e 1001	(5)	
Ports:	Create Inline Tool	-		O GS G	roup		
W Maps	Create Inline Tool Group						
GigaSMART®				O Virtu	al Port		
Inline Bypass & Active Visibility	E			O GS C	perati	on	

Figure 36 InlineSSL Map Workflow: Creating inline tool

b. Configure the inline tool as illustrated below.

🙆 GigaVUE-FM	HC2-Inline-SSL (H Seciet)				 		q C	1	B admin -	0
: Rowe	Inline Tool Cisco-ASA-IPS								OK C	ancel
 Overview Workflows Nade Topology 	Inline Tool Info							o inline	Network(s)	
manic	Alles	Cisco-ASA-IPS						O Inline	Tool(s)	
Ports	Comment	cominisent						O GS Gr	oup	
G GigaSMART®	Ports							O Virtua	l Port	
Active Visibility		Port Editor						O GS Op	peration	
Dussis	Pert A	•						O inline	Rule Based M	lap
 Roles and Users Health 	Port B	•						O Inline	First Level Ma	p
Logs	Configuration							O inline	Second Level	Мар
Settings	Enabled	2						O Collec	tor Map (bypa	ass)
• Get Started	Failover action	Tool Bypass -								
Abour	Recovery Mode	autometic •								
	Inline tool sharing mode	Crable (Additional sags on the tool side)								
	Flex Traffic Pach	Select feectraffic path								
	Heartbeats									
	Enable Regular Heartbeat	N.						*		
		E 'au una 07	1	A 4 14/	<i>c</i>	· · · · · · · · · · · ·	,			

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.

<u> </u> GigaVUE-FM		Q C 📌 🗄 💷 🤊 🛛
HOME	GigaSMART Group	Cik Cancel
 A Overview N Workflows ▲ Node Topology 	✓ GigaSMART Group Info	Inline Network(s)
	Alias GSG5 Port.list unit -	 Inline Tool(s) GS Group
S GUISMARTS	← GigaSMART Parameters	O Virtual Port
9- mime typess	✓ Resource Buffer	O GS Operation
Chassis Chassis Roles and Users Settings	Enable Resource Packet Buffer () Enable Resource CPU () ASF (Application Session Filtering) ()	O Inline Rule Based Map O Inline First Level Map
Curront O Gei Starrent O Mout	✓ Dedup Action © Court: # Drop IP Teles: # Include © Ignore IP TOS # Include © Ignore TCP Sequence # Include © Ignore TCP Sequence # Include © Ignore TLAN © Include # Ignore Timer (ga) 5000	O Inline Second Level Map O Collector Map (bypass)
		~

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.

🞯 GigaVUE-FM	0.115.94.11 (n (eries)			Q	C 🚺	B edm	in• 🕐
HOME	Virtual Ports					OK	Cancel
A Overview							
Vorkflows	Alies	vp50			O In	ine Network(s)	
and a second second second second second second	GigaSMART Group	6565	*		O Ini	ine Tool(s)	
Ports	Mode	GTP Overlap			1		
W Maps	Inline Failover Action	Virtual port bypass •			0.03	Group	
G GIBSMARTE	Note: Default fail	over action for vport is Virtual port bypass.			O VI	rtual Port	
🎓 inline Bypess					0.65	Operation	
\$YEJ BAR					0.0.	operation	
IIII Chessis					O In	ine Rule Based	Map
• Seconda					O In	ine First Level M	Map
тыннонт					O In	ine Second Lev	el Map
Get Starsed About					0 00	llector Map (by	pass)

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.

🞯 GigaVUE-FM				۹	C	1	в	admn•	
HOME	GigaSMART Ope							OK Cancel	
A Overview									
A Hode Topology	Alies	out-issi				Inline	Networ	K(S)	
	GigaSMART Groups	6565				Inline	Tool(s)		
A Ports	GigaSMART Operations (GSOP)	Select one or more GSOP type(5)				GS Gro	oup		
W Maps		Inline SSL	×						
9 GigaSMARTIE		inline_SSL_sample_config	•		•	Virtual	Port		
Sector					c	GS Op	eration		
III Charles					c) Inline	Rule Ba	sed Map	
O Sentings					c) Inline	First Lev	vel Map	
Sumoni Get Started					c	Inline !	Second	Level Map	
0 About					c	Collect	tor Map	(bypass)	

Figure 40 InlineSSL Map workflow: Creating GigaSMART Operation

- 11. Configure the Inline Rule Based Map
 - a. Provide details as illustrated below and click **OK**.

🙆 GigaVUE-FM	101159411 # Servey	Q C 🍂 🗄 🚥 🧕 Ø
and the second se	New Map	OK. Center
 Overview Workflowi 	₩ Map Infe	Inline Network(s)
A Note Topology	Mag Alan para/HTP/H(1,1,1 Commonti	 Inline Tool(s)
¥ Naps Ø GigsSMARTE	Type indice * Suttype Sythus *	GS Group
 Here Spass Fritter There 	Traffic Peth Normal * Vormal *	GS Operation
Roses and Loses Semage Lange Get Started	Functionary Search Destination	O Inline First Level Map O Inline Second Level Map
O About	GigaSMART Openations (650P) Torra 🔻	O Collector Map (bypass)
	✓ Map Rules	
	Queb Status Import Anta Rule x Rule 1 Conducts serce	
	Fort/Destination X Mm< 80 Max. 0 to 05010	»

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.

🮯 GigaVUE-FM		Q C 📌 💾 admin- 🛛
HOME	New Map	OK Cancel
Overview Workliews	✓ Map Info	Inline Network(s)
La kode topology minisc ▲ Ports ¥ Mepi G organization	Mep Allas parate_nonHTTP_(H_{1},1,1) Comments Type Type Inline Proc.Lowel Subcype Ingress to Wrisal Port	 Inline Tool(s) GS Group Virtual Port
Infine typess	✓ Map Source and Destination	GS Operation
STITUE III: Charses A Roles and Users O Settings SUPPORT O Get Started	Port Editor Seurce Destination Image: Control of the second se	 Inline Rule Based Map Inline First Level Map Inline Second Level Map
0 About	✓ Map Rules	O Collector Map (bypass)
	Quick Editor Import Add a Rule; x Rule 1 Condition search	>>

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**.

🚳 GigaVUE-FM	10.115.94.11 (Hismes)	Q C 🥀 💾 💷 0
HOME	New Map	OK Cancel
Overview Workflows Mode Topology	✓ Map Info	Inline Network(s)
TRAFFIC POTIS W Mapp GigaSMART®	Map Allas rrapert, SSL, (N, 1, 1, 1) Coemannes Type Inline Second Level * Subtype Egress from Virtual Port *	 Inline Tool(s) GS Group Virtual Port
sectore	✓ Map Source and Destination	 GS Operation
Chassis Chassis Chassis Chassis Chass	Part Editor Source Transformation - Destination (GSCS) • GigaSMART Operations (GSCP) •	Inline Rule Based Map Inline First Level Map Inline Second Level Map Inline S
• ADOA	✓ Map Rules	O Collector Map (bypass)
	Curis Estar Import Add a Nule Wiley Order	
3	≪ Map Permissions	»

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.

🞯 GigaVUE-FM	10.115.94.11 (H Senters)	Q C 🥂 🗄 admo- 🛛
HOME	New Map	OK. Canot
 Overview Workflows Node topology 	✓ Map Info	Inline Network(s)
tharric Ports	And p Anas propension free, (r, c, c, q)	 Inline Tool(s) GS Group
W MADI GigaSMARTB P Infine Bypess	Type intinin * Subtype Collector *	 Virtual Port
SCOTTON Chessies	Trans Park Typess ■ Map Source and Destination	 GS Operation Inline Rule Based Map
Gettings	Furt Editor Source	 Inline First Level Map Inline Second Level Map
C Get Started	Descination Select ports. • GigsSMART Operations (GSOP) None •	O Collector Map (bypass)
	✓ Map Rules Quick Estror Import Adda Rule	
	← Map Order	
	<c .<="" priority="" th=""><th>»</th></c>	»

Figure 44 InlineSSL Map workflow: Creating the Shared Collector Map

c. Review the maps created by the workflow.

🙆 GigaVUE-FM								۹	C		н	admin •	0
HONE	Maps Map Templates	Filter Templates											
A Distivery	Maps							New Clone	(Tedel) / D	wists.	Delete All		4
A Node Topology													
TRAFFIC	Alas	Comments	Туре	Subtype	Priority	Number of rules	Source	Destination	GSOP		Ac	cess Level	Contracts
Ports Wildows	parse_HTTP_IN_1_1		inline	byRule	.3.	1	Pin default_inline_net	t impervation			adi	mun	~
GigaSMARTE	bypass_rest_IN_1_1_1		inline	collector(ByPass)		0	default_inline_net	L.			adi	nin	
🎾 Inline Dypess	parse_non-HTTP_IN_1_1		inlineFirstLevel	ingressToVp	2	(i	default_inline_net	. 💟 vp50			ad	min	
Sectors III Chasses	Impect_SSL_IN_1_1_1		inlineSecondLevel	egressRomVp	1	0	💟 vp50	Impervator	out-issi		edi	milita -	

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.

🞯 GigaVUE-FM	10.115.94.11 or Series					۹	C	1	в	admin •	0
номе	Inline Network default_i	nline_net_1_1_1								OK G	ncei
 Overview Workflows 	Inline Network Info										
A Node Topology	Alias	default_inline_net_1_1_1									
A Ports W Maps	Ports	Comment									
S GigaSMART®	and and a second se	Port Editor									
Series	Port A	1/2017	•								
 Roles and Users Serrings 	Configuration										
Culterari O Con Garried	Traffic Path	To Inline Tool	*								
About	Link Failure Propagation	8									
	Physical Bypass	0									
	Redundancy Profile		•								

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.

🞯 GigaVUE-FM									۹	C	۸	Ë	admin •	0
	Ports Port Gro	ups Tunnel Ports	Port Pairs 1	fool Mirrors Stack Ur	iks			×	Filter					Clear
	All Ports Ports	Discovery Statistics												
	Ports								Box ID/Slot ID Select a Box/Slo	ot (D		•		
	Filtered By : Port Type	Total Filtered Ports	11 Clear Filter						Port Allas Type Port Allas					
	O Port Id	Allas	Турс	Speed	Admin	Link Status	Transceiver Type	Ave	Port ID					
	1/1/105			1G	Enabled	up	sťp cu	07	Туре рогт #					
	I/1/1/16			1G	Enabled	up	sfp cu	07	СТуре					
	📋 😐 1/1/x10	OO8_tool_port	0	1G	Enabled	up.	sfp cu	07	Tout * Inine to	erebrk * Ini	ne Tout. P	್		
	I/1/x17		60	10G	Enabled	up	bps sx/sr	0/	Admin Status					
Roles and Users	I/1/x18		60	10G	Enabled	up	bps sx/sr	0/	(All	Enab	led	C Disabler	ł	
Settings	1/1/x19				Disabled	÷	bps sa/st	07	Link Status	© Up		C Down		
	1/1/x20		8		Disabled		bps sx/sr	07	Speed					
	I/1/x21		1 23		Disabled	4	bps sx/sr	0/	Select Port Sp	and 💌				
	1/1/k22		8		Disabled		bps sx/sr	07	Transceiver Typ	e celler Typic•				
	I/1/23		8		Disabled		bps sx/sr	0/	c					
	1/1/x24				Disabled		bps sx/sr	.07	c					

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.

🥘 GigaVUE-FM	10.115.94.11 (H Series)					Q 0	: 🔺	admin 🗸	8
HOME	Inline Networks Inline Network Groups	Inline Tools Inline Tool Group	ps Inline Serial Too	lls Heartbeats Redunda	incles				
A Overview	Inline Networks						New	Clone Edit I	Delete
Node Topology	Alias	Comment	Type	Forwarding State	Link Propagation	Physical Bypass		Traffic Path	
TRAFFIC	default_inline_net_1_1_1		protected	normal	true	disabled		To Inline Tool	
Ports	default_inline_net_1_1_2		protected	physicalBypass	true	enabled		Bypass	
GigaSMART®	default_inline_net_1_1_3		protected	physicalBypass	true	enabled		Bypass	
P Inline Bypass	default_inline_net_1_1_4		protected	physicalBypass	true	enabled		Bypass	
				Total Items : 4					

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.

🎯 GigaVUE-FM	10.115.94.11 (H Series)								۹	C		Ë	admin 🕶	8
номе	Inline Networks	Inline Network Groups	Inline Tools	Inline Tool Groups	Inline Serial Tools	Heartbeats	Redundancies							
A Overview	Inline Tools									New	Clone	Recover	Edit	Delete
A Node Topology	D. Atlan	C	Ownersting of Costs	talan Ta	1 Channa - C	- iter and the time	Conditional Linearching Contra-		and the				<i>a.</i>	
TRAFFIC	Alias	Lomment	up	enabled	* Status P	ool Bypass	Up	e default	ronie		медацие на	earcoeac Pro	nine	
Ports	Health	Status				Total Items	01	Heal	th Sta	tus				
GigaSMART®														
Inline Bypass														

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.

oigaVUE-FM	10.115.94.11 (H Series)								Q	C	۰	Ë	admin +	8
номе	Maps Map Templates	Filter Templates												
♠ Overview ★ Workflows	Maps Map Groups	Statistics												
A Node Topology	Maps						1	New C	lone	Edit	Delete	Delete All	=	ά
TRAFFIC														
Ports													1	Columns
ነበ Maps	Alias	Comments	Type	Subtype	Priority	Number of rules	Source	Destination	n	GSO	P	A	ccess Level	
🗳 GigəSMART®	parse_HTTP_IN_1_1_1		inline	byRule	1	1	INAA default_Inline_ne	t, 🗰 impe	rva101			a	dmin	^
🖗 Inline Bypass	bypass_rest_IN_1_1_1		inline	collector(ByPass)		0	IN default_inline_ne	۹				a	fmin	
SYSTEM	parse_non-HTTP_IN_1_1	1	InlineFirstLevel	IngressToVp	2	1	iN default_Inline_ne	r. 🔽 vp50				a	imin	
I Chassis	inspect_SSL_IN_1_1_1		inlineSecondLevel	egressFromVp	1	0	V vp50	iT imper	rva101	out-is:	sl	a	İmin	
© Settings	Health Status													

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.

	Po	rts Port Groups	Tunnel Po	rts Por	: Pairs	Tool Mirrors	Stack L	inks					x	Filter				Clear
	All	Ports Ports Disco	overy Stat	listics														
	St	atistics												Box ID/Slot ID Select a Box/Sic	c ID	•		
	0	Port ID	00	0015	Octer	s /sec	Unicast	Packets	Non-Unic	ast Packets	Packe	ts /sec	Packet Drops	Port Alias Type Port Alias				
TF Mars			Hx	Тх	Rx	Tx	RX	Ťκ	Rx	Tx	Rx	Ťκ	Rx	Port ID				
G GeoSMARTER		\varTheta 🚺 1/1785	188.63 M	9.96 M	63	63	148.03 K	54,46 K	88.79 K	88 79 K	1	1	D	Type port #				
 Inline Bypass 	0	1/1/x6	9.96 M	188.63 M	63	63	54.46 K	148.03 K	88.79 K	88.79 K	- 1C	- 3	0	Туре				
	0	🔿 🚺 1/1/x10	0	0	0	o	0	0	0	0	0	σ	Ð	Initine Network	Inline Tool > Too	-		
	10	l 🚺 1/1/x17	95.55 M	2.51 G	1.51.K	38.27 K	1.27 M	2.46 M	22.49 K	73	21	41	0					
	.0	I/1/2/18	2.51 G	96.78 M	38.31 K	1.53 K	2.5 M	1.29 M	73	22.49 K	41	22	0	Admin Status			-	
Roles and Users		1/1/1/x19	0	0	0	0	0	0	0		0	0	0	® Al	Enabled	O Disablei	d	
• Settings	U	1/1/x20	0	٥	D	0	0	0	0	o l	0	0	D	Link Status	⊖ Up	Down		
	0	1/1/x21	0	0	0	Ó	0	0	0	0	0	0	0					
	10	1/1/x22	0	0	0	0	0	0	0	0	0	.0	0	1				
About	.0	1/1/x23	0	0	0	0	0	0	0	c	0	0	0					
		1/1/x24	0	0		0	0	0	0	a	0	0	p					

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.

🮯 GigaVUE-FM	10.115.94.11	(H Series)			Q	G	н	admin 🗸	8
номе	Maps	Map Templates Riter Templates							
Overview	Maps	Map Groups Statistics							
🔥 Workflows	Statis	tics							Clear
TRAFFIC									
Ports		↑ Map Alias	Total Counters				Rules		
ነሰ Maps		bypass rest IN 1 1 1	27K Packets, 4.19M By	tes					
S GIgaSMART®	0	parse HTTP IN 1.1.1	72K Packets, 90.97M B	ytes			1		
Inline Bypass		parse non-HTTP IN 1.1.1	3.64M Packets, 2.48G E	Bytes			1		
SYSTEM			Total Items : 3						

Figure 52 Viewing Maps statistics

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

Mage	🮯 GigaVUE-FM				Q	с 🔺	drnin -)
May M		Maps Map Templates Filter Templates	×	Map: parse_HTTP_IN_1_1_1			Edit	1
Image: Ports Image: Mage:		Maps Map Groups Statistics Statistics					Hour Day Week Month (Use Mouse Scroll for Zeem In/Out)	
Support Adaptifie Adaptifie Adaptifie Adaptifie Comment Type Inline Bidirectional Support /ul>	TRAFFIC TY Maps S GigaSMARTO Inline Bypass 2YSTEM Chessis Roles and Users S Settings	Map Alas Dypass resc Ni 1 1 parse HTTP Ni 1 1 parse non ITTP Ni 1 1 parse non ITTP Ni 1 1	«	0 2017/43-31 10:12 0 Ours Rate (Br/n) 0 20163/21:022 20163/21:022 20163/21:022 20163/21:022 Cota Rate (Br	t t Vs) = Packets (sps)	2017-00-31 10:5	2 Tar	•
About Comment Comment P33.5005 About Type Inline Interestional Interestictuation Interestional Interestinterestice Interestictuational Intere				✓ Map Info	✓ Map Rules			
Contraction Destination Destin				Comment Type Inline Sub Type byRule Source @ default Inline net 1 1 1.	Rule 1 Bi-directional	√ 6		
		<i>"</i>		Destination impervation	portDst	80		

Figure 53 Viewing statistics for Classic Inline Map

Verifying GigaSMART Group Statistics

To verify GigaSMART group statistics:

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

🥸 GigaVUE-FM	10.115 94.11 (H Series)								Q	С		н	admin +	8
	GigaSMART Operations	s (GSOP) Gig	aSMART Groups	Virtual Ports	NetFlow / IPFIX	Seneration In	nline SSL Passive SSL	Application Session Filtering	GTP Whitelist					
	GigaSMART Groups	Statistics												
	Statistics												Clear U	pload
- Dorte	GS Group Allas	Rx Packets	Tx Packets	Rx Octets	Tx Octets	Packet Drops	Packets Received Errors	Heartbeat status of eport	Heartb	eat Rx Packe	:5	Heartbe	at Tx Packets	
W Maar	GSG2	0	0	0	0	0	0	up	179076			179076		
G GIRASMARTE	GSG5	3725229	3705226	2537824870	2529035714	0	0	up	179076			179076		

Figure 54 Viewing GigaSMART Group statistics

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

🥝 GigaVUE-FM	10.115.94.11 (H Series)								(a c	A 🗄	admin -
номе	GigaSMART Operations	(GSOP) Gig	aSMART Groups	Virtual Ports	NetFlow / IPFIX 0	Ser X	GS Group: GSG5					
A Overview	GigaSMART Groups	Statistics										
Norkflows	Statistics						✓ Aggregated 1/5/e1					
an Node Topology						_		1 sec	1 min	5 min	10 min	15 min
TRAFFIC	GS Group Allas	Rx Packets	Tx Packets	Rx Octets	Tx Octets	Packet I	CPU Useful Time	0	0	0	0	0
Ports	G5G2	0	0	0	0	0	CPU Idle Time	1560	976	974	970	956
וו Maps	GSG5	3725229	3705226	2537824870	2529035714	0	CPU Useful Percent	0	0	0	0	0
GigaSMART®							CPU Idle Percent	100	100	100	100	100
📽 Inline Bypass							Rx Packets	0	6	3	0	0
SYSTEM							Packet Drops	0	0	0	0	0
III Chassis						_	Packets Receive Errors	0	0	0	0	0
🚢 Roles and Users						~<						
Settings						-						

Figure 55 Viewing historical statistics of GigaSMART Group

Verifying GigaSMART Operation Statistics

To verify GigaSMART operations statistics:

- Verify stats reported under Navigation Pane > Traffic > GigaSMART > GigaSMART Operations (GSOP) > Statistics.
- 6. Click the GigaSMART Operation alias name to view the historical statistics.

🮯 GigaVUE-FM	10.115.94.11 (H	Series)								Q	G		Ë I	admin 🗸	8
номе	GigaSMAR	Operations (GSOP)	GigaSMART Groups	Virtual Ports	NetFlow / IPFl	X Generation	Inline SSL	Passive SSL	Application Session Filterin	GTP Whitelist					
A Overview	GigaSMART	Operation Stat	istics												
🏷 Workflows 🚠 Node Topology	Statisti	ics													
70.15510															
Borte	GSOP Alias	GS Group Alias	Map Allas	Rx Packets	Tx Packets	Rx Octets	Tx Octets	Packet Drops	Packet Drops No Init	Packets Terminated	Packe	ts Parse Errors		GS Operations	
۲۲ Maps	out-issi	GSG5	Inspect_SSL_IN_1_1_1	3.77 M	3.75 M	2.57 G	2.56 G	0	0	0	0			inline Ssl	
GigaSMART®															
🖗 Inline Bypass															

GigaVUE-FM	10.115.94.11 ()							Q	G	-	B	admin +	3
	GigaSMAR	T Operations (GSOP)	GigaSMART Groups	Virtual Ports	NetFlow / IPFI	X Ger X							
	GigaSMAR	T Operation Sta	tistics										
	Statist	ics					GS Group Alias: GSG5						
							Map Allas: Inspect_SSL_II	IN_1_1_1					- 1
	GSOP Allas	GS Group Alias	Map Allas	Rx Packets	Tx Packets	Rx Octets	ta Ganaral						- 1
	out-issi	GSG5	Inspect_SSL_IN_1_1_1	3.77 M	3.75 M	2.57 G	• General						-
GigaSMART®							Pkts Drop: 0						
Inline Bypass system							Pkts Rx: 3,767,936						
							Octets Rx: 2,566,436,72	26					
Roles and Users Settings							Pixts Term: 0						
							Octets Tx: 2,557,545,13	35					
Get Started About							Pkts Tx: 3,747,697						- 1
							Pkts Drop No Init: 0						
							Pkts Parse Err: 0						
							> Dssl						
							> Header Remove						
javascript:void(0)							> Sapf						

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.

🞯 GigaVUE-FM	10.115.94.1	1 (H Series)											Q	C	1	Ë	admin 🕶	8
номе	GigaSh	MART Opera	tions (GSOP)	GigaSMART Grou	ips V	irtual Ports	NecFlow	/ IPFIX Gen	×									Close
🕈 Overview	SSL Pro	ofiles	Key Store	Signing CA T	rust Store	Global	Defaults	Network /	Access									
N Workflows	Inlin									✓ Session Statistics								
🚠 Node Topology										Neme	Total	Active						
TRAFFIC	¥ Sum	mary									i di tan	Active						
Ports						in and the				Intercepted Sessions	29	17						- 1
₩ Maps	GigaSMA	RI	GS Group	Intercepted Sessio	ins (/vctive/1	ocal)	De	L Sessions (crypted	Non-De	SSL Sessions	29	17						
GigaSMART®	15.61		0000	16.1.07					16.130	Decrypted	9	1						- 1
🖝 Inline Bypass	1/5/61		6565	16727			07	8	167.19	Non-decrypted	20	16						
SYSTEM	✓ Sess	ion Statisti	cs							Non-SSL Sessions	0	0						
Roles and Users	Number	Interface	Src IP	Dst IP	Src Port	Dst Port	SNI		"	Forwarded Sessions	0	0						
Settings	#1	1/5/e1	192.168.1.3	63.241.103.45	62309	443	www.ansi.org	g		No. Delicy Statistics								
SUPPORT	#2	1/5/e1	192.168.1.3	204.2.197.201	62316	443	cspix.media6	5degrees.co	m	 Foncy statistics 								
Get Started	#3	1/5/e1	192.168.1.3	63.241.103.45	62310	443	www.ansi.org	g	_	Network Connection Loss	0							
About	#4	1/5/e1	192.168.1.3	104.16.27.235	62294	443	m.addthis.co	m		Decrypt	11							
	#5	1/5/e1	192.168.1.3	104.16.24.235	62295	443	m.addthised	ige.com	_	No Decrypt	18							
	#6	1/5/e1	192.168.1.3	205.210.187.194	62303	443	p.rfihub.com	1		Ut Loskup								
	#7	1/5/e1	192.168.1.3	63.241.103.45	62312	443	www.ansi.org	g	_	UT LOOKUP								
	#8	1/5/e1	192.168.1.3	63.241.103.45	62313	443	www.ansi.org	g		Url Un-categorized	0							
K.K.K.	#9	1/5/e1	192.168.1.3	104.16.26.2.35	62305	443	su addinis.co	em	_	Url Category Found	11							
K.K.K.K.	#10	1/5/e1	192.168.1.3	104 16 27 225	62315	443	m addithin co	2		Url Category Missing	0							
	#17	1/5/e1	192 168 1 3	104 16 16 35	67298	4/3	s7 addthis co		_	Url Category Match	0							
	<	1.0001	100.100.1.3		014.70													*

Figure 58 Viewing InlineSSL session summary

8. Click Show Details to view more details.

🎯 GigaVUE-FM							Keywords				Q	C	Ш	admin 🗸 👔	•
номе	GigaSh	MRT Operat	ions (GSOP)	GigaSMART (Groups	Virtual Po	rts NetFlow / IPFIX Ge	x	Session Det	tails : 1/5/e1				Close	1
A Overview	SSL Pro	ofiles	Key Store	Signing CA	Trust Scor	e Glo	bal Defaults Network	Access							Т
🏷 Workflows 📥 Node Topology	Inlin	e SSL S	ession S	Statistics					Counter Name	Network Server					
									Source IP	192.168.1.3					
Ports	✓ Sum	mary							Destination IP	63.241.103.45					
ዝ' Maps	GigaSMA	RT	GS Grou	ip S	SL Sessions	(Active/Tota	al)	No	Source Port	51554					
5 GigaSMART®				C	ecrypted	Non- Decrypter	1		Destination Port	443					
🍄 Inline Bypass	No Inline	SSL Session	Summary.						Protocol	SSL outbound					
SYSTEM	✓ Sessi	ion Statisti	cs						TCP State	Na:EST Nb:EST Ta:INIT Tb:INIT					
Roles and Users	Number	Interface	Src IP	Dst IP	Src Port	Dist Port	SNI		Decryption	NO					
Settings	#1	1/5/e1	192.168.1.3	104.16.21.35	51558	443	s7.addthis.com		Error	NO_ERR					
SUPPORT	#2	1/5/e1	192.168.1.3	216.58.194.200	51559	443	www.googletagmanager.co	m *.go	55L State	SSL_BYPASS					
Get Started	#3	1/5/e1	192.168.1.3	104.16.21.35	51557	443	s7.addthis.com	*.adi	C25 Status	EST					
About	#4	1/5/e1	192.168.1.3	216.58.194.196	51549	443	www.google.com		S2C Status	551					
	#5	1/5/e1	192.168.1.3	10.115.1.130	49396	40004									
	#6	1/5/e1	192.168.1.3	216.52.31.83	51587	443	cm.adgrx.com		1001 Status	TOOL BYMAS					
	47	1/5/e1	192.168.1.3	63.241.103.45	51554	443	www.ansi.org		Policy Verdict	NO_DECRYPT					
XXXX	#8	1/5/e1	192.168.1.3	207.200.74.133	51581	443	pixeLadvertising.com	pixel	Policy Match Fields	DOMAIN					
K K K K K K K K K K K K K K K K K K K	#9	1/5/01	192.168.1.3	52.52.238.30	51574	443	idsync.weborama.fr		URL Category						
25.26.26	#10	1/5/01	192.168.1.3	05.241.103.45	51502	443	www.ansi.org		URL Filter Result						
	#11	1/5/e1	192.168.1.3	104.16.27.235	51560	443	m.addthisedge.com	*.adi	Interface Pair	Na/Nb					÷

Figure 59 Viewing InlineSSL session detail statistics