

Deployment Guide: Inline SSL GigaVUE-OS 5.4

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 http://www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners

DOCUMENT REVISION - 9/5/2018

Contents

DEPLOYMENT CHECKLIST	5
INTRODUCTION	8
FLOWCHART FOR DEPLOYING THE INLINE SSL SOLUTION	12
USE CASES	14
ENABLING HTTPS INSPECTION FOR INTERNAL APPLICATIONS	15
ENABLING COMPLIANCE REQUIREMENTS ENFORCEMENT FOR DECRYPTED HTTPS TRAFFIC	20
ENABLING HTTPS INSPECTION FOR INTERNET TRAFFIC WITH AN EXPLICT PROXY	24
ENABLING HTTPS INSPECTION IN A HIGH-DENSITY DATA CENTER	29
ENABLING COMPLEX INLINE TOOL ARRANGEMENTS TO INSPECT INBOUND HTTPS TRAFFIC	42
ENABLING OUT-OF-BAND TOOLS TO INSPECT ALL INBOUND HTTPS TRAFFIC	44
ENABLING INLINE TOOLS TO INSPECT BOTH INBOUND AND OUTBOUND HTTPS TRAFFIC	46
CONFIGURATION TASKS	
Using the Inline SSL Configuration Workflow	48
Using the Inline SSL Map Workflow	55
Updating Inline Network Settings	61
DEPLOYING APF	62
VERIFICATION TASKS	67
VERIFYING PORT STATUS	67
VERIFYING INLINE NETWORK STATUS	67
VERIFYING MAP STATUS	68
VERIFYING PORT STATISTICS	69
VERIFYING MAP STATISTICS	69
VERIFYING GIGASMART GROUP STATISTICS	70
VERIFYING GIGASMART OPERATION STATISTICS	71
VERIFYING INLINE SSL SESSION STATISTICS	72
TROUBLESHOOTING GUIDE	73
GENERIC TROUBLESHOOTING STEPS	73
Ноw То	73
ISSL MONITOR MODE	76

Deployment Checklist

Deploying the Inline SSL Solution on a Gigamon device requires significant groundwork. This section provides a pre-deployment, deployment, and post-deployment checklist to help you plan and complete your deployment.

Use these checklists to make sure that the deployment is successful.

Pre-deployment checklist

- Review Inline SSL Decryption Guide GigaVUE-OS 5.4 to get familiar with the feature.
- Review the GigaVUE-OS Release Notes v5.4 for known issues that may impact your use case.
- Review the bandwidth (aggregate and SSL), latency, connections per second, and concurrent connection requirements for the applications you plan to decrypt.
- □ Analyze traffic flow by capturing pcaps with the existing set-up to identify packet attributes for filtering-in the intended traffic for inspection.
- Prioritize and deploy the Inline SSL Solution in phases and give a monitoring period of at least 48 hours between phases before proceeding with the next phase.
- For GigaVUE-HC2 devices, upgrade the GigaVUE-OS to 5.3.01.01 or later and the U-Boot to 2011.06.09 or later. For GigaVUE-HC3 devices, upgrade the GigaVUE-OS to 5.3.01.01 or later.
- □ Install the Inline-SSL license on the intended GigaSMART® module.
- Install or upgrade GigaVUE-FM to version 5.4 or later with the required licenses. Ensure that the GigaVUE-FM version matches with the GigaVUE-OS version. (GigaVUE-FM has workflow-based configurations to ease inline SSL deployment.)
- Verify that the Network Time Protocol (NTP) is configured so that the timestamps in the controller card logs are syncronized with the local time zone.
- □ Verify that email notifications are configured for, at least, the following events:

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
caviumcputemp:	Cavium CPU temperature notification

Backup the existing configuration so the configuration can be restored if necessary.

Deployment checklist

- Peered devices connected to side-A and side-B inline network ports must be operating at the same speed. Check the end-to-end connectivity across inline network links by redirecting the traffic along the bypass path (before redirecting the traffic to the inline tool).
- □ Inline tools **must** be configured in transparent mode to seamlessly work with the Inline SSL Solution.

NOTE: Heartbeat must 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.

Verify that inline tool(s) can accept Q-in-Q (double-tagged) traffic or disable the Inline Tool Sharing Mode option while configuring an inline tool.

NOTE: While creating inline tools using the Inline SSL Map workflow in GigaVUE-FM, the *Inline Tool Sharing Mode* option is enabled by default. This allows the Inline SSL solution to add a VLAN tag to decrypted HTTPS traffic that is forwarded to inline tool(s), and then strip the VLAN tag when forwarding encrypted traffic to the inline network. However, if the inline network traffic were to be VLAN-tagged, the decrypted HTTPS traffic would carry dual VLAN tags.

- 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 best practice, configure maps with more specific rules, first, before configuring maps with lessspecific or generic rules.
- □ If your network has IP fragments, make sure your first-level inline SSL map has a rule to filter-in TCP-protocol traffic. This will prevent IP fragments from getting lost.

NOTE: If the first-level map rule filters-in traffic based on the destination port, instead of protocol, then the GigaSMART engine will receive only the first fragment, because subsequent IP fragments will not carry TCP port information. As a result, the inline SSL decryption would not be able to decrypt all the fragments.

- □ Before directing traffic to the GigaSMART module, make sure that the 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.
- Application owners should execute sanity tests and measure application response times before and after deploying the solution. (Gigamon devices allow you to monitor inline-ssl statistics, but not the health of the applications.) The network operations team should ensure that the overall health of the network is maintained during the deployment.

Post-deployment checklist

- □ As a best practice, back-up of the configuration after the deployment for reference in case any issues are encountered later.
- □ Monitor traffic for at least 48 hours before proceeding with the next deployment.

Unsupported

- Inline SSL maps do not honor *ingress-vlan-tag* configurations on the member ports of an inline network group.
- Inline SSL does not support traffic-paths on inline network(s) to be set to *monitoring* mode.
- Inline SSL is not supported with Gigamon Resiliency for Inline Protection (GRIP).

Deployment notes

- Private key and certificate formats supported: PEM and PKCS #12.
- MitM Private key and certificate type supported: RSA.
- Private key must be installed before installing the certificate.
- A server's certificate file that is installed in a GigaVUE device must be a complete certificate chain and should include all of its intermediate CA certificates along with related trusted store certificates (Inter CA, Root CA).

Introduction

This deployment guide provides instructions for deploying Inline SSL on GigaVUE-OS 5.4 within an enterprise network. The use cases and configuration examples in this document are for illustration purposes only.

The Enterprise Network illustration in Figure 1 shows two diagrams:

- the Physical Topology diagram shows a user segment, a server farm, an internal firewall, an external proxy, an external firewall, and a gateway;
- the Logical Topology diagram shows the network's internal and external traffic flows.

Enterprise customers may want to inspect SSL traffic destined to internally-hosted applications and/or remote applications hosted on the Internet.



Figure 1 Enterprise Network

GigaSECURE® Security Delivery Platform's patented Flow Map® Technology coupled with its prevention capabilities, such as the Inline Bypass and Inline SSL solutions, offers a scalable model for enterprises to seamlessly inspect traffic as illustrated in Figure 2.

Even though intercepting inbound and outbound SSL sessions are illustrated separately, they can be achieved at the same time using a single GigaSMART® module. SSL traffic traversing server segments and links connecting to external networks can be intercepted at the same time using a single device if the associated links are connected via the Gigamon device.

Deploying the Inline SSL solution in server segments will enable intercepting the inbound SSL sessions and the East-West traffic. Deploying the solution in links connecting to external networks will enable intercepting the outbound SSL sessions and the North-South traffic.



Figure 2 GigaSECURE® Security Delivery Platform's enterprise network deployment

Solution Requirements

- Deployment mode: Inbound or Outbound inline SSL decryption/encryption.
 - Network traffic: Untagged or single VLAN tagged.
- Security Tools: Cisco Firepower IPS, FireEye APT, Imperva WAF and/or Splunk.

Setup (for illustration)

- Gigamon Device: 1 x GigaVUE-HC2
- Bypass Combo Module: 2 x BPS-HC0-D25B4G
- GigaSMART® module: 2 x SMT-HC0-X16 module

- GigaVUE-OS: Version 5.4 GA release
- GigaVUE-FM: Version 5.4 GA release

NOTE: GigaVUE-HC3 can be used instead of GigaVUE-HC2 depending on the performance requirements.

The above solution can also be deployed hierarchically in a high-density datacenter as illustrated in Figure 3 .

- The GigaVUE-HC1 devices in the Edge Layer enable aggregating the inline traffic.
- The GigaVUE-HC2 devices in the Core Layer enable Inline SSL inspection by directing the decrypted traffic to security tools.
- The cross links between the edge and core node provide node-level and link-level resiliency.
- The cross links between the core nodes and the WAFs provide resiliency to the inline tool.

In this setup, traffic steering to the inline tools is set as follows:

- a portion of the decrypted traffic is inspected by Intrusion Prevention System (IPS),
- a portion of the decrypted traffic is inspected by Web Application Firewall (WAF), and
- the rest of the decrypted traffic is inspected by both IPS and WAF.



Figure 3 Two-tier hierarchical deployment of GigaSECURE® Security Delivery Platform

Solution Requirements

- Deployment mode: Inbound or Outbound inline SSL decryption/encryption.
- Network traffic: Untagged or single VLAN tagged.
- Security Tools: Imperva WAF and Cisco Firepower IPS. (tools should support Q-in-Q if the network traffic is tagged)
 - Decrypted traffic: Portion of traffic to WAF, portion to IPS and the rest to both.
- Traffic load sharing: Redundant core nodes and to the security tools.
- Redundancy: Dual edge and core devices for high availability.

Setup (for illustration)

- Edge devices: 2 x GigaVUE-HC1 / GigaVUE-HC2s
- Core devices: 2 x GigaVUE-HC2s
- GigaSMART® modules: 2 x SMT-HC0-X16 module with inline-ssl license
- GigaVUE-OS: Version 5.4 GA release
- GigaVUE-FM: Version 5.4 GA release

Benefits

•

- Provides scalable architecture.
- Works seamlessly for untagged or single tagged network traffic.
- Provides option to bypass traffic that does not require inspection.
- Protects existing investments: Selectively feeds traffic and/or load balances traffic among multiple tools.
- Caters to increase in performance requirements: GigaSMART® modules can be grouped to meet increase in performance requirements. Up to five GigaSMART® modules can be installed in a GigaVUE-HC2 device.
- Caters to security and compliance requirements: Encrypted/decrypted traffic can be directed to another GigaSMART® module for generating metadata or selectively masking Personally Identifiable Information (PII). Refer to the latest *GigaVUE-OS Users Guide* for more information.
- Provides tool failover action.
- Allows adding/removing inline tools with minimal downtime.

Refer to the latest *Inline SSL Decryption Guide for GigaVUE-OS* for more details about GigaSECURE® Inline SSL Solution. Deploying the Inline SSL Solution also requires good understanding about Gigamon's Inline Bypass Solutions. Refer to the latest *GigaVUE-OS CLI Users Guide* for more details.

The following section describes deploying the above solutions.

Flowchart for deploying the Inline SSL Solution



Figure 4 Flowchart for deploying the Inline SSL Solution-Part 1



Figure 5 Flowchart for deploying the Inline SSL Solution—Part 2

Use Cases

This section describes the following use cases:

- Enabling HTTPS inspection for internal applications
- Enabling to enforce compliance requirements for decrypted HTTPS traffic
- Enabling HTTPS inspection for Internet traffic
- Enabling HTTPS inspection in a high-density datacenter
- Enabling complex inline tool arrangements to inspect inbound HTTPS Traffic
- Enabling an out-of-band tool to inspect all inbound HTTPS traffic
- Enabling an Inline tool to inspect both inbound and outbound HTTPS traffic

Enabling HTTPS Inspection for Internal Applications

Gigamon's Inline SSL Solution can be deployed to enable inspecting HTTPS traffic destined to internally hosted applications as illustrated below. It requires installing the intended server key pair (i.e. certificate and private key) in the Gigamon device.



Figure 6 GigaSECURE® inbound Inline SSL Solution Deployment.

Requirements

- Traffic flow: decryption/encryption is stateful. Let us review the traffic flow to identify packet attributes for filtering-in intended traffic using Flow Map®.
 - *Without Inline SSL Solution*: As illustrated above, the clients' traffic is sent on VLAN 100 to the Internal Firewall, which is the default gateway, via the Gigamon device. The firewall forwards traffic destined to internal servers on VLAN 201 to the Load Balancer, which in turn sends the traffic to the servers on VLAN 200.

With Inline SSL Solution: The clients' traffic loops back at the Internal Firewall. The same traffic traverses through the Gigamon device twice, but with different VLANs, 100 and 200 respectively. Hence, for intercepting the internal traffic, the rule set in Flow Map® must be configured with server IP, VLAN 200 and protocol TCP. If VLAN is not included in the map rule, the Gigamon device would drop the TCP connection upon receiving the duplicate traffic from the firewall. As a result, the interception would fail.

The traffic that does not require inspection could either be bypassed or sent to inline tools. This use case will filter in HTTP traffic and send it to the inline tool, and send the rest of the traffic along the bypass path.

Note: The rule set for filtering-in the intended traffic could include the destination port of a server. If the port number is included inadvertently and the application traffic were to be prone to IP fragmentation, the Gigamon device would not be able to decrypt all fragments since the TCP port number is carried only in the first fragment.

- Inline network requirements: Two protected inline network links are required. The uplink and the down link are port channels. Hence, the inline network links must be grouped to aggregate traffic. Until the flow maps are configured, Physical Bypass must be enabled on the protected inline networks to make sure that the network traffic is not affected.
- Inline tool requirements: The decrypted traffic must be inspected by an Advance Persistent Threat (APT) system, FireEye NX 2500. Since the inline network links are grouped, the Gigamon device will insert additional VLAN tag in the decrypted traffic that is sent to the inline tool. Since the network traffic is tagged, the decrypted traffic will be dual tagged. Since the inline tool can handle Q-in-Q traffic, Shared Mode will be enabled for the corresponding inline tool in the Gigamon device.

NOTE: If an inline tool cannot handle Q-in-Q, Shared Mode must remain disabled for the corresponding inline tool in the Gigamon device.

 Applications' requirements: Business and compliance requirements dictate which applications must be inspected. It is recommended to identify the list of applications to be inspected and deploy them in batches by interleaving monitoring periods (at least 48 hours) between the batches. This use case will demonstrate decrypting traffic that is destined to https://s2.example.com; rest of the HTTPS traffic will not be decrypted.

If the server certificate were to expire, the traffic is expected to continue to be inspected until the certificate is renewed.

 Key pair requirements: Deploying inbound Inline SSL Solution requires installing keypairs of intended applications in the Gigamon device. As seen below, https://s2.example.com certificate has Example Root CA as the root CA and has Example Sub CA as the intermediate CA.

The Example Root CA certificate is not included in the Inline SSL Trust Store, so the Trust Store must be updated.

While installing a server certificate in the Gigamon device, its intermediate CA certificates must also be provided. Hence, the server certificate and the Example Sub CA certificates must be copied in to a single file for installing in the Gigamon device. (Refer to the attached: Example Sub CA Certificate.)

2		Certificate Viewer: "s2.example.com"	+ = >
<u>G</u> eneral	Details		
Certifi	icate <u>H</u> ierar	chy	
▼Exan	nple Root CA		
▼E>	ample Sub C	A	

Figure 7 s2.example.com certificate chain

Example Sub CA Certificate



Ø DOWNLOAD from PDF Attachments

Configuration

The following prerequisite tasks must be completed before deploying the Inline SSL Solution in the Gigamon device.

Prerequisites:

- 1. Unlock the Keychain Password.
- 2. Update the Trust Store with the Root CA certificate of the server.
- 3. Install the server key pair and its certificate chain in the Key Store.
- 4. Create the inline SSL policy profile
 - a. Since no other traffic except that destined to https://s2.example.com must be decrypted, the default action should be retained as no-decrypt.
 - b. Policy rule must be configured to decrypt traffic destined to the IP address corresponding to https://s2.example.com.
 - c. Keymap must be configured with the key pair alias name corresponding to https://s2.example.com.

NOTE: The Gigamon device checks whether a server certificate matches by comparing its fingerprint with that of the one configured in the keymap. Hence, even if there were to be more than one application sharing the same certificate, only one keymap entry would suffice.

Inline SSL Configuration workflow in GigaVUE-FM walks through each of the above tasks. To launch the workflow, select the device from GigaVUE-FM Navigation Pane > Physical Nodes. From the device navigation pane, select: Workflows > Inline GigaSMART Operations.

Refer to Using Inline SSL Configuration Workflow in the Configuration Tasks section for the detailed steps.

To deploy the Inline SSL Solution:

1. Configure Inline Network Group

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

Since the inspected traffic must be inspected by the APT, a corresponding inline tool link must be created in the Gigamon device.

- 3. Configure GigaSMART Group
- 4. Configure Virtual Port
- 5. Configure Inline SSL GigaSMART Operation
- 6. Configure flow maps: Based on the earlier observations, below flow maps must be configured.
 - a. Classic Inline Map: To filter in HTTP traffic from the inline network group and send it to the inline tool.

NOTE: Classic Inline Map must not be created if Shared mode is disabled (Tagless mode) for inline tool(s). All TCP traffic can be forwarded to the GigaSMART module instead and Policy Rules can be configured in the inline-SSL profile to selectively decrypt the traffic.

- b. Inline First Level Map: To filter in the TCP traffic on VLAN 200 from the inline network group that is destined to the intended server IP address and send it to the virtual port for decryption.
- c. Inline Second Level Map: To decrypt traffic received on the virtual port by using Inline SSL GigaSMART operation (GSOP) and send the decrypted traffic to the inline tool.
- d. Shared Collector Map: To filter in the rest of the traffic from the inline network group and send it along the bypass path.

Flow B in Inline SSL Map workflow in GigaVUE-FM walks through each of the above steps.

To launch the workflow:

- 1. Select the device from the GigaVUE-FM Navigation Pane > Physical Nodes.
- From the device navigation pane, select: Workflows > Inline GigaSMART Operations. Refer to Using Inline SSL Map Workflow in the Configuration Tasks section for the detailed steps.
- After configuring the flow maps, the Physical Bypass must be disabled for the inline networks to allow the traffic to flow through the Gigamon device. The traffic-path of the inline networks must be set to toinline-tool. Refer to Updating Inline Network Settings in the Configuration Tasks section of this document for the detailed steps.

Gigamon device's CLI configuration:



OWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify inline SSL decryption/encryption:

- 1. Ports' health and statistics
- 2. Inline network health
- 3. Inline tool health
- 4. Map health and statistics
- 5. Virtual port or GigaSMART operation (GSOP) statistics
- 6. Inline SSL session summary
- 7. Inline SSL session runtime statistics

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

NOTE: If the Gigamon device were to fail in intercepting the TCP connections, configure the inline passall map between the inline network group and the inline tool. Capture the packet at the inline tool and analyze the traffic flow. Review the packet attributes to filter in the intended traffic. Deploy the Inline SSL Solution again and verify. Alternatively, the out-of-band inline network map can be configured. Please refer the Deployment Checklist section for details.

Enabling Compliance Requirements Enforcement for Decrypted HTTPS Traffic

For compliance purposes, the decrypted HTTPS traffic that is monitored out-of-band may have to be modified before feeding to an out-of-band tool. Figure 8 illustrates deploying GigaSECURE® Inline SSL Solution along with out-of-band GigaSECURE® Adaptive Packet Filtering (APF) Solution to mask Personally Identifiable Information (PII) from decrypted SSL traffic to meet such requirements. Decrypted traffic is directed to a Hybrid port. The APF GigaSMART operation (GSOP) is applied on the traffic that is looped back before forwarding to the out-of-band tool.



Figure 8 Compliant GigaSECURE® inbound Inline SSL Solution and out-of-band APF Deployment

Requirements

Most of the requirements discussed for Enabling HTTPS inspection for internal applications apply to this use case as well, except for the following ones.

Inline tool requirements: The decrypted traffic must be inspected by the IPS (Cisco ASA) followed by the APT (FireEye NX 2500). Since the inline network links are grouped, the Gigamon device will insert additional VLAN tag in the decrypted traffic that is sent to the inline tool. Since the network traffic is tagged, the decrypted traffic will be dual tagged. Since both inline tools can handle Q-in-Q traffic, Shared mode will be enabled for the corresponding inline tools in the Gigamon device.

NOTE: When the decrypted traffic is required to be inspected by more than one inline tool, even if one of the inline tools does not support Q-in-Q, Shared Mode must remain disabled for all inline tools in the Gigamon device.

Masking requirement: Identify which PIIs must be masked and how they are formatted. This
use case will demonstrate masking gender, age, email, credit card number and password in
https://s2.example.com/login.html.

<) → ୯ ଘ	(i) Attps://s2.example.com/login.html
First Name: Harry	
Last Name: Potter	
Gender: Male	
Age: 24	
E-mail: harry.potter@email.com	n
Credit card no.: 1234567890	12
Username: hpotter	
Password: cooldude	
Submit	

Figure 9 s2.example.com/login.html

Figure 10 provides packet capture of the decrypted HTTPS POST request. Notice the format in which the PIIs are presented as highlighted at the bottom.

POST /loginNew.php HTTP/1.1	
Host: s2.example.com	
Jser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86 64; rv:59.0) Gecko/20100101 Firefox/59.0	
<pre>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</pre>	
Accept-Language: en-US,en;q=0.5	
Accept-Encoding: gzip, deflate, br	
Referer: https://s2.example.com/login.html	
Content-Type: application/x-www-form-urlencoded	
Content-Length: 140	
DNT: 1	
Connection: keep-alive	
Jpgrade-Insecure-Requests: 1	

Figure 10 Wireshark® capture of the HTTPS POST request

- GigaSMART module: Inline SSL GigaSMART operation (GSOP) cannot be combined with other GSOPs. Hence, another GigaSMART module must be used for configuring APF.
- Optical transceiver. Only an optical port can be configured as a hybrid port. SFP+ transceiver should be plugged in one of the ports for the purpose.

Configuration

Please refer the Inline SSL Solution configuration described for "Enabling HTTPS Inspection for Internal Applications."

Use the following steps to mask the PIIs using APF pattern matching. Refer to Deploying APF in the Configuration Tasks section of this for the detailed steps.

To mask the PII using APF pattern matching:

- 1. Configure the port connected to the SIEM as a tool port.
- 2. Create a copy of the decrypted HTTPS traffic.
- 3. Configure the port that has optical transceiver as a hybrid port.
- 4. Configure inline second level map to direct the decrypted HTTPS traffic from the existing virtual port to the hybrid port using the existing inline SSL GigaSMART operation (GSOP).
- 5. Configure the APF GSOP.
 - a. Create a GigaSMART group with the other GigaSMART® module.
 - b. Create a virtual port for the GigaSMART group.
 - c. Create the APF GigaSMART Operation.
- 6. Configure flow maps for applying the APF GSOP.
 - a. First Level Map: To filter in TCP traffic received from the hybrid port and send it to the new virtual port for masking.
 - b. Second Level Map: To apply APF GSOP on the traffic received from the new virtual port for masking PIIs using the following GigaSMART APF RegEx rules and send the matching traffic to the SIEM.

```
gsrule add pass pmatch mask 0x2a RegEx "(?<=gender\\=)[\\x20-
\\x7e]{4}" 45..1518
gsrule add pass pmatch mask 0x2a RegEx "(?<=age\\=)[\\x20-\\x7e]{2}"
45..1518
gsrule add pass pmatch mask 0x2a RegEx "(?<=email\\=)[\\x20-
\\x7e]{22}" 45..1518
gsrule add pass pmatch mask 0x2a RegEx "(?<=creditCard\\=)[\\x20-
\\x7e]{12}" 45..1518
gsrule add pass pmatch mask 0x2a RegEx "(?<=password\\=)[\\x20-
\\x7e]{8}" 45..1518
```

c. Shared Collector Map: To filter in rest of the traffic received from the new virtual port and send it to the SIEM.

After configuring the flow maps, the Physical Bypass must be disabled on the inline network links to allow the traffic to flow through the Gigamon device. The traffic-path of the inline network links must be set to to-inline-tool.

Refer to Updating Inline Network Settings in the Configuration Tasks section of this for the detailed steps.

Gigamon device's CLI configuration:



OWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify inline SSL decryption/encryption:

- 1. Ports' health and statistics
- 2. Inline network health
- 3. Inline tool health
- 4. Map health and statistics
- 5. Virtual port or GigaSMART operation (GSOP) statistics
- 6. Inline SSL session summary
- 7. Inline SSL session runtime statistics

The APF masking can be verified using packet capture as illustrated below



Figure 11 Wireshark® capture of the HTTPS POST request after APF masking

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

Enabling HTTPS Inspection for Internet Traffic with an Explict Proxy

Gigamon Inline SSL Solution can be deployed to enable the inspection of HTTPS Internet traffic. As illustrated below, an Explicit Proxy is deployed to access the Internet. SSL sessions are set up differently when an explicit proxy exists. Clients initiate the TCP connection with the explicit proxy, which in turn initiates a TCP connection to a remote site. After the TCP connection is established, clients send HTTP-connect to the explicit proxy for initiating the SSL session with the remote site. The Gigamon device requires the startTLS option to be set for intercepting such sessions.

NOTE: Typically, clients send SSL Client Hello after establishing the TCP connection to a server. In this scenario, clients send SSL Client Hello after initiating HTTP connect to the explicit proxy. Hence, startTLS must be enabled on the Gigamon device to wait a little longer for intercepting the SSL session. If startTLS is not enabled, the Gigamon device will deem the connection as non-SSL soon after receiving the HTTP connect.



Requirements

- Traffic flow: Inline SSL decryption/encryption is stateful. Let us review the traffic flow to identify packet attributes for filtering-in intended traffic using Flow Map®.
 - Without Inline SSL Solution: As illustrated above, the clients' traffic is sent on VLAN 100 to the Internal Firewall, which is the default gateway, via the Gigamon device. The firewall forwards traffic destined to remote servers via the Gigamon device to the Explicit Proxy, which in turn sends the traffic to the External Firewall. The External Firewall does PAT (Port Address Translation) and forwards traffic to the remote servers.
 - With Inline SSL Solution: Internal Firewall sends L3 traffic to the Explicit Proxy. Hence, for intercepting the outbound traffic, the rule set in Flow Map® must be configured with protocol TCP.

The traffic that does not require inspection could either be bypassed or sent to inline tools. This use case will demonstrate filtering-in HTTP traffic and send it to the inline tool, and sending the rest of the traffic to the inline tool.

- Inline network requirements: Two protected inline network links are required. The uplink
 and the down link are port channels. Hence, the inline network links must be grouped to
 aggregate traffic. Until the flow maps are configured, Physical Bypass must be enabled
 on the protected inline networks to make sure that the network traffic is not affected.
- Inline tool requirements: The decrypted traffic must be inspected by an Advance Persistent Threat (APT) system, FireEye NX 2500. Since the inline network links are grouped, the Gigamon device will insert additional VLAN tag in the decrypted traffic that is sent to the inline tool. Since the network traffic is tagged, the decrypted traffic will be dual tagged. Since the inline tool can handle Q-in-Q traffic, Shared mode will be enabled for the corresponding inline tool in the Gigamon device.

NOTE: If an inline tool cannot handle Q-in-Q, Shared Mode must remain disabled for the corresponding inline tool in the Gigamon device.

- URL category requirements: Business and compliance requirements dictate which URL categories must be inspected. It is recommended to identify the list of categories to be inspected and deploy them in batches by interleaving monitoring periods (at least 48 hours) between the batches. This use case will demonstrate decrypting all Internet traffic except for few selected URL categories such as Finance, Healthcare and Legal.
- Signing CA requirements: In SSL proxy mode, the Gigamon device spoofs valid server certificates by re-signing it with the Primary Signing CA. If any Security Exceptions are allowed, even the invalid certificates will be re-signed by the Primary Signing CA until and unless the Secondary Signing CA is configured. In this use case, Security Exceptions are retained with the default values. Hence, only the Primary Signing CA is required.

The Primary Signing CA certificate must be installed in clients' browser so that it can validate the certificate without reporting any warning.

NOTE: If the Primary Signing CA is not configured, the Gigamon device will operate as a TCP proxy. As a best practice, install a Secondary CA, as well, to manage connections to sites with invalid certificates.

- Certificate Revocation Check requirements: Both CRL and OSCP certificate revocation checks are supported by the Gigamon device. This use case will enable both CRL and OCSP certificate revocation checks. The Gigamon device is expected to act as a TCP proxy if the certification revocation check were to fail.
- Network Access requirements: Since URL categorization and Certificate Revocation checks are required, the GigaSMART engine must have connectivity to the Internet. This use case will enable network access using DHCP.

NOTE: Alternately, user can assign static IP address to the GigaSMART engine.

Configuration

The following tasks must be completed before deploying Inline SSL Solution in the Gigamon device.

Configuration prerequisites:

- 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: As a best practice, install a Secondary CA, as well, to manage connections to sites with invalid certificates.

- 4. Create the inline SSL policy profile.
 - a. Since all Internet traffic must be inspected except for few selected URL categories, the default action should be changed to decrypt.
 - b. Enable OCSP and CRL certification revocation checks with the Hard fail option.

NOTE: When both OCSP and CRL certificate revocation checks are enabled, OCSP check will be performed first. If a server certificate does not support OCSP, the certificate revocation check will fall back to CRL. If the revocation check is unknown, the session will either be decrypted (Soft fail) or TCP proxied (Hard fail) depending on the configured failover option. As a best practice, if the revocation check is unknown, configure the TCP proxy (Hard fail) for those sessions.

- c. StartTLS should be enabled for port 8080 (port number of the explicit proxy).
- 5. Set policy rules to "no-decrypt" for categories such as financial_services, health_and_medicine, individual_stock_advice_and_tools, legal URL, and others as needed.
- 6. Configure the network access for the GigaSMART® engine interface by enabling DHCP.

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

To launch the workflow:

1. Select the device from the GigaVUE-FM Navigation Pane > Physical Nodes.

- 2. From the device navigation pane, select: Workflows > Inline GigaSMART Operations.
- Refer to Using Inline SSL Configuration Workflow in the Configuration Tasks section for the detailed steps.
- 4. Complete the following steps to deploy the Inline SSL Solution.

To deploy the Inline SSL Solution:

1. Configure Inline Network Group

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
- 3. Configure GigaSMART Group
- 4. Configure Virtual Port
- 5. Configure Inline SSL GigaSMART Operation
- 6. Configure flow maps: Based on the earlier observations, below flow maps must be configured.
 - a. *Classic Inline Map*: To filter in HTTP traffic from the inline network group and send it to the inline tool.

NOTE: If the shared mode is disabled for inline tool(s), do not create a Classic Inline Map to filter traffic to the tools. Instead, send all the TCP traffic to the GigaSMART engine, and then configure Policy Rules in the inline-SSL profile to selectively decrypt the traffic.

- b. *Inline First Level Map*: To filter in the TCP traffic from the inline network group and send it to the virtual port for decryption.
- c. *Inline Second Level Map*: To decrypt traffic received on the virtual port by using Inline SSL GigaSMART operation (GSOP) and send the decrypted traffic to the inline tool.
- d. *Shared Collector Map*: To filter in the rest of the traffic from the inline network group and send it to the inline tool.

NOTE: When Shared Mode is disabled for inline tool(s), the inline SSL maps track flows based on MAC address. Unlike the inline SSL Maps, the Shared Collector Map would require an internal VLAN tag to track flows. Hence, the Shared Collector map cannot be configured to direct traffic to inline tool(s). Instead, it can be configured to direct traffic along the bypass path.

Flow A in the **Inline SSL Map** workflow in GigaVUE-FM walks through each of the above steps.

To launch the workflow:

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

4. Complete the following steps to deploy the Inline SSL Solution.

After configuring the flow maps, the Physical Bypass must be disabled for the inline networks to allow the traffic to flow through the Gigamon device. The traffic-path of the inline networks must be set to to-inline-tool.

Refer to Updating Inline Network Settings in the Configuration Tasks section for the detailed steps.

Gigamon device's CLI configuration:



Ø DOWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify inline SSL decryption/encryption:

- 1. Ports' health and statistics
- 2. Inline network health
- 3. Inline tool health
- 4. Map health and statistics
- 5. Virtual port or GigaSMART operation (GSOP) statistics
- 6. Inline SSL session summary
- 7. Inline SSL session runtime statistics

Refer to Verification Tasks section for the detailed steps.

NOTE: If the Gigamon device were to fail in intercepting the TCP connections, configure the inline passall map between the inline network group and the inline tool. Capture the packet at the inline tool and analyze the traffic flow. Review the packet attributes to filter in the intended traffic. Deploy the Inline SSL Solution again and verify. Alternatively, the out-of-band inline network map can be configured. Please refer the Deployment Checklist section for details.

Enabling HTTPS Inspection in a High-Density Data Center

Figure 13 illustrates deploying GigaSECURE® Security Delivery Platform in a two-tier hierarchical architecture for aggregating traffic and enabling inline SSL inspection for traffic destined to internally hosted applications in a high-density datacenter.



Figure 13 Two-tier hierarchical deployment of GigaSECURE® Security Delivery Platform





Edge Layer Device Configuration

To configure the Edge layer devices:

1. Configure the inline network ports as illustrated below:

Ports : 1/2/x5	
Alias	
Comment:	
Port Role:	
¥ Darameters	
• Falameters	
Admir	Rable
Туре	Inline Network
Speed	1 10G 💌
Duples	K ● Full ◎ Half
Auto Negotiation	n 🔲 Enable
VLAN Tag	g 100
Egress Vlan Taj	g 🖲 None 🖉 Strip
Force Link U	n 🗖 Enable

Figure 15 Configuring Inline Network Port

- a. The inline network ports can be protected or unprotected. If the uplinks to the firewalls / routers are configured for resiliency, unprotected ports can be used. Inline network ports' speed can be either 1Gb or 10Gb.
- b. Inline network group configuration adds distinct VLAN tags for the traffic that ingresses on each of the inline network ports. For this solution, you **must** configure the same VLAN ID on the member ports of an inline network. Different inline networks in an inline network group can be configured with different VLAN tags.
- 2. Configure the inline networks as illustrated below:

Inline Network defa	ault_inline_net_1_2_1	
Inline Network Info		
Alies	default_inline_net_1_2_1	
Comment	Comment	
Ports		
	Port Editor	
Port A	1/2/x5	•
Port B	1/2/x6	•
Configuration		
Traffic Path	To Inline Tool	•
Link Failure Propagation	V	
Physical Bypass		
Redundancy Profile	Select redundancy profile	•
Figure 16	Configuring Inline Network	(

3. Configure the inline network groups as illustrated below:

Inline Network Gro	up ING1
Inline Network Group Info	
Alias	ING1
Comment	Comment
Inline Network Links	
Inline Network	iN•• default_inline_net_1_2_1 iN•• default_inline_net_1_2_2

Figure 17 Configuring Inline Network Group

4. Configure the Inline Tools as illustrated below.

NOTE: Heartbeat is intentionally disabled by default, as indicated by the unselected check box. The inline tool for an edge device is another Gigamon device, and heartbeat between Gigamon devices is not supported. The inline tool failure action is triggered when a peer port is physically down due to either link failure or device failure.

Inline Tool IT1	
Inline Tool Info	
Alias	ITI
Comment	comment
Ports	
	Port Editor
Port A	1/1/x1 (HC2-1-T1A) •
Port B	1/1/x2 (HC2-1-T1B)
Configuration	
Enabled	
Lindbleu	
Failover action	ToolByPass •
Recovery Mode	automatic -
Inline tool sharing mode	Enable (Additional tags on the tool side)
Flex Traffic Path	To Inline Tool x v
Heartbeats	
Enable Regular Heartbeat	
Regular Heartbeat Profile	default -
HB IP Address A	0.0.0.0
HB IP Address B	0.0.0.0
Enable Negative Heartbeat	
Negative Heartbeat Profile	Ψ.
Figure 18	Configuring Inline Tool

5. Configure inline tool groups as illustrated below:

NOTE: Failover Action is set to *Network Port Forced Down* for enabling Physical Bypass on protected inline network or for enabling the traffic on unprotected inline network to switchover to the redundant path.

Inline Tool Group ITG1	
Inline Tool Group Info	
Alias	ITG1
Comment	Comment
Ports	
Inline Tools	П •• m П •• т 2 •
Inline Spare Tool	Select inline spare tools •
Configuration	
Enabled	
Release Spare if Possible	
Failover Action	NetworkPortForcedDown *
Failover Mode	Spread -
Minimum Healthy Group Size	1 •
Hash	advanced *
Flex Traffic Path	To Inline Tool x v

Figure 19 Configuring Inline Tool Group

- 6. Configure the Inline Maps:
 - a. Configure rule-based Inline Map for forwarding all traffic to the Core layer as illustrated below. The same can be achieved by configuring pass-all map however a rule-based map provides flexibility to filter in only the intended traffic.

Map Info	
Map Alias	AliTraffic_to_HC2
Comments	
Enable	
Туре	Inline
Subtype	By Rule 👻
Traffic Path	Normal
Map Source and Destination	
Source	Port Editor
Destination	- • • • •
GigaSMART Operations (GSOP)	None *
Map Rules	
≭ Rule 1 (Read Only) Rule Comment	Quick Editor Import Add a Rule Condition search •
	MAC Source X 00:00:00:00:00 / 00:00:00:00
Map Order	
Priority	v

b. *Configure the inline shared collector map*, as illustrated below, to forward all other traffic along the inline network.

✓ Map Info				
Map Alias	bypass_rest			0
Enable	2			
Туре	Inline	*		
Subtype	Collector	T		
Traffic Path	ByPass	Ψ		
✓ Map Source and Destination	n			
	Port Editor			
Source	INA ING1 ×		•	
Destination	Select ports		•	
GigaSMART Operations (GSOP)	None		¥	

Figure 21 Configuring Shared Collector Inline Map

7. Click Floppy-Disk icon in the top menu to save the device configuration to the nonvolatile memory.

Core Layer Device Configuration

As stated above, the devices in the Core layer can decrypt/encrypt inline SSL traffic as well as steer and load balance decrypted traffic among inline tools.

Steering traffic to inline tools depends on how the inline tools are expected to inspect the decrypted traffic. In the scenario described above, the decrypted traffic must be inspected by the IPS followed by the WAF. Since there is more than one WAF, you should combine them in to an inline tool group to enable the Gigamon device to load-balance decrypted traffic among the WAFs.

To achieve this, the Gigamon device must be configured to forward decrypted traffic to the IPS. The inspected traffic must also be physically looped back to another inline network on the same device for forwarding the traffic to the WAF inline tool group, as illustrated in Figure 22.



Figure 22 Traffic steering at a Gigamon device in the Core layer.

To configure the Core layer devices:

1. Configure inline network ports.

Ports : 1/4/x13							
Alias Comment: Port Role:	NSU1A						
✓ Parameters							
Auto	Admin Type Speed Duplex Negotiation VLAN Tag ess Vlan Tag	Enable Inline Net Inline Net Inline Net Enable None Full None Full	Work				
✓ Ports Discovery							
Network Discove Gigamon	Discovery 🔁 ry Protocols Discovery 🤁	C Enable	C LLDP	CDP			
✓ Alarms							
Buffer Threshold (%) Utilization Threshold (%)	Rx High	0				Tx Low	0

Figure 23 Configuring Inline Tool Port

NOTE: The inline network ports can be unprotected if the uplinks that are connected to the edge Gigamon devices are configured for resiliency. The inline network ports' speed can be either 1Gb or 10Gb. Configure inline network ports as illustrated below.

2. Configure the inline networks as illustrated below.

Inline Network NSU1					
Inline Network Info					
Alias	N5U1				
Comment	Comment				
Ports					
	Port Editor				
Port A	▶ 1/4/x13 (NSU1A) -				
Port B	N 1/4/x14 (NSU1B)				
Configuration					
Traffic Path	To Inline Tool •				
Link Failure Propagation					
Figure 24	Configuring Inline Network				

3. Configure the inline network groups as illustrated below.

Inline Network Group ING1					
Inline Network Group Info					
Alias	ING1				
Comment	Comment				
Inline Network Links					
Inline Network	INI NSUT				
Figure 25	Configuring Inline Network Group				
4. Configure the inline tools as illustrated below.

Inline Tool ISSL_IT	
Inline Tool Info	
Alias	ISSLJT
Comment	comment
Ports	
	Port Editor
Port A	1/4/x11 (ISSL_ITA)
Port B	1/4/x12 (ISSL_JTB) -
Configuration	
Enabled	
Failover action	NetworkPortForcedDown •
Recovery Mode	automatic •
Inline tool sharing mode	Enable (No additional tags on the tool side)
Flex Traffic Path	To Inline Tool x *
Heartbeats	
Enable Regular Heartbeat	
Regular Heartbeat Profile	default -
HB IP Address A	0.0.0.0
HB IP Address B	0.0.0.0
Figure	26 Configuring Inline Tool

5. Configure the inline tool groups as illustrated below.

Inline Tool Group Imperva_T	ſĠ
Inline Tool Group Info	
Alias	Imperva_TG
Comment	Comment
Ports	
Inline Tools	ITTE Imperval TTE Imperva2
Inline Spare Tool	Select inline spare tools
Configuration	
Enabled	V
Release Spare if Possible	
Failover Action	ToolByPass •
Failover Mode	Spread -
Minimum Healthy Group Size	1 -
Hash	advanced *
Flex Traffic Path	To Inline Tool x v
Fiaure 27	Configuring Inline Tool Group

6. Configure Inline Maps:

Two sets of Inline Maps, one for feeding decrypted traffic to the IPS and the other for feeding decrypted traffic to the WAF inline tool group, must be configured.

a. Configure the First Level Inline SSL Map for filtering-in the intended traffic and the Second Level Inline SSL Map for feeding decrypted traffic to the IPS.

Map: AllTraffic_to_GS		Map: Intercepte	edTraffic
Map Info			
Map Alias	AllTraffic_to_GS	✓ Map Info	
Comments		Man Alias	IntercentedTraffic
Enable	×	map Allas	merceptearrant
Туре	Inline First Level	Comments	
Subtype	Ingress to Virtual Port	Enable	2
ap Source and Destination		Туре	Inline Second Level
	Port Editor	Subtype	Egress from Virtual Port
Source			
Destination	🖸 opt -	 Map Source and Destination 	on
GigaSMART Operations (GSOP)	None *		Port Editor
p Rules		Source	Vp1 ×
	Quick Editor Import Add a Rule		
x Rule 1	Condition search	Destination	ITT ISSLJT -
Rule Comment	Comment		
	MAC Source	x GigaSMART Operations (GSOP)	ISSL-GSOP(ISSL)

Figure 28 Configuring first level Inline SSL map – and – Configuring second level Inline SSL map

b. Configure classic Inline Maps as illustrated below for feeding decrypted traffic to the WAF inline tool group and bypassing rest of the traffic. Note that the map rules matching the inner VLAN tags correspond to the network traffic.

Map Info	
Map Alias	Imperva_Traffic
Comments	
Enable	*
Туре	Inline 🔻
Subtype	By Rule 🔻
Traffic Path	Normal
Man Source and Destination	
	PortEcitor
Source	The second secon
Destination	TIS Impana_16 -
GigaSMART Operations (GSOP)	None
Map Rules	
	Quick Editor Import Add a Rule
x Rule 1	Condition search
(Read Only	
Rule Comment	Inner VI AN
	Min 500 Max 1 to 4094
	Subset 🔻
× Rule 2 (Read Only	Condition search • Ress. © Drop © Bi-directional
	Command
Rule Comment	West and the second
Rule Comment	Inner VLAN

Figure 29 Configuring Classic Inline Map for sending traffic to WAF inline tool group

✓ Map Info			
Map Alias	Imperva_Collector		
Comments			
Enable	×		
Туре	Inline	Ŧ	
Subtype	Collector	*	
Traffic Path	ByPass	T	
✓ Map Source and Destination			
	Port Editor		
Source	Imperva_IN ×		•
Destination	Select ports		•
GigaSMART Operations (GSOP)	None		Ŧ

7. Click Floppy-Disk icon in the top menu to save the device configuration to the nonvolatile memory.

Gigamon device's CLI configuration:



issl-high-density-dc -CoreDevice2.cfg.pd





OWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify inline SSL decryption/encryption:

- 1. Ports' health and statistics
- 2. Inline network health
- 3. Inline tool health
- 4. Map health and statistics
- 5. Virtual port or GigaSMART operation (GSOP) statistics
- 6. Inline SSL session summary
- 7. Inline SSL session runtime statistics

Refer to VerificationTasks section for the detailed steps.

Enabling Complex Inline Tool Arrangements to Inspect Inbound HTTPS Traffic

Gigamon's Inline SSL Solution can be deployed to enable the inspection of HTTPS traffic destined to internally hosted applications with multiple tools connected in a series, as illustrated in Figure 31.



Figure 31 GigaSECURE® inbound Inline SSL Solution multiple tool in series.

Requirements

- Traffic flow: Requirements discussed in the use case Enabling HTTPS Inspection for Internal Applications' apply to this use case as well, additional requirements are listed below.
- *Inline tools requirements*: The decrypted traffic must be inspected by tools that are connected in a series that includes Advance Persistent Threat (APT) and FireEye NX 2500s in an inline tool group, and Imperva WAFs as inline tools connected in serial.

Configuration

To inspect HTTPS Traffic and guide it through tools connected in series:

- 1. Configure tool group with both FireEye's and enable advanced hashing.
- 2. Configure inline serial pair with inline-tool group, along with Imperva.

Refer to the Inline SSL Solution configuration described in the use-case "Enabling HTTPS Inspection for Internal Applications."

Gigamon device's CLI configuration:



OOWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify inline SSL decryption/encryption:

- 1. Ports' health and statistics
- 2. Inline network health
- 3. Inline tool health
- 4. Map health and statistics
- 5. Virtual port or GigaSMART operation (GSOP) statistics
- 6. Inline SSL session summary
- 7. Inline SSL session runtime statistics

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

NOTE: If the Gigamon device were to fail in intercepting the TCP connections, enable SSL in monitor mode, Please refer to ISSL Monitor mode for details. Capture the packet at the inline tool and analyze the traffic flow. Review the packet attributes to filter in the intended traffic. Deploy the Inline SSL Solution again and verify. Alternatively, the out-of-band inline network map can be configured to send the traffic to out-of-band tool. Please refer the Deployment Checklist section for details.

Enabling Out-Of-Band Tools to Inspect All Inbound HTTPS Traffic

Gigamon's Inline SSL Solution can be deployed to enable an out-of-band tool to inspect all inbound HTTPS traffic, as illustrated in Figure 32.



Figure 32 GigaSECURE® inbound Inline SSL Solution with SIEM

Requirements

- Most of the requirements discussed for 'Enabling HTTPS Inspection for Internal Applications' apply to this use case as well, except for the following ones
- *SIEM Tool Requirement*: The SSL, non-SSL, non-TCP traffic sent to Splunk out-ofband tool, since the inline network links are grouped.

Configuration

Please refer the Inline SSL Solution configuration described for "Enabling HTTPS Inspection for Internal Applications."

To deploy SIEM:

- 1. Configure the port connected to the SIEM as a tool port.
- 2. *Inline First Level Map*: To filter in the TCP traffic from VLAN 100 from inline network group and send it to the virtual port for decryption.
- 3. *Inline Second Level Map*: To decrypt traffic received on the virtual port by using Inline SSL GigaSMART operation (GSOP) and send the decrypted traffic to the inline tool.
- 4. *Inline Second Level OOB Map*: To decrypt traffic received on the virtual port by using Inline SSL GigaSMART operation (GSOP), non-SSL and non-TCP traffic from virtual port to tool port (out-of-band tool).
- 5. *Shared Collector Map*: To filter in the rest of the traffic from the inline network group and send it to the inline tool.

Gigamon device's CLI configuration:



OOWNLOAD from PDF Attachments

Monitoring

- 1. Monitor the following to verify inline SSL decryption/encryption
- 2. Ports' health and statistics
- 3. Inline network health
- 4. Inline tool health
- 5. Map health and statistics
- 6. Virtual port or GigaSMART operation (GSOP) statistics
- 7. Inline SSL session summary
- 8. Inline SSL session runtime statistics
- 9. Verify on SIEM for decrypted, non-ssl, and non-tcp sessions.

Enabling Inline Tools to Inspect both Inbound and Outbound HTTPS Traffic

The Gigamon Inline SSL Solution can be deployed to use one GigaSMART engine to decrypt both inbound and outbound traffic at the same time, as illustrated in Figure 33.





Requirements

Traffic flow: Most of the requirements discussed for "Enabling HTTPS Inspection for Internet Traffic with an Explict Proxy" apply to this use case as well, except for the following ones.

Client traffic from VLAN 100 would be intercepted by a single GigaSMART engine for both inbound and outbound connections.

Configuration

Please refer the Inline SSL Solution configuration described for "Enabling HTTPS Inspection for Internet Traffic with an Explict Proxy"

To set-up inline tools to inspect both inbound and outbound HTTPS traffic:

- 1. Configure the GigaSMART Group (only single GigaSMART engine).
- 2. Configure the Virtual Port (single virtual port for both inbound and outbound).

- 3. Configure the Inline SSL GigaSMART Operation.
- 4. Configure flow maps:

Based on the earlier observations, the following flow maps must be configured:

- 1. *Inline First Level Map*: configure to filter-in the TCP traffic from VLAN 100 in an inline network group and send it to the virtual port for decryption.
- 2. *Inline Second Level Map*: configure to decrypt traffic received on the virtual port by using the Inline SSL GigaSMART operation (GSOP) and sending the decrypted traffic to the inline tool.
- 3. *Shared Collector Map*: configure to filter in the rest of the traffic from the inline network group and send it to the inline tool.

Gigamon device's CLI configuration:



OWNLOAD from PDF Attachments

Monitoring

Monitor the following to verify inline SSL decryption/encryption:

- 1. Ports' health and statistics
- 2. Inline network health
- 3. Inline tool health
- 4. Map health and statistics
- 5. Virtual port or GigaSMART operation (GSOP) statistics
- 6. Inline SSL session summary
- 7. Inline SSL session runtime statistics

Refer to Verification Tasks section for the detailed steps.

NOTE: If the Gigamon device were to fail in intercepting the TCP connections, Enable SSL in monitor mode, Please refer the ISSL Monitor mode Capture the packet at the inline tool and analyze the traffic flow. Review the packet attributes to filter in the intended traffic. Deploy the Inline SSL Solution again and verify. Alternatively, the out-of-band inline network map can be configured to send the traffic to the out-of-band tool. Please refer the Deployment Checklist section for details.

Configuration Tasks

This section provides steps for the following tasks

- Using the Inline SSL Configuration Workflow
- Using the Inline SSL Map Workflow
- Updating Inline Network Settings
- Deploying APF

Using the Inline SSL Configuration Workflow

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

To use the Inline SSL Configuration Workflow:

1. Configure the Keychain Password (Figure 34)

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)			۹	C	A 🖱 (admin 👻	8
номе	Inline SSL Configuration: Keychain Password						Prev N	Next
	Keychain Password Password is net Setup	Keychain password is mandatory for inline 55L	Action Setup Krychein Pessword]		Keychain Pas Key Store Signing CA Trust Store Policy Profile Network Acce	sword	

Figure 34 Inline SSL Configuration Workflow: Keychain Password

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

🧐 GigaVUE-FM	10.115.94.11 (H Series)			۹	C		💾 admin 🗸 💡
номе	Inline SSL Keychain Passwo						Reset Submit Cancel
A Overview						L	
T Workflows	Keychain password is	nandatory for accessing the Key Store and adding Private Keys. Please setup your password.				O Key	chain Password
📥 Node Topology	Password		0			O Key	Store
TRAFFIC	Confirm Password					C Key	Store
Ports						O Signi	ing CA
`₩ Maps							
GigaSMART®						O Trus	t Store
Inline Bypass							
SYSTEM						O Polic	y Profile
Chassis						O Netv	vork Access

Figure 35 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
	Inline SSL Configuration: Key Store					Prev	Next
Overview Voerview Voerview	Inline SSL requires both private key and certificate. Select or add a new Key Pair. Key Pair Action Select a Key Pair. Add Key Pair Cenerate Certificate Cenerate Certificate)		Keyci Keysi Keysi Signi O Signi O Trust O Polici O Netw	hain Pas Store ng CA : Store y Profile vork Acc	ess	

Figure 36 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.

🞯 GigaVUE-FM				Q, C, 🌲 💾 admin-) 😯
	Key Pair			OK Cancel
	Key Pair Alias *	mitm_primary		Keychain Password
	Terre	- DEM D////11		6
	type	FEW O PROTE		O Key Store
🌢 Ports	Private Key	Copy and Paste 🔹 Install from URL 💿 Install from Local Directory		O Signing CA
	Path	scp://root@121.0.0.1/root/sslcert/self_signed/primaryRSA.key	0	O signing CA
		g. scp://username@121.0.0.1/path/filename		O Trust Store
	Password			
				O Policy Profile
Delay and lights	Certificate	Copy And Paste 💌 Install from UKL 🔘 Install from Local Directory		O Network Access
Carring		Same remote location as Private Key		
- Security	Path	scp://root@121.0.0.1/root/ssicert/self_signed/primaryRSA.crt	0	
		g. scp://username@121.0.0.1/path/liename		
	Password	***		
	Note: Private Key and	Certificate are both required for Inline SSL		
3	** •			»

Figure 37 Inline SSL Configuration Workflow: Updating the Key Store

- d. Click **Prev** from the top menu to install another key pair.
- 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 38 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	0.115.94.11 (H.Series) Q C	🜲 💾 admin 🗸 😯
номе	Signing CA	OK Cancel
🕈 Overview		
T Workflows	✓ Primary Root CA	Keychain Password
Node Topology TRAFFIC	Key Peir Alles mtm_primary	O Key Store
Ports	✓ Secondary Root CA	Signing CA
ዝና Maps 🗳 GigaSMARTΦ	Key Peir Alles mon_secondary -	O Trust Store
Inline Bypass SYSTEM		O Policy Profile
Chassis		O Network Access

Figure 39 Inline SSL Configuration Workflow: Configuring Signing CA

- 4. Update the Trust Store:
 - a. 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.
 - Download the Trust Store from the device navigation pane: GigaSMART > Inline SSL > Trust Store > Actions.
 - Append the missing certificate in the file.
 - Click Replace Trust Store and update the Trust Store.

🞯 GigaVUE-FM	HC2-Inline-SSL (H Series)	Q	G	4	💾 admin• 🥐
HOME	Trust Store				OK Cancel
Overview Workflows Mode Topology TRAFFIC Ports Maps GigaSMART® Inline Bypass	 Install from URL Install from URL Install from URL Install from Local Directory File Name 			 Keyo Key Sign Trus 	thain Password Store Ing CA st Store
Active Visibility SYSTEM Chassis				O Polic	cy Profile work Access

Figure 40 Inline SSL Configuration Workflow: Updating the Trust Store

- 5. Configure the Inline SSL profile
 - a. Click Create.



Figure 41 Inline SSL Configuration Workflow: Policy Profile

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





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
♠ Overview N Workflows ▲ Node Topology	Alles* inline_55s_sample_config	Keychain Password I
TRAFFIC	> Policy Configuration	O Key Store
Ports	Security Exceptions	 Signing CA
ዝ' Maps ይ GigaSMART®	✓ Whitelist/Blacklist	Trust Store
Inline Bypass	Whitelist 🛞	1
SYSTEM B Chassis A Roles and Users Support G Get Started About		O Policy Profile O Network Access
	Construction of the second se Second second sec	»»

Figure 43 Inline SSL Configuration Workflow: Configuring Whitelist/Blacklist in the Policy Profile

- d. 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	tions FM 10.115.94.11 (H Series)					۹	C		8	dmin - 🥐
HOME									0	OK Cancel
Cvervew Viorkflows Local Topology Tauric Ports Vi Maps GiguSMART® GiguSMART® Collection	V Policy Rules	Rule y boo, nets v confirmed spam sources	Vecrypt © No Decrypt V Vecrypt © No Decrypt V Vecrypt © No Decrypt Vecrypt © No Decrypt	×				 Keych Key S Key S Signin Signin Trust Trust Polic Netw 	nain Passw itore ng CA Store y Profile iork Access	vord s
 ▲ Roles and Users ✦ Health i Logs ♦ Settings 	x Rule 3 Catego Value X Rule 4	ny hacking	Vecrypt © No Decrypt	×						
O Get Started O About	X Rule 5 Value X Rule 5 Value Value X Rule 6	ry keyloggers_and_monitoring v @ f ry malware_sites v @ f	v Oecrypt © No Decrypt v	×						
*	Catego Value	ry phising_and_other_frauds	T	×				»		

Figure 44 Inline SSL Configuration Workflow: Configuring Policy Rules in the Policy Profile

e. 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.
- f. Click **OK** from the top menu to configure the inline SSL profile.

🚳 GigaVUE-FM	HC2-Inline-SSL (H Series)				ର ୯	📌 💾 admin• 📀
номе	Inline SSL Profile: inline					OK Cancel
Cverview Variations Anode Topology TRAFFIC Ports Vaps GassMART® Inline Sypass Active Visibility	(4) p	SMTP 465 LDAP 636 NNTP 563 HTTP 443	25 389 119 80	9		 Keychain Password Key Store Signing CA Trust Store Policy Profile
Chassis	✓ TCP Timeout					O Network Access
Roles and Users	TCP Inactive Timeout (minutes) 5					
 Settings 	✓ Server Key Map					
SUPPORT Get Started About		Add Server Key Map Dele Server * Key Pair Alias *	192.168.200.246 \$2.example2.com	×		
*						»

Figure 45 Inline SSL Configuration Workflow: Configuring Key Map in the Policy Profile

- 6. Configure Network Access:
 - a. GigaSMART® module must have connectivity to the Internet for URL categorization and Certificate Revocation checks.

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

b. Click Configure Network Access.

oigaVUE-FM	10:115.94.11 (H Series)	ຊ	C	4 ⁹	Ë	admin 👻	8
номе	Inline SSL Configuration: Network Access					Prev	Next
🕈 Overview	Each GigaSMART card requires IP address configuration for network access.			Keycł	hain Pas	sword	
Node topology TRAFFIC Ports Maps GigasMART® Inline Bypass SYSTEM Distance Chassis	Action Configer Network Access			 Ney S Signir Signir Trust Policy Netw 	tore ng CA Store y Profile vork Ac i	cess	

Figure 46 Inline SSL Configuration Workflow: Network Access step

c. Enable DHCP or manually configure the IP address.

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



Figure 47 Inline SSL 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 gateway to make sure that the connectivity exists.

🮯 GigaVUE-FM	10.115.94.11 (H Series)				Q	C	4 ⁰	Ш	admin 👻	?
номе	Ports Port Groups Tunnel Ports P	Port Pairs Tool Mirrors	Stack Links X	Port: 1/5/e1					Ed	dit.
A Overview	All Ports Ports Discovery Statistics			✓ Port Info						
🏷 Workflows 🚠 Node Topology	Ports			Status up	I.					
TRAFFIC				Hardware Address 00:	:1d:ac:18:0d:17					
Ports	Filtered By : None			IP Address 10.	115.94.30					
`₩ Maps	Port Id Alias	Туре	Speed	Netmask 25	5 255 248 0					
🗳 GigaSMART®	1/2/x6	18		Gateway 10.	.115.88.1					
🍄 Inline Bypass	1/2x7	N		DNS IP 10.	.10.1.20					
SYSTEM	1/2/x8	N		MTU 15	00					
Chassis	1/2/x9	N		DHCP En	abled					
Roles and Users	1/2/x10	N	<<							- 1
	1/2/x11	10		✓ Ping Test						
Get Started	1/2/x12	N		IP Address / Host 10.115.88.1 Ping Clear	-					
About	1/2/x13	N		Ding Paculie						
	1/2/x14	N								
	1/2/x15	8		PTNS 10.115.88.1 (10.115.88.1) from 10.115.94.30 mgwt0.12: 56(84)) bytes of da	ta.				^
	1/2/x16	8		64 bytes from 10.115.88.1: icmp_soq=1 ttl=255 time=0.130 ms 64 bytes from 10.115.88.1: icmp_soq=2 ttl=255 time=0.268 ms						
685868	1/5/e1	8		64 bytes from 10.115.88.1: 1cmp_seq=3 ttl=255 time=0.258 ms 64 bytes from 10.115.88.1: 1cmp_seq=4 ttl=255 time=0.258 ms 54 bytes from 10.115.88.1: 1cmp_seq=5 ttl=255 time=0.244 ms						
			Showing 31, 42 of 42							•

Figure 48 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 the Inline SSL Map Workflow

Inline SSL 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 Inline SSL 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 49 Inline SSL Map Workflow: Flow B

To use the Inline SSL Map Workflow:

1. Configure Inline Networks:

The use cases in this configuration guide require creating inline network group with two inline network links.

a. Click Create Inline Network Group.

🞯 GigaVUE-FM		Q	C		в	admin -	0
	Inline SSL Map: Inline Network(s)					Prev	Next
Overview Workflows Mode Topponer	Select an Inline Network or Inline Network Group.			O Inli	ne Net	work(s)	
TRAFFIC Ports Waps GigaSMARTS Inline Bypass & Active Visibility	Inline Network(s) Action Select a Inline Network Port or Inline Net Create Inline Net Create Inline Net	n Network twork Group		O Inlin O GS O Virt	ne Tool(Group ual Port Operati	s) : on	
	Figure 50 Inline SSL Map Workflow: Inline Net	etwork					

b. Provide details as illustrated below and Click OK.

🞯 GigaVUE-FM					۹	G		В	admin •	0
HOME Overview	Inline Network Group	ING-Core							ок с	lancel
► Workflows ▲ Node Topology	Inline Network Group Info						O Inlin	ne Netv	vork(s)	
TRAFFIC	Allas	ING-Core					O Inlin	e Tool(s	5)	
Ports	Comment	Comment.				_	O GS C	Group		
GigaSMART®	Inline Network Links						O Virtu	ual Port		
as Active Visibility	Inline Network	detaut_intre_net_1,3,3 *	tefault_inline_net_1,3,4 *	1			O GS C	Operatio	on	

Figure 51 Inline SSL Map Workflow: Creating inline network group

- 2. Configure Inline Tool
 - a. Click Create Inline Tool.

🞯 GigaVUE-FM	HC2.Htire-SSL(H Series)	Q	C	_ 	8	admin -	0
	Inline SSL Map: Inline Tool(s)					Prev	Next
A Overview							
Workflows	Select an Inline Tool or Inline Tool Group or Inline Tool Serial.			O Inlin	e Netw	ork(s)	
	Inline Tool(s) Action			I O Inlin	e Tool	(5)	
TRAFFIC	Select a destination port			1			
Maps				O GS C	roup		
GigaSMART®	Create Inline Tool Group				al Port		
Inline Bypass	Create Inline Tool Serial						
es Active Visibility				OGSO	perati	on	

Figure 52 Inline SSL Map Workflow: Creating inline tool

b. Click **Port Editor** and create inline tool ports.

🙆 GigaVUE-FM	HC2-Inline-SSL (H Series)					Q	C	A ²	H .	dmin 👻	0
номе	Inline Tool		×						C	ж сі	lose
A Overview			1/1	1/x17	port allas	In	line Networ	< 💌	9	Enable	
Workflows	Inline Tool Info		1/1	1/x18	port alias	In	line Networ	. •		Enable	
	Alias Alias		1/1	1/x19	portalias	In	line Networi	< -	V	Enable	
Ports	Comment com	popt	1/1	1/x20	port alias	In	line Networ	< -	V	Enable	
🍸 Maps	comment	hent	1/1	1/x21	port alias	In	line Networ	< -		Enable	
GigaSMART®	Ports		1/1	1/x22	port alias	In	line Networ			Enable	
 Active Visibility 	er Port B	ditor	1/1	1/x23	port alias	In	line Networ	. •		Enable	
SYSTEM	Port A Select	inline tool ports.	1/1	1/x24	port alias	In	line Networ	< •		Enable	
L Chassis			1/2	2/x1	port alias	N	etwork	-	12	Enable	
Roles and Users Health	Port B Select	Inline tool ports.	1/2	2/x2	port alias	N	etwork	•	E	Enable	
I≣ Logs	Configuration		1/2	2/x3	port alias	In	line Tool	•	V	Enable	
Settings	Enabled 🗵		1/2	2/x4	port alias	In	line Tool	•	Ø	Enable	
SUPPORT	Failover action Tool	Bypass -	1/2	2/x5	port alias	In	line Tool	-	V	Enable	
About			1/2	2/e1	NA	gigas	mart		N	A	
	Recovery Mode autor	matic -			Showing 1 - 30 of 83	14. 44	1 2 3	₩ Н			

Figure 53 Inline SSL Map Workflow: Creating inline tool ports

c. Configure the inline tool as illustrated below.

🙆 GigaVUE-FM	HC2-Inline-SSL (H Series)	Q C	🕂 💾 🖓 admin 🗸 😯
HOME	Inline Tool Cisco-ASA-IPS		OK Cancel
Overview Workflower			
A Node Topology	Inline Tool Info		Inline Network(s)
TRAFFIC	Alies	Cisco-ASA-IPS	O Inline Tool(s)
Ports	Comment	comment .	O GS Group
GigaSMART®	Ports		O Virtual Port
 Inline Bypass Active Visibility 		PortEditor	O GS Operation
DYSTEM	Port A	11/2/x3 •	O Inline Rule Based Map
Roles and Users	Port B	12/x4 ·	O Inline First Level Map
E Logs	Configuration		O Inline Second Level Map
 Settings 	Enabled	×	O Collector Map (bypass)
Ger Started	Failover action	Tool Bypass.	
O About	Recovery Mode	automatic -	
	Inline tool sharing mode	C Enable (Additional tags on the tool side)	
Murfur	Flex Traffic Path	Select flex traffic path . *	
	Heartbeats		
0	Enable Regular Heartbeat	Ø.	»

Figure 54 Inline SSL Map Workflow: Configuring inline tool

- 3. Configure the GigaSMART Group:
 - a. Click Create.
 - b. Provide details as illustrated below and click **OK** from the top menu.

🞯 GigaVUE-FM		Q C 📌 💾 etmin= 🕄
	GigaSMART Group	OK Cancel
 Overview Workflows Node Tappingv 	← GigeSMART Group info	Inline Network(s)
Taking Ports	Allas 0555 Port Lite	Inline Tool(s) O GS Group
S Ggissmants	GigaSMART Parameters Security Buffer	O Virtual Port
STITER E Chases Ables and Users Settings	Enable Resource Packet Buffer 💿 Enable Resource CPU 💿 ASF (Application Session Filtering) 💿	GS Operation Inline Rule Based Map Inline First Level Map
Surport O'CersStarted O'About	✓ Dedup Action © Count ® Drop IP Toless ® Include © Ignore IP TOS ® Include © Ignore TCP Sequence ® Include © Ignore VLAN © Include ® Ignore Timer (ps)	O Inline Second Level Map O Collector Map (bypass)
		»

Figure 55 Inline SSL Map workflow: Creating new GigaSMART Group

- 4. Configure Virtual Port:
 - a. Select Create.
 - b. Enter an alias name and click **OK** from the top menu.

🥝 GigaVUE-FM 🛛 10	1.115.94.11 (H (enes)			Q	C 📢	💾 admin• ?
HOME						OK Cancel
HOSE A Corenteev To Autoritions A Noort Topology TOLERE A Parts A Raine A Raine Rypeas Strates A Raine and Unless A Raine and A Raine and A Raine A Rai	VITUAI PORTS Alies GigesMART Group Mode Infine Failover Action None: Default fail	vp50 OSG5 GTP Overlap Virtual port bypass over accien for vport is Virtual port bypass.	a de la constante de la consta		 Iniin Iniin GS C O Virtu GS C Iniin Iniin Iniin Colle 	ok Caroli e Network(s) e Tool(s) iroup ual Port)peration e Rule Based Map e First Level Map e Second Level Map escord Level Map

Figure 56 Inline SSL Map workflow: Creating new Virtual Port

- 5. 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				Q	с 🍂	Hadman ?
	GigaSMART Ope					OK Cancel
Cherview Vointloop Lood: Topology	Alia GigsSMART Groups GigsSMART Operations (630P)	out-tail 6565 Select one or more CSOP type(b) . Initiae 554. Lettine_SSA_sample_config	* * *		 Inline Inline GS G Virtu GS O Inline Inline Inline Inline Colle 	e Network(s) e Tool(s) al Port peration e Rule Based Map e First Level Map e Second Level Map ctor Map (bypass)

Figure 57 Inline SSL Map workflow: Creating GigaSMART Operation

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

Now Map Or Correl Now Map Now Map Info Now Map Info Search Now Map Info Search Search Search Now Map Info Search Search Search	🙆 GigaVUE-FM	10.11554-11 (classes)	Q C 📌 💾 🕬 0
A Concore • Mag bride	wang (New Map	OK Cancer
A Note Storage if eight is gera (TD P) (1) is intermediate the storagera (TD P) (1) is intermediate the storage is gera (TD P)	 Overview Viork/tows 	₩ Map info	 Inline Network(s)
* Map Source and Destination Maine Suid Based Map Inline Rule Based Map Inline Rule Based Map Inline Stratud Inline Stratu	A Nores Topology Tolarsic A Insets W Maps Colgesmante P Milline Bypaso	Map Alter parts_11772 /k (. 1, 1) Consense ************************************	Inline Tool(s) Inline Tool(s) G G Group Virtual Port G G Operation
4 finite det doors Initial d	T Cunton	← Map Source and Destination	O Jolion Rule Recod Man
V Map Rules V Map Rules	Roles and Lovers Genergy Loverset Control Con	Port Bitor	Inline First Level Map O Inline Second Level Map O Collector Map (bypass)
Gass Base: mpm: Add a Rule x But 1 Conduct same. * Fass Stopp Withdecional Rule Commit: * Pressi * Mulve: TOP 0 * Mulve: TOP * 6 Mulve: TOP * 6 Mulve: TOP * 6		▼ Map Rules	
Max 000 Max 000 5535		Ourin Status Import Add a Rule w.Rule 1 Conducts starts	
	á l	Nev 10 Max 0 to 15535	>>

Figure 58 Inline SSL Map workflow: Creating Classic Inline Map

- 7. Configure the Inline First Level Map:
 - a. Provide details as illustrated below and click **OK**.

GigaVUE-FM		Q C 📌 💾 admini 😯
	New Map	QK Cancel
	✓ Map Info	Inline Network(s)
	Map Allas parae, non-HTTP_UH_1,1_3 Comments Type Inline Proc Level Subtype Ingress to Virtual Port	Inline Tool(s) GS Group
	← Map Source and Destination	GS Operation
Schrol E Chasses Roles and Users Semings Suprom Suprom	Port Editor Secure Descination GigsSMART Operations (050P) Home	 Inline Rule Based Map Inline First Level Map Inline Second Level Map
	✓ Map Rules	O Collector Map (bypass)
	Quick Editor Import Add a Rule. x Rule 1 Condition search * # Pass. © Drop B idnectional Rule Comment Control = 1 #	»

Figure 59 Inline SSL Map workflow: Creating Inline First Level Map

- 8. Configure the Inline Second Level Map:
 - a. Enter an alias name and click **OK**.

🞯 GigaVUE-FM	10.115.94 11 (risenes)	Q C 🥀 💾 🔤 🛛
HONE	New Map	OK Cancel
Overview Norkflows A Norkflows	✓ Map Info	 Inline Network(s)
TAUTIC A Parts Y Maps S OperAnatte A Inter Expans Sector A Inter and Units S Sectory United Units Cases Sectory United Operations Sectory United D Sectory United D Sectory Units Sectory Units Sectory Units Sectory	Map Allas Inspect SSL_IN_1_1_1 Comments Inspect SSL_IN_1_1_1 Type Inspect SSL_IN_1_1_1 Subtype Egress From Virtual Port	 Inline Tool(s) GS Group Virtual Port
	✓ Map Source and Destination	GS Operation
	Por Editor Source Destination GigsSMART Operations (ISSOP Out inst (ISSOS)	 Inline Rule Based Map Inline First Level Map Inline Second Level Map
1	✓ Map Rules	O Collector Map (bypass)
	Quark Liston import i Add a Bule ✓ Map Order Priority	
4	🗸 🗸 Map Permissions	»

Figure 60 Inline SSL Map workflow: Creating Inline Second Level Map

- 9. 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 Series)	Q C 🥂 💾 admin- 😯
HOME	New Map	OK Canol
Overview St. Workflows A Note: Involver	✓ Map Info	 Inline Network(s)
TRAFFIC PTOTES W Maps GogostMARTE Printine Bypess Security	Mep Alles bypes,res.(h,1,1,1) Commence Type inime • Subtype Collector. • Traffic Pach byPass. •	 Inline Tool(s) GS Group Virtual Port GS Operation
Chessis	✓ Map Source and Destination	Inline Rule Based Map
Ables and Upers Settings Uperset Get Saturat Adout	Port Editor Source Destination Select ports GigsSMART Operations (GSOP)	 Inline First Level Map Inline Second Level Map Collector Map (bypass)
	✓ Map Rules	
	Quick Editor Import Add a Rude	
	<c priority="" t<="" th=""><th>»</th></c>	»

Figure 61 Inline SSL Map workflow: Creating the Shared Collector Map

c. Review the maps created by the workflow.

🞯 GigaVUE-FM									۹	C 🚺	· 8	admin +	0
	1	idaps Map Templates	Filter Templates									1	
	N	Maps							New Clone	Edil Deleti	E Delete A	-	4
	D	Allas	Comments	Type	Subtype	Priority	Number of rules	Source	Destination	GSOP		Access Level	Contains
 Ports W. Inters 		parse_HTTP_IN_1_1_1		Inline	byRule	.1	.1	etault_inline_net	imperva101			admin	
	12	bypass_rest_IN_1_1_1		inline	collector(ByPass)		0	default_inline_net				admin	
		parse_non-HTTP_IN_1_1_1		inlineFirstLevel	ingressToVp	2	(i	default_inline_net	Vp50			admin	
Sectors III Chasses	8	Inspect_SSL_IN_1_1_1		inline5econdLevel	egressFromVp	1	0	🖬 vp50	Impervation	out-tist		admin	

Figure 62 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 be intercepted by 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** by deselecting the "**Physical Bypass**" check box 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 ethernet link-up event, there may be a slight glitch in the traffic flow.

🙆 GigaVUE-FM	10.115.94.11 (H Server)					Q	С	1	н	admin •	
HONE	Inline Network default_i	nline_net_1_1_1								OK Cance	6
Overview Workflows	Inline Network Info										
TRAFFIC	Alias Comment	default_inline_net_1_1_1 Comment									
W Maps	Ports										
Inline Dypess		PortEditor									
WITH Chasse	Port A Port B	10007 101007	•								
 Seconds 	Configuration										
support	Traffic Path	To Inline Tool									
About	Link Failure Propagation Physical Bypass										
	Redundancy Profile		٠								

Figure 63 Updating Inline Network

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

Deploying APF

To deploy APF:

- 1. Configure a GigaSMART group using the spare GigaSMART® module:
 - a. Go to the device navigation pane: Traffic > GigaSMART > GigaSMART Groups > New.
 - b. Provide details as illustrated below and click **OK**.

🥹 GigaVUE-FM	10.115.94.11 (H Series)					Q	C	Ш	admin 🗸	?
HOME	GigaSMART Group								ОК	Cancel
A Overview										
🎀 Workflows	✓ GigaSMART Group Info									
📥 Node Topology										
TRAFFIC	Alias	G5G 2								
Ports	Port List	E 1/2/01 ·	-							
₩ Maps										
💋 GigaSMART®	 GigaSMART Parameters 									
Inline Bypass										

Figure 64 Configuring GigaSMART Group

- 2. Configure a virtual port in the above GigaSMART group.
 - a. Go to the device navigation pane: Traffic > GigaSMART > Virtual Ports > New.
 - b. Provide details as illustrated below and click **OK**.

GigaVUE-FM Solutions FM 10.115.94.11 (H Series)			۹	С	1	Н	admin 🕶	0
HOME Virtual Ports							OK	Cancel
A Overview								
™ Workflows Allas ▲ Node Topology Allas	vp20							
GigaSMART Group	GSG2	Ŧ						
Mode Mode	GTP Overlap							
ገበ Maps Inline Failover Action	Virtual port bypass							
GigaSMART® Note: Default fail	over action for vport is Virtual port bypass.							
🚱 Inline Bypass								
@ Active Visibility								

Figure 65 Configuring Virtual Port

- 3. Configure a Hybrid port.
 - a. Go to the device navigation pane: Traffic > Ports.
- 4. Select the port that must be configured as a hybrid port.
 - a. Click Edit from the Ports menu.
 - b. Provide details as illustrated below and click **OK**.

🞯 GigaVUE-FM		۹	G	*	ВI	admin • 😯
	Ports : 1/1/x9					OK Cancel
	Allas Comment					
🖨 Ports	▼ Parameters					
	Admin @ Enable Type Itons • Speed Securit Special • Duplex © Full © staff Auto Negotistics © Enable Force Link Up © Enable					
	> Alarms					
	➤ Filters					
	> Permissions					

Figure 66 Configuring hybrid port

- 5. Configure the out-of-band map with the above hybrid port as the destination
 - a. Go to the device navigation pane: Traffic > Maps.
 - b. Click New from the Maps menu.
 - c. Provide details as illustrated below and click **OK**.

🞯 GigaVUE-FM	10 115 94 11 (H Series)	Q	C	*	🗄 admin 🔹 😯
HDME	New Map				OK Cancel
Node Topology	✓ Map Info				
ttaatiiC ▲ Pures ¥ Mage ⊈ GigaSMART® I Intine Bypass	Map Allas OOII, map 1N, 1, 1, 1 Comments Type Infine Sectord used Subtype Egmis OOB from Vertual Post: +				
V Intine Bypass	✓ Map Source and Destination				
Trystea Chassis A Roles and Users Settings Current G Ges started Adoptr	Port Editor Source 2005 Destination 1000 GigsSMART Operations (650P)				
	> Map Rules				
	> Map Order				
	Map Permissions				

Figure 67 Configuring out-of-band map

- 6. Configure the APF GigaSMART Operation.
 - a. Go to the device navigation pane: Traffic > GigaSMART > GigaSMART Operations (GSOP) > New.
 - b. Provide details as illustrated below and click **OK**.

🚳 GigaVUE-FM Solu							Q	C	A	Ш	admin •	0
HOME											OK Ca	ancel
A Overview												
N Workflows ▲ Node Topology	Alias	mask_data										
TRAFFIC	GigaSMART Group	GSG2		•								
A Ports	GigaSMART Operations (GSOP)											
W Maps		APF (Adaptive Packet Filtering)			×							
 Inline Bypass 		Enabled	8									
Active Visibility												

Figure 68 Configuring APF GigaSMART Operation

- 7. Configure rule-based First Level map with the above hybrid port and the virtual port as **Source** and **Destination** respectively for filtering-in TCP traffic.
 - a. Go to the device navigation pane: Traffic > Maps.
 - b. Click New from the Maps menu.
 - c. Provide details as illustrated below and click **OK**.

🙆 GigaVUE-FM Solu	tions FM 10.115.94.11 (H Series)		Q	C	1	B	admin 🗸 🚺	
номе							OK Cancel	
🕈 Overview 🏷 Workflows	✔ Map Info							I
📥 Node Topology	Map Alias	oob_filter_ttp						l
TRAFFIC	Comments							I
ዝՐ Maps	Enable	×						ı
🗯 GigaSMART®	Туре	First Level Y						I
Inline Bypass Active Visibility	Subtype	By Rule *						ı
CVETEM	Traffic Type	Control						
Chassis	✓ Map Source and Destination							
2 Roles and Users		Port Editor						1
♣ Health ≔ Loss	Source	🛄 1/1/z10 🗸 –						I
Settings	Destination							I
SUPPORT	CI-STAND OF STAND							ı
Get Started	Gigasmaki Operations (GSOP)	None						J.
About	✓ Map Rules							4
		Quick Editor Import Add a Rule						ı
	× Rule 1	Condition search • ® Pass © Drop 🔲 Bi-directional						ı
	Rule Comment	Comment						П
		Protocol X						
*		Value TCP • 6						•

Figure 69 Configuring rule-based first-level map for filtering in intended traffic for masking.

- Configure regular shared collector map with the hybrid port and the tool port connected to the out-ofband tool as **Source** and **Destination** respectively for filtering-in traffic that does not match the APF rules.
 - a. Go to the device navigation pane: Traffic > Maps.
 - b. Click **New** from the Maps menu.
 - c. Enter the details as illustrated below and click OK.

🞯 GigaVUE-FM Solu	Itions FM 10.115.94.11 (H Series)		Q	C	4 ⁹	Ë	admin 🔹 😯
							OK Cancel
Norkflows	✓ Map Info						
	Map Alias	oob_map_scol					
🛋 Ports	Comments						
	Enable	8					
	Туре	Regular T					
	Subtype	Collector					
							_
	 Map Source and Destination 						
Roles and Users		Port Editor					
	Source	111/1/10 ⁻					
	Destination						
	Destination						
	GigaSMART Operations (GSOP)	None *					
	✓ Map Rules						
6 About		Aviel Editor Imager Add a Dula					
	M Max Order	Quartentor Import Paulo nue					
	✓ Map Order						
	I						*

Figure 70 Configuring regular shared collector map.

9. Configure rule-based Second Level map with the virtual port and the tool port connected to the out-ofband tool as Source and Destination respectively for masking data based on pattern matching as illustrated below to the nonvolatile memory.

- a. Go to the device navigation pane: **Traffic > Maps**.
- b. Click **New** from the **Maps** menu.
- c. Enter the details as illustrated below and click **OK**.

💿 GigaVUE-FM							Q	C	8	fmin •	0
	Edit Map: mask-pli								0	K Can	cel
Overview	✓ Map Info										
Node Topology	Map Alias	mask pi		0							
	Comments										
Ports	Enable										-
GigaSMART®	Туре	Second Level									
Inline Bypass	Subtype	By Rule 👻									
	✓ Map Source and Destination										
NITTER TO CONTRACT		Port Editor									
 Roles and Users Health 	Source										
🗐 Logs 🌢 Settings	Destination										
	GigaSMART Operations (GSOP)	mask_data(GSG2)	x x								
 Get Started About 	✓ Map Rules										
	× Rule 1	Add a Bule									
	Rade Comment.	Connect Patern Math Top (resp.) Programmeruguad-Subject 46 is 1518 Patern Mach Hitt, Hitt Patern Mach Hitt, Hitt Mach Jah From To									

Figure 71 Configure rule-based second level map for applying APF GigaSMART operation (GSOP).

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 the 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**.

Ports Port Gro	ups mannerports	run ralls	rou wirrurs Statik U	185 1				Filter		
All Ports Ports	Discovery Statistics						_	1		
Ports								Box ID/Slot ID		
Filtered By : Port Type	Total Filtered Ports	11 Clear,Filter						Port Alles Type Port Alles		
D Port Id	Allas	Type	Speed	Admin	Link Status	Transceiver Type	AV	Port ID		
1/1/105			1G	Enabled	up	sfp cu	07	C Type port #		
I/1/1/86			1G	Enabled	up	sfp cu	07	СТуре		
🗐 🕐 1/1/x10	OO8_tool_port	0	16	Enabled	up.	sfp cu	07	Toul * inine Network * Inin	# Tool #	
1/1/x17		80	10G	Enabled	up	bps sx/sr	0/	Admin Status		
🔲 🔹 1/1/x18		63	105	Enabled	up	bps sw/sr	0/	(● All	.d © Disabi	led
1/1/x19				Disabled	+	bps sa/sr	07	Link Status	© Down	e:
1/1/x20		8		Disabled		bps sx/sr	07	Speed		
💷 🔹 1/1/x21		63		Disabled	4	bps sx/sr	0/	Select Part Speciel 👻		
1/1/k22		8		Disabled	-	bps sa/sr	07	Transceiver Type		
- A10023		m		Dicabled		hnt cylor	0/			

Figure 72 Viewing Ports status

Verifying Inline Network Status

To verify Inline Network status:

- 1. Go to the 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						Q (2 🔺	admin -	8
HOME	Inline Networks Inline Network Groups	Inline Tools Inline Tool Grou	ps inline Seri	al Tools Heartbeats Red	lundancies				
A Overview	Inline Networks						New	Clone Edit	Delete
A Node Topology	Alias	Comment	Туре	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	
GigaSMART0	default_inline_net_1_1_3		protected	physicalBypass	true	enabled		Bypass	
Finline Bypass	default_Inline_net_1_1_4		protected	physicalBypass	true	enabled		Bypass	
				Total Items : 4					

Figure 73 Viewing Inline Network status

3. Inline tool status:

- a. Go to the device navigation pane: Traffic > Inline Bypass > Inline Tools.
- b. Select Inline Tools and verify that the inline tool has the following status:
 - Inline Tool Health Status: Green
 - Inline Tool Status: Enabled
 - Combined Heartbeat Status: Up
 - Heartbeat Profile 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)								Q	C		Ë	admin 🕶	0
номе	Inline Networks Inli	ine Network Groups	Inline Tools	inline Tool Groups Inline Seri	al Tools Heartbeats	Redundancies								
A Overview	Inline Tools									New	Clone	Recover	Edit	Delete
A Node Topology	Alias	Comment	Operational State	Inline Tool Status	FailoverAction	Combined Heartbeat Status	ſ	Heartbeat	Profile		Negative He	sartbeat Pro	rile	
	🔲 🗨 impervat01		up	enabled	Tool Bypass	up		🗨 defaul	t					
₩ Ports	Health Stat	us			Total Items :	1		Hea	alth Sta	tus				
GigaSMART®														
Inline Bypass														

Figure 74 Viewing Inline Tool status

Verifying Map Status

To verify map status:

- 1. Go to the 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.

🎯 GigaVUE-FM								(۹	C		Ë	admin +	8
HOME	Maps Map Templates	Filter Templates												
A Overview	Maps Map Groups Sta	atistics												
🔁 Node Topology	Maps							New Clo	one	Edit	Delete	Delete All	=	÷
TRAFFIC														
Ports													+	Columns
ገኛ Maps	Alas	Comments	Type	Subtype	Priority	Number of rules	Source	Destination		GSO		A	ccess Level	
5 GIgaSMART®	oparse_HTTP_IN_1_1_1		inline	byRule	1	1	iN++ default_inline_ne	imperv	va101			ad	min	^
🖗 Inline Bypass	bypass_rest_IN_1_1_1		inline	collector(ByPass)		0	IN•• default_inline_ne					ad	min	
SYSTEM	parse_non-HTTP_IN_1_1_1		InlineFirstLevel	IngressToVp	2	1	ine_ne	V vp50				ad	min	
Roles and Users	imspect_SSL_IN_1_1_1		inlineSecondLevel	egressFromVp	1	0	V vp50	iT •• imperv	va101	out-is:	il.	ad	min	
Settings	Health Status													

Figure 75 Viewing Maps status

Verifying Port Statistics

To verify port statistics:

- 1. Go to the device navigation pane: Traffic > Ports > Filter.
- 2. Filter in inline network, inline tool, tool and/or hybrid ports (if any), and verify that the ports are receiving traffic.

🥘 GigaVUE-FM	10 115 9	4 11 (H Series)												Q	C I	L H	admin +	0
HOME	Por	rts Port Groups	Tunnel Po	irts Por	t Pairs	Tool Mirrors	Stack L	links					×	Filter				Clear
A Overview	All	Ports Ports Disc	overy Sta	distics														
🏷 Workflows 👍 Node Topology	St	atistics												Box ID/Slot ID Select a Box/Sic	cID	•		
TRAFFIC	.0	Port ID	00	tets	Octer	s /sec	Unicast	Packets	Non-Unio	ast Packets	Packe	its /sec	Packet Drops	Port Alias				
Ports			Rx	Tx	Rx	Tx	Rx	Ťĸ	Rx	Tx	Rx	Тх	Rx	Type Port Alias				
₩ Maps	5	🛛 🚺 1/1/x5	188.63 M	9.96 M	63	63	148.03 K	54,46 K	88 79 K	88 79 K	1	1	0	Port ID				
9 GigaSMARTE	.0	0 1/1/06	9.96 M	188.63 M	63	63	54,46 K	148.03 K	88.79 K	88.79 K	£.	1	0	Dune				
 Initia Evolusis 	0	🛛 🚺 1/1/x10	0	0	0	o	0	0	0	0	0	σ	o	Inine Network	Inine Tool > 1	501 -		
SYSTEM		• 🔯 1/17x17	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					
🔟 Chassis	0	1/1/x18	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	() Factoria	0.5144		
Roles and Users	0	• 🔣 1/1/x19	0	, U	0	0	0	0	0	.0	0	0	0		 Enabled 	O DISAL	ieu	
• Settings	0	1/1/2/20	0	٥	D	0	0	0	ò	a	0	0	0	Link Status (e) All	Θ υρ	© Down		
surron)	0	1/1/x21	0	0	0	0	0	0	0	0	0	0	0					
Get Started	10	1/1/x22	0	0	0	.0	0	0	0	0	0	.0	0	1				
O About	0	● 1/1/x23	0	0	0	0	0	0	0	0	0	0	0					
		1/1/x24	0	O	D	o	0	0	0	c.	0	0	0	1				

Figure 76 Viewing Ports statistics

Verifying Map Statistics

To verify map statistics:

1. Verify stats reported from the 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	В	admin +	8
номе	Maps	Map Templates Filter Templates						
A Overview	Maps	Map Groups Statistics						
🔥 Workflows	Statis	stics						Clear
TRAFFIC								
Ports	•	↑ Map Alias	Total Counters			Rules		
ነሆ Maps	•	bypass rest IN 1 1 1	27K Packets, 4.19M Bytes			-		
💋 GigaSMART®	•	parse HTTP IN 1.1.1	72K Packets, 90.97M Bytes			1		
🖗 Inline Bypass		parse non-HTTP IN 1_1_1	3.64M Packets, 2.48G Bytes			1		
SYSTEM			Total Items : 3					

Figure 77 Viewing Map statistics

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

oigaVUE-FM	10.115 94 11 (H Series)			Q	с 🔺	💾 admin 🗸 💡
номе	Maps Map Templates Filter	Templates	Map: parse_HTTP_IN_1_1_1			Edit
A Overview	Maps Map Groups Statistics					Hour Day Week Month
🕅 Workflows	Statistics					(Use Mouse Scroll for Zoom In/Out)
TRAFFIC			9-			
Ports	Map Allas		8-			
ነዠ Maps	bypass rest IN 1 1	L1	6-			
S GigaSMART®	Darse HTTP IN 1	ц	5- 2017-03-31 10:12			
🗭 Inline Bypass	parse non HTTP II	<u>N 1 1 1</u>	4- Data Rate (Bit/s) 0			
SYSTEM			Packets (pps) 0			
III Chassis			1-			
🚨 Roles and Users			< <p></p>	31 10:32	2017-03-31 10:52	1 1 1
Settings				Data Rate (BIt/s) Packets (pps)		Time
SUPPORT			✓ Map Info	✓ Map Rules		
About			Comment	Pass Rules Rule 1		
			Type inline	Bi-directional	~	
			Sub Type byRule	in4Proto	6	
			Source education Source	ip in to co		
			Destination imperval01	portDst	80	
			GSOP			
			Priority 1			
	<<		✓ Map Permissions			

Figure 78 Viewing statistics for Classic Inline Map

Verifying GigaSMART Group Statistics

To verify GigaSMART group statistics:

1. Verify stats reported under the device navigation pane: **Traffic > GigaSMART > GigaSMART Groups > Statistics**.

🙆 GigaVUE-FM									Q	G	A 🖰	admin 🗸 😯
номе	GigaSMART Operations	(GSOP) Gig	ISMART Groups	Virtual Ports	NetFlow / IPFIX (Seneration In	line SSL Passive SSL	Application Session Filtering	GTP Whitelist			
A Overview	GigaSMART Groups	Statistics										
🏷 Workflows 🛦 Node Topology	Statistics											Clear Upload
7048710												
- Dorm	GS Group Allas	Rx Packets	Tx Packets	Rx Octets	Tx Octets	Packet Drops	Packets Received Errors	Heartbeat status of eport	Heartb	eat Rx Packets	Heartbe	at Tx Packets
W Mapr	GSG2	0	0	0	0	0	0	up	179076		179076	
GigaSMART®	GSG5	3725229	3705226	2537824870	2529036714	0	0	up	179076		179076	
🏠 Inline Bypass												

Figure 79 Viewing GigaSMART Group statistics

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

🮯 GigaVUE-FM										c	x C	🐥 E	admin -	0
номе	G	igaSMART Operations	(GSOP) Giga	SMART Groups	Virtual Ports	NetFlow / IPFIX G	er X	GS Group: GSG5						
A Overview	0	ilgaSMART Groups	Statistics											
☆ Workflows	S							✓ Aggregated 1/5/e1						
and reade reporting)									1 sec	1 min	5 min	10 min	15 min	
TRAFFIC		GS Group Allas	Rx Packets	Tx Packets	Rx Octets	Tx Octets	Packet E	CPU Useful Time	0	0	0	0	0	
Ports		GSG2	0	0	0	0	0	CPU Idle Time	1560	976	974	970	966	
۱۴ Maps	0	6565	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	D	0	
SYSTEM								Packet Drops	0	0	0	0	0	
III Chassis								Packets Receive Errors	0	0	0	0	0	
🚢 Roles and Users							~<							
Settings														



Verifying GigaSMART Operation Statistics

To verify GigaSMART operations statistics:

- 1. Verify stats reported under the device navigation pane: **Traffic > GigaSMART > GigaSMART > Operations (GSOP) > Statistics**.
- 2. Click the GigaSMART Operation alias name to view the historical statistics.

🞯 GigaVUE-FM	10.115.94.11 (H	l Series)								Q	G	🐥 E	admin 🗸	8
номе	GigaSMART	F Operations (GSOP)	GigaSMART Groups	Virtual Ports	NetFlow / IPFE	K Generation	Inline SSL	Passive SSL	Application Session Filterin	g GTP Whitelist				
A Overview	GigaSMAR	F Operation Stati	istics											
🏷 Warkflows 🚠 Nade Tapalogy	Statisti	ics												
TRAFFIC														
- Ports	GSOP Alias	GS Group Allas	Map Allas	Rx Packets	Tx Packets	Rt Octets	Tx Octets	Packet Drops	Packet Drops No Init	Packets Terminated	Packe	ts Parse Errors	GS Operation	ons
11 Mans	out-issi	GSG5	Inspect_SSLJN_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									Q	C	Ë	admin +	8
номе	GigaSMAR	Coperations (GSOP)	GigaSMART Groups	Virtual Ports	NetFlow / IPFl	X Ger X	GS Operation Statistics: o	ut-issl					
A Overview	GigaSMART	Coperation Stat	istics										
🏷 Workflows 👍 Nade Tapalogy	Statisti	ics			G5G5								
TRAFFIC	GSOP Alias	GS Group Alias	Map Alias	Rx Packets	Tx Packets	Rx Octets	Map Alias:	Inspect_SSL_IN_1_1_1					
Ports	out-Issl	G5G5	inspect_SSLUN_1_1_1	3.77 M	3.75 M	2.57 G	✓ General						
S GigaSMART®							Pkts Drop:	0					
Inline Bypass system							Pkts Rx:	3,767,936					
111 Chassis							Octets Rx:	2,565,436,726					
Roles and Users Settings							Pkts Term:	0					
SUPPORT							Octets Tx:	2,557,545,135					
 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 82 Viewing historical statistics of GigaSMART Group

Verifying Inline SSL Session Statistics

To verify Inline SSL session statistics:

1. Verify stats reported under the device navigation pane: **Traffic > GigaSMART > Inline SSL > Statistics**.

🥹 GigaVUE-FM	10.115.94.1												Q	С	1	Ш	admin 🕶	8
HOME	GigaSi	WART Opera	tions (GSOP)	GigaSMART Grou	ips V	irtual Ports	NetFl	ow / IPFIX Ge	×									Close
A Overview	SSL Pr	ofiles	Key Store	Signing CA Ti	rust Store	Global	Defaults	Network	Access									
☆ Workflows	Inlin									✓ Session Statistics								
🚠 Node Topology									_	Name	Total	Active						
TRAFFIC	✓ Sum	✓ Summary								Incompany Constants		17						- 1
Ports	Grasm	RT	65 Group	Intercented Sessio	ins (Active/T	inral)		SSI Sessions	(Active/T	Intercepted sessions	29	17						- 1
II Maps	Gauna		ab aloup	intercepted sease	no presion	-o-cony		Decrypted	Non-De	SSL Sessions	29	17						- 1
Inline Bypass	1/5/e1		6565	16/27				0/8	16/19	Decrypted	9	1						- 1
										Non-decrypted	20	16						
SYSTEM	✓ Sess	✓ Session Statistics								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	lorg		Policy Statistics								
SUPPORT	#2	1/5/e1	192.168.1.3	204.2.197.201	62316	443	cspix.med	dia6degrees.c	om	 Forcy statistics 								
• Get Started	#3	1/5/e1	192.168.1.3	63.241.103.45	62310	443	www.ansi.org			Network Connection Loss	0							
About	#4	1/5/e1	192.168.1.3	104.16.27.235	62294	443	m.addthis.com m.addthisedge.com			Decrypt	11							
dia dia	#5	1/5/e1	192.168.1.3	104.16.24.235	62295	443				No Decrypt	18							
	#6	1/5/e1	192.168.1.3	205.210.187.194	62303	443	p.rfihub.c	:om		Url Lookup	11							
	#0	1/5/e1	192.168.1.3	63.241.103.45	62312	443	www.ansi	Lorg		Url Un-caracterized								
	#9	1/5/e1	192.168.1.3	104 16 26 235	62305	443	suaddthis	s.com		on on categorized								
	#10	1/5/e1	192,168,1,3	63 241 103 45	62315	443	www.ansi	org		Uri Category Found	11							
(DKDKD	#11	1/5/e1	192.168.1.3	104.16.27.235	62293	443	m.addthis	s.com		Url Category Missing	0							
	#12<br </th <th>1/5/e1</th> <th>192,168.1.3</th> <th>104.16.16.35</th> <th>62298</th> <th>443</th> <th>s7.addthis</th> <th>s.com</th> <th>_</th> <th>Uri Category Match</th> <th>0</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	1/5/e1	192,168.1.3	104.16.16.35	62298	443	s7.addthis	s.com	_	Uri Category Match	0							

Figure 83 Viewing Inline SSL session summary

2. Click Show Details to view more details.

🎯 GigaVUE-FM							Keywords				Q	C	В	admin 🗸	8
номе	GigaSl	WART Operat	tions (GSOP)	GigaSMART G	Groups	Virtual P	orts NetFlow / IPFIX Ger	x	Session Det						Close
A Overview	SSL Pr	ofiles	Key Store	Signing CA	Trust Sto	re Gl	obal Defaults Network A	ccess							
Norkflows	Inlin								Counter Name	Network Server					
									Source IP	192.168.1.3					- 1
Ports	✓ Sum	imary							Destination IP	63.241.103.45					- 1
וו Maps	GigaSMA	GigaSMART GS Group SSL Sessions (Active/Total)					al)	N	Source Port	51554					- 1
GigaSMART®		Decrypted Non- Decrypted					d		Destination Port	443					- 1
🖗 Inline Bypass	No Inline	SSL Session	Summary.						Protocol	SSL outbound					- 1
SYSTEM	✓ Sess	ion Statisti	cs						TCP State	Na:EST ND:EST Ta:INIT TD:INIT					- 1
Roles and Users	Number	Interface	Src IP	Dst IP	Src Port	Dst Port	SNI		Decryption	NO					- 1
Settings	#1	1/5/e1	192.168.1.3	104.16.21.35	51558	443	s7.addthis.com		Error	NO_ERR					- 1
SUPPORT	#2	1/5/e1	192.168.1.3	216.58.194.200	51559	443	www.googletagmanager.com	n *.go	SSL State	SSL_BYPASS					- 1
Get Started	#3	1/5/e1	192.168.1.3	104.16.21.35	51557	443	s7.addthis.com	*.ad	C25 Status	EST					
About	#4	1/5/e1	192.168.1.3	216.58.194.196	51549	443	www.google.com		S2C Status	51					
	#5	1/5/e1	192.168.1.3	10.115.1.130	49396	40004			Tool Cranue	TOOL BYDASS					
	#6	1/5/e1	192.168.1.3	216.52.31.83	51587	443	cm.adgrx.com		Tool Status	1000_019/03					
	#7	1/5/01	192.168.1.3	03.241.103.45	51581	443	nivel advertising com	nixe	Policy Verdict	NO_DECRYPT					
	#9	1/5/e1	192.168.1.3	52,52,238,30	51574	443	idsync.weborama.fr	pixe	Policy Match Fields	DOMAIN					
() K D K D	#10	1/5/e1	192.168.1.3	63.241.103.45	51502	443	www.ansl.org		URL Category						
	#11	1/5/e1	192.168.1.3	216.58.194.205	51531	443	www.google-analytics.com	*.go	URL Filter Result						
	<< #12	1/5/e1	192.168.1.3	104.16.27.235	51560	443	m.addthisedge.com	*.ad	Interface Pair	Na/Nb					



Troubleshooting Guide

Generic Troubleshooting Steps

In the event of encountering any issues, it is recommended to bypass traffic at various levels in the Gigamon device (see below), and isolate the issue b/w the Gigamon device and the inline tools.

- 1. Bypass traffic at the inline SSL policy level by enabling decrypt tool-bypass, no-decrypt tool-bypass or non-ssl-tcp tool-bypass as required.
- 2. Bypass traffic at the GigaSMART® module by setting inline network(s) traffic-path to bypass.
- 3. Bypass the Gigamon device by enabling Physical Bypass on inline network(s).

If the issue were to be found with the Gigamon device, it is recommended to

- 1. Collect the Controller Card logs (optional; required for any chassis/module related issues).
- 2. Collect the GigaSMART® module logs by executing the following commands
 - a. file gs-fetch port < GigaSMART engine interface> file /var/log/messages
 - b. file debug-dump upload messages tftp://<ipAddress>/messages
- 3. Collect CLI response for the following
 - a. show diag detail
 - b. show apps inline-ssl session any
 - c. show apps inline-ssl stats detail

In addition to the above information, collect information about

- 1. Type of client (Desktop or Handheld device)
- 2. Version of the operating system and the browser used by clients
- 3. Screen captures of issues encountered at clients (including pcaps if necessary)
- 4. Type of application (browser hosted or app based)
- 5. Logs/reports/pcaps from application monitoring tools (required for analyzing response times) and other inline tools deployed for inspection

How To...

How to verify certificate chain

Verify Authority Key Identifier (AKI) and Subject Key Identifier (SKI) extensions in the given certificates as described below.

If a server certificate has two intermediate CAs, do the following:
- 1. AKI in a server certificate must match SKI in its issuer (that is first intermediate CA) certificate.
- 2. AKI in the first intermediate CA certificate must match SKI in the second intermediate CA certificate.
- 3. AKI in the second intermediate CA certificate must match SKI in the root CA certificate.

How to verify a server certificate that is installed on the Gigamon device

Verify that the Thumbprint (or Fingerprint) Property of the actual certificate matches with the certificate installed on the Gigamon device.

How to find that private key and certificate match

Use the following openssl commands to verify the md5 hash of the keypairs.

```
openssl x509 -noout -modulus -in certificate.crt | openssl md5
openssl rsa -noout -modulus -in privateKey.key | openssl md5
```

How to extract keypairs from pfx to PEM format

Use the following commands to extract private key and certificate from a certificate in pfx format.

```
openssl pkcs12 -in yourcert.pfx -nocerts -out privatekey.pem -nodes
openssl pkcs12 -in yourcert.pfx -nokeys -out publiccert.pem -nodes
```

How to remove passphrase from a RSA private key

Use the following openssl command to remove passphrase from a key (ex. prv_key.key).

openssl rsa -in prv key.key -out new key.key

Open the new_key.key using the following command; openssl must not prompt for entering the passphrase.

openssl rsa -text -in new key.key

How to flag Unknown CA or Invalid and Expired certificates while decrypting outbound SSL sessions

By default, the Primary Signing CA certificate will be used for re-signing all certificates. As a result, when a client browser is updated with the Primary Signing CA certificate, it shall not flag invalid or expired certificates, or certificates issued by an unknown CA. To re-sign such certificates with a different certificate, configure the Secondary Signing CA on the Gigamon device. It is not recommended to install Secondary Signing CA certificate in client browsers to enable them to flag such certificates.

How to change the SSL State from Bypass:no_config to Decrypting for outbound SSL sessions

SSL State for outbound SSL sessions is reported as Bypass:no_config when either the Primary Signing CA is not Configured or when the Keychain Password is locked. The Keychain Password is not stored on the Gigamon device. If the node reboots, the Keychain Password must be entered to unlock SSL functionality on the device.

How to ensure that outbound inline SSL sessions are decrypted with Certificate Revocation Check enabled

When certificate revocation check is enabled, the GigaSMART® module must have access to the Internet to verify certificates. By default, outbound SSL sessions will be decrypted if the certificate revocation check status is unknown.

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 gateway to make sure that the connectivity exists.

🮯 GigaVUE-FM	10.115.94.11 (H Series)					Q	C	4 °	Ш	admin +	8
HOME	Ports Port Group:	s Tunnel Ports	Porc Pairs Tool Mirrors	Stack Links X	Port: 1/5/e1						Edit
♠ Overview ☆ Workflows ▲ Node Topology	All Ports Ports Dis	scovery Statistics			♥ Port Info						
	Ports				Status u	ıp					
TRAFFIC					Hardware Address 0	0:1d:ac:18:0d:17					
Ports	Filtered By : None				IP Address 1	0.115.94.30					
Ήr Maps	Port Id	Alias	Туре	Speed	Netmask 255 255 248 0						
GigaSMART®	0 1/2/86				Gateway 1						
🍄 Inline Bypass	1/2h7		8		DNS IP 1						
SYSTEM	1/2/x8		N		MTU 1	500					
Chassis Released license	1/2/x9		N		DHCP E	nabled					
Koles and osers Settings	1/2/x10		N	<<							-1
	1/2/x11		N		✓ Ping Test						
Get Started	1/2/x12		N		IP Address / Host 10.115.88.1 Ping Clear						- 1
About	🗎 🔍 1/2/x13		N		Pior Peruite					- 1	
	1/2/x14		8		Fing resolut					- II	
	1/2/x15		8		PTNS 10.115.88.1 (10.115.88.1) from 10.115.94.30 mg#t0.12: 56(8	14) bytes of da	ta.				^
	1/2/x16		8		64 bytos from 10.115.88.1: icmp_soq=1 ttl=255 timc=0.100 ms 64 bytos from 10.115.88.1: icmp_soq=2 ttl=255 timc=0.200 ms						
			8		64 bytes from 10.115.88.1: 10Hp_seq=3 ttl=25 tlHe=0.253 Hb 64 bytes from 10.115.88.1: 10Hp_seq=4 ttl=255 tlHe=0.256 Hb 64 bytes from 10.115.88.1: 10Hp_seq=5 ttl=255 tlHe=0.244 Hb						
*	4			Showing 31, 42 of 42						•	* ×

GigaSMART engine interface Quick View window

How to verify if SSL sessions are bypassed because of performance or resource constraints

SSL sessions will be bypassed if performance limits are exceeded for Connections per Second or Concurrent sessions. Memory resource constraints may also force SSL sessions to be bypassed. Check with your Sales Engineer for the performance metrics. To find whether SSL sessions are bypassed because of the said issues, execute "show apps inline-ssl stats resource" hidden CLI command and check whether **Overload Nodecrypt** condition is enabled. An excerpt of the CLI resonse is provided below for reference.

The Gigamon device will automatically disable Overload No-decrypt as and when the performance falls back to the supported range or when the memory resource constraints are resolved.

HC2-Inline-SSL (config) # show apps inline-ssl stats resource

----- FPA/Heap/Buffers Info -----

Overload No-decrypt	=	= Disabled				
Concurrent connections	=	0	(max:0)			

TCP Proxy CPS = 0/26/10/2000 (ls/max/10ms burst/limit) = 0 % / 0 % (1s/5s)CPU usage Num SSL flow bypassed = 0 |-- Max CPS reached = 0|-- Max conn reached = 0 |-- FPA pool exhausted = 0 |-- Heap exhausted = 0 |-- Max CPU reached = 0

How to verify if the GigaSMART module has crashed

Execute "show apps inline-ssl stats crashinfo" hidden CLI command to check whether the GigaSMART module has crashed.

ISSL Monitor mode

ISSL Monitor mode is enabled from the inline-ssl app global settings. After the inline ssl configuration, if monitor mode is enabled, the inline ssl app does not the terminate the session. Instead monitor app collects the info and forwards the packets. The packets are forwarded to the tool or network port depending on non-ssl-tcp tool bypass configuration. For any Monitor mode enable/disable should be done seamlessly without any other configuration changes.

For the packets coming from the network port, the monitor app collects packet flow info. In the first version, monitor app collects the following information:

Monitor Summary:

- Total Incomplete TCP handshake: Have not seen all the TCP handshake messages, but the data packets are seen
- Total TCP established sessions: All handshake packets seen (SYN/SYN-ACK/ACK)
- Total Sessions with multiple vlan ids:
- All the outer VLAN IDs used in the network
- All inner VLAN IDs used in the network
- All the network interfaces the traffic is seen
- Duplication SYN counters
- Duplicate SYNACKs
- Totals SYN/SYNACK

Per session info

- The <src ip, src port, dst ip dst port>
- Session state (SYN/ SYNACK/ EST)

- VLAN ID used in the session
- Network interface used in this session

Cases analyzed by the iSSL functionality:

- **Asymmetrical Routing**: This process identifies and analyzes when a session has packets coming from multiple inline network pairs or if the GigaSMART engine cannot capture all the TCP and handshake messages.
- Duplicate SYN Counter: This process provides a count of duplicate SYN events found in the monitored traffic. A duplicate SYN event is when more than one TCP SYN packet is received before the SYN ACK packet is received in a given TCP session.
- In addition to the above, the following information can also be identified: max CPS of the traffic, current CPS, total number of sessions, total encrypted traffic, IP fragments (Ipfrags).

To enable ISSL monitor mode via GigaVUE-FM, Navigation plane \rightarrow Navigate to GigaSMART \rightarrow Inline Bypass \rightarrow Global Defaults \rightarrow check the checkbox on "Enable SSL session monitor".

🞯 GigaVUE-FM	MC2-Inline-SSL (H Series)			Q	1	C	Ш
HOME	Inline SSL Defaults						
A Overview							
T Workflows	Version	Min	Max				
at Node Topology		⊛ SSLv3	© 55LV3				
TRAFFIC		@ TLS1.0	0 71/51.0				
Ports		IN TICLA	a not t				
W Maps		10 TO 1.1					
GIERSMART®		⊜ TLS1.2	* TLS1.2				
P-Inline Bypass	Caching persistence						
an Active Visibility	SSL Sessions Resumption	8					
SYSTEM	SSL Session Monitor						
IIII Chassis			Note: SSL Sessions Resumption only for debugging purpose as this will affect performance				
Roles and Users							
A Health							
Settings							
HURROW)							
TE Logs							
e Debug							
Get Started							
O About						5	

Verify the SSL monitor Stats Navigate to Inline-SSI → Monitor statistics

🙆 GigaVUE-FM	HC2-Inline-SSL (H Senet)						Q 📌	C H admin ?
HOME A Overview N Workflows	GigaSMART Operations (GSC SSL Profiles Key Store	DP) GigaSMART Groups Signing CA Trust Stor	Virtual Ports NetFlow / IPFIX e Global Defaults Netwo	Generation Inline SSL P. rk Access Cache Persistence	essive SSL Application Session Session Statistics Monito	n Fritering Whitelist Po v Stansous	n Throttie	
A Node Topology TEATRI: Ports Y Maps	Inline SSL Session	n Monitor						Export Report Clear Statistics
S GigaSMART® Inline Bypass Active Visibility	✓ Interface Packet Live St	tatistics						
SYSTEM	Interface	Total Packets	SYN	SYN-ACK	Single VLAN	Multiple VLAN	IP Header Fragment	IP Sub Fragment
Chassils Chassils A Roles and Users	13/24	4240	228	0	4240	0	0	0
A -Health	1/3//23	7428	0	270	7428	0	0	ũ
Settings	1/3//21	42	0	28	42	0	0	0
suprom III Logs ● Debug ● Get Started	1542	4)	0	0	et i	ũ	0	0
0 About								

How to verify configurations in the CLI

Execute the following CLIs for verifying the configurations:

show inline-network

NOTE: Physical Bypass should be disabled, Traffic Path should be to-inline-tool and Forwarding Status should be Normal.

- show inline-network-group
- show inline-tool

Note: Inline-Tool Enable should be true, Shared Mode should be true (if set), Operational State should be up, Tool A/B Status should be up, Heart-Beat Enable should be true and Heart-Beat Status should be up.

show inline-tool-group

NOTE: Enable should be true.

show port params port-list <>

NOTE: Admin should be enabled, Link status should be up and Duplex should be full.

- show map all
- show gsgroup all
- show vport all

NOTE: Status should be up.

show gigasmart engine details [optional for inbound]

NOTE: Status should be up and up IP addresses should be assigned.

show gigasmart engine arp [optional for inbound]

NOTE: IP Address should be assigned.

- show gsop alias <>
- show apps keystore all
- show apps inline-ssl trust-store all

NOTE: Certificate chain of destination servers should be installed.

- show apps inline-ssl global
- show apps inline-ssl profile all

How to monitor statistics in the CLI

Execute the following CLIs for monitoring traffic:

- show port stats port-list <>
- show map stats all
- show gsop stats all
- show gsgroup stats all
- show vport stats all
- show gigasmart engine stats [optional]
- show apps inline-ssl session summary
- show apps inline-ssl session any

NOTE: Protocol should be TLS/SSL, Decryption should be YES, Error should be NO_ERR, SSL State should be Decrypting.

- show apps inline-ssl session match hostname <>
- show apps inline-ssl stats detail

Monitor Mode statistics in CLI

Use the following commands to display monitor mode statistics:

- show apps inline-ssl monitor summary
- show apps inline-ssl monitor session any

```
show apps inline-ssl monitor session match ipv4-src <src ip>
|ipv4-dst <dst ip> | 14port-src <sport> | 14port-dst <dport>
```

See Inside Your Network™