Deployment Guide:
Inline SSL

GigaVUE-OS 5.4

Contents

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 less-specific 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.
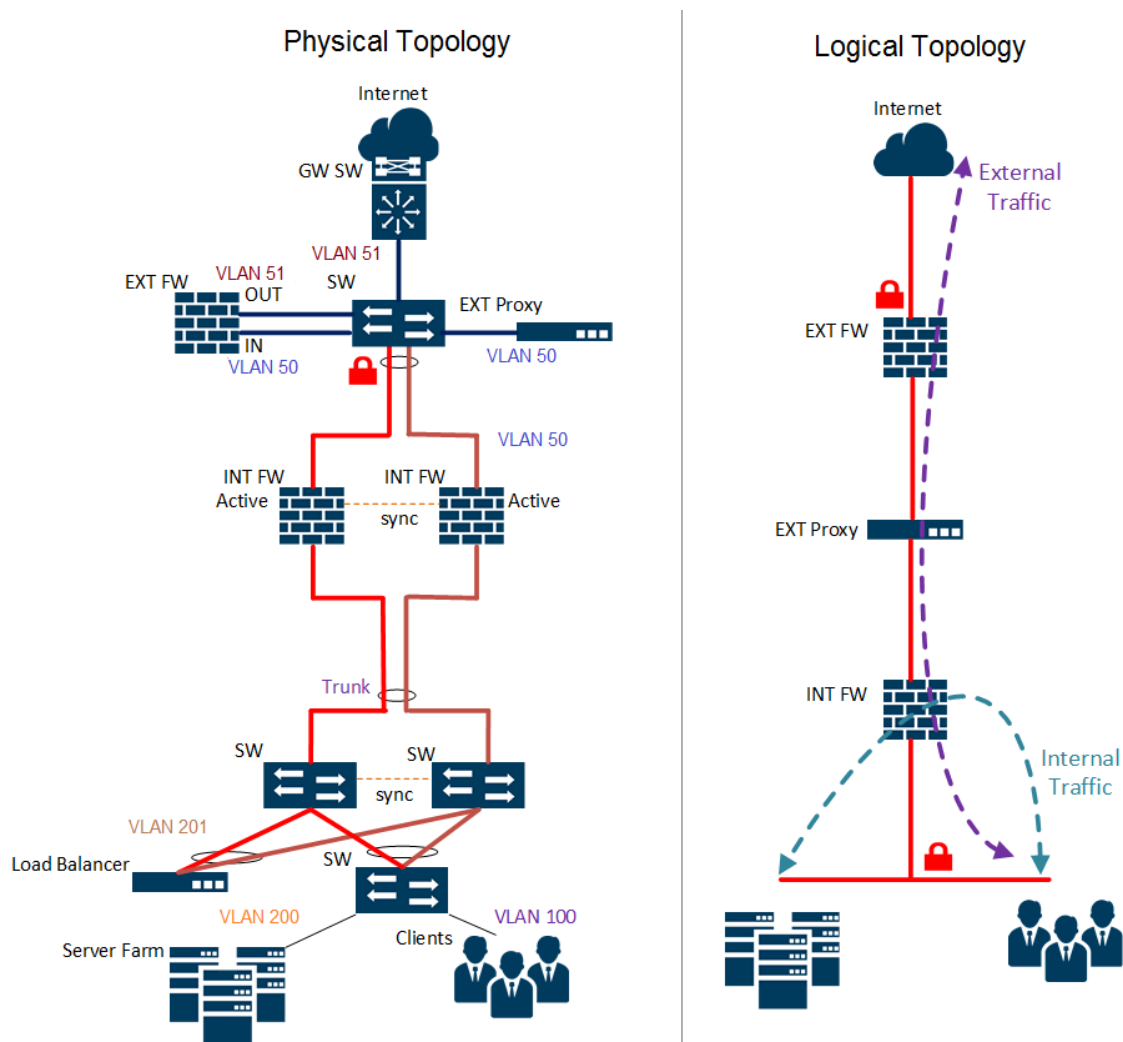

Figure 1 Enterprise Network

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.
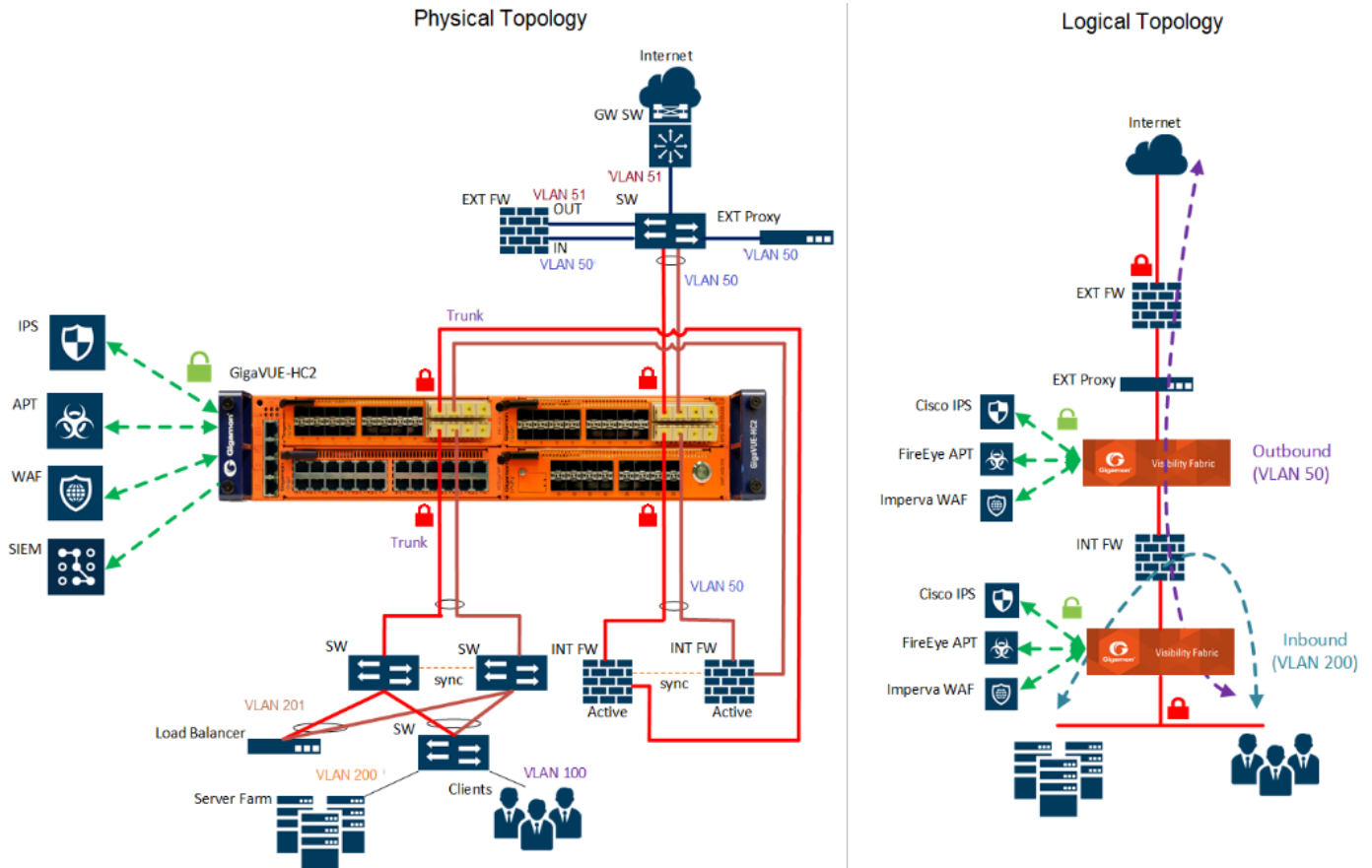

Figure 2 GigaSECURE® Security Delivery Platform's enterprise network deployment

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

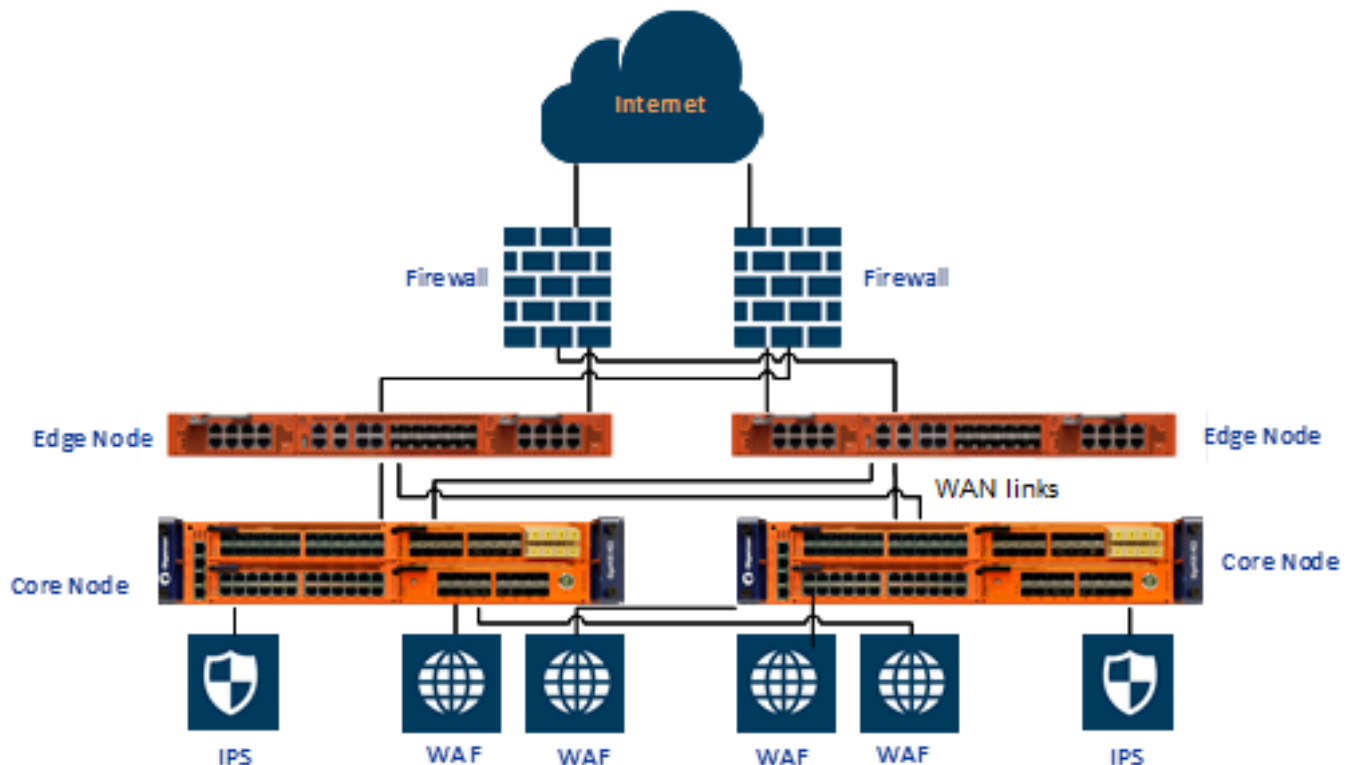- the rest of the decrypted traffic is inspected by both IPS and WAF.

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.

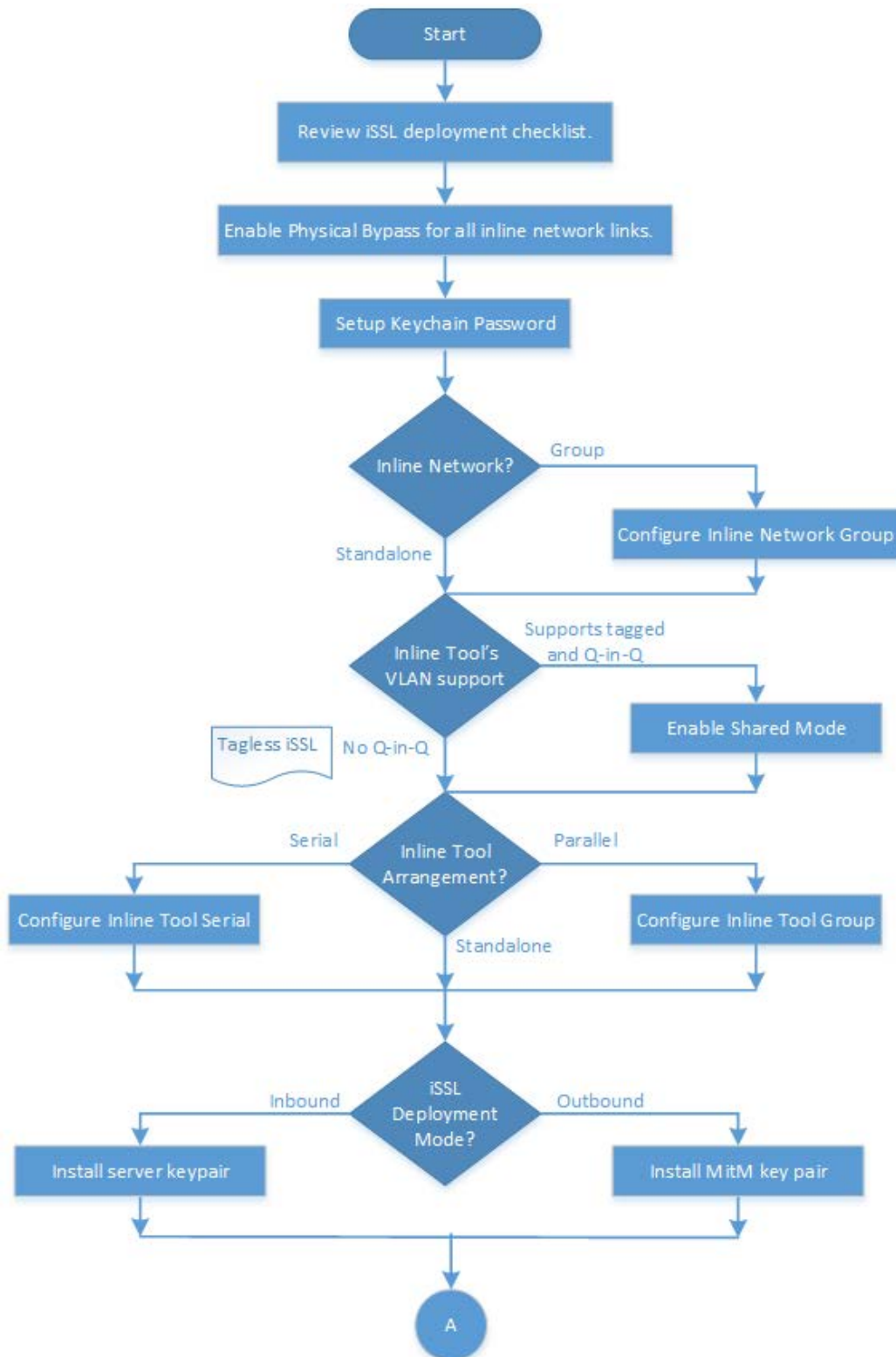# Flowchart for deploying the Inline SSL Solution

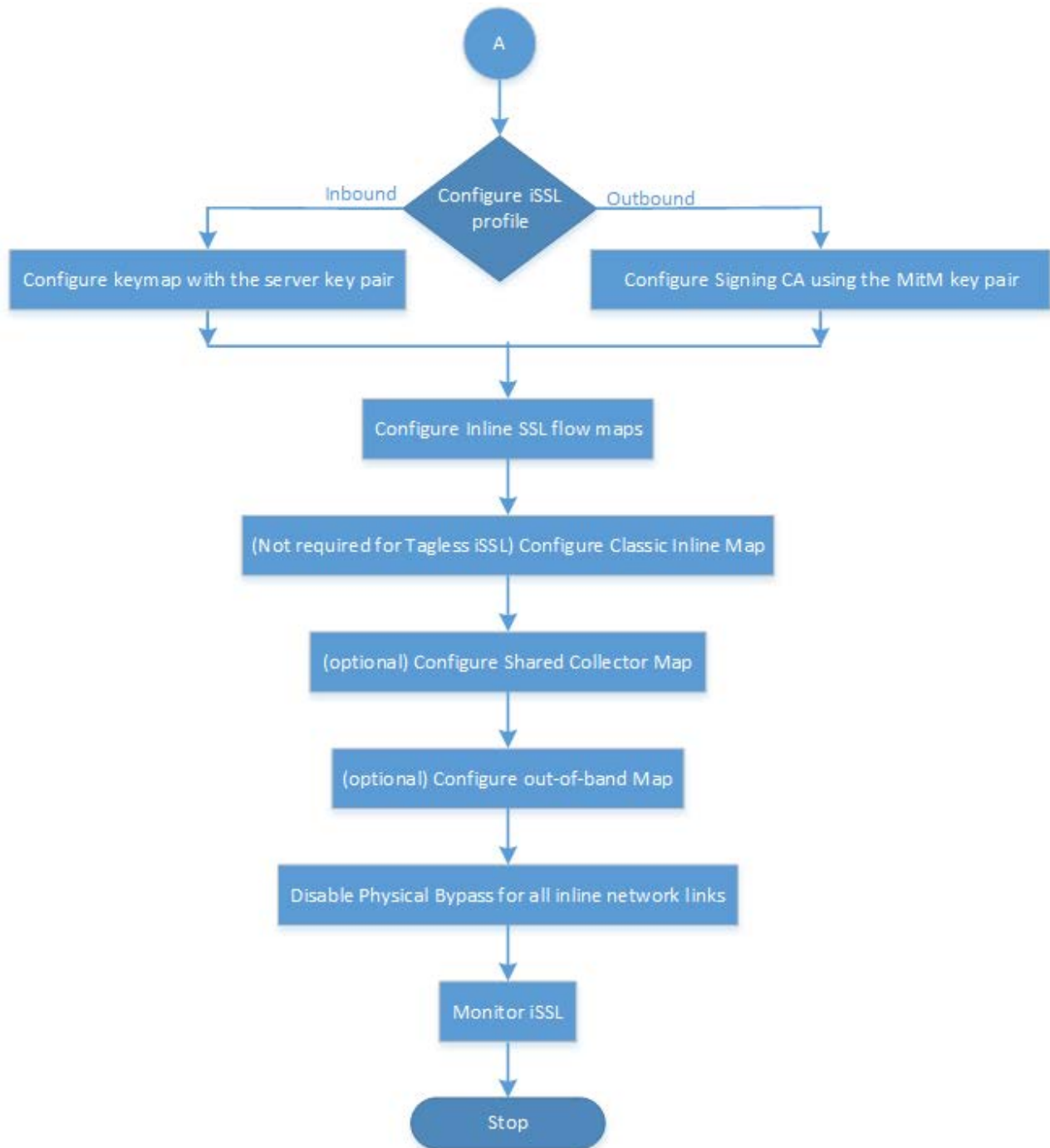*Figure 4 Flowchart for deploying the Inline SSL Solution—Part 1*

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.
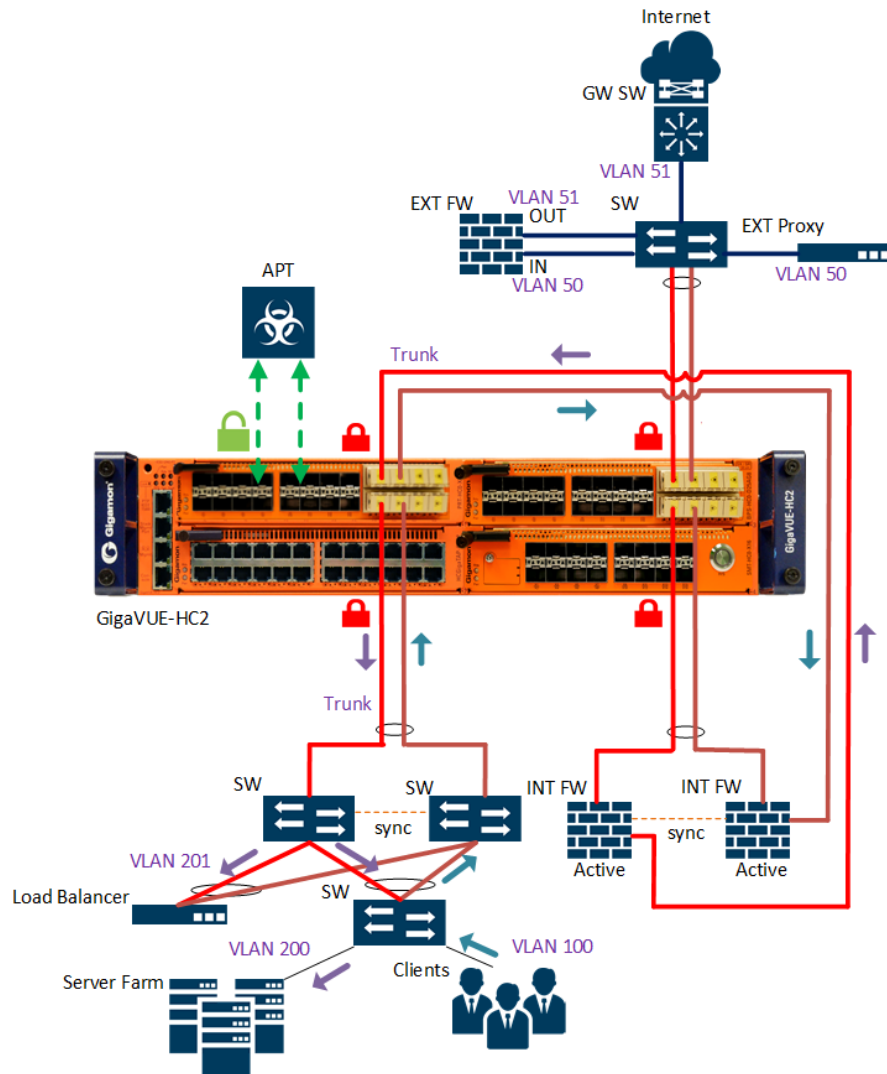

Figure 6 GigaSECURE® inbound Inline SSL Solution Deployment.

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.)

Figure 7 s2.example.com certificate chain

Example Sub CA Certificate

 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.
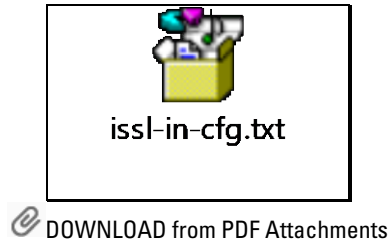
2. Configure Inline Tool

   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**.

2. 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.

3. 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 of this document for the detailed steps.

Gigamon device's CLI configuration:

issl-in-cfg.txt

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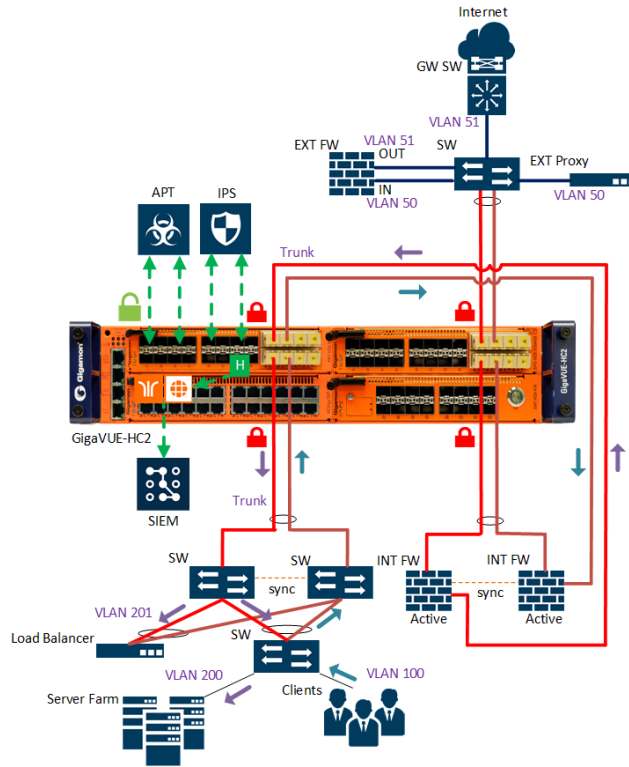
Figure 8 Compliant GigaSECURE® inbound Inline SSL Solution and out-of-band APF Deployment

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.

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.
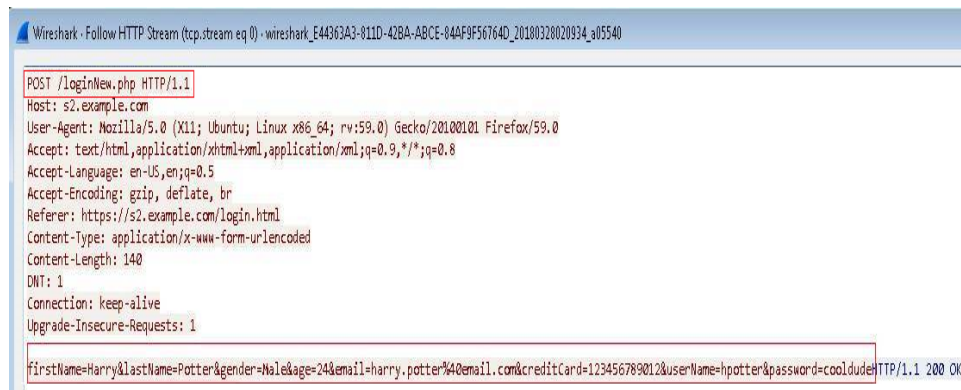

Figure 10   Wireshark® capture of the HTTPS POST request

- *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:

issl-in-with-APF-maski ng-cfg.txt

📎 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
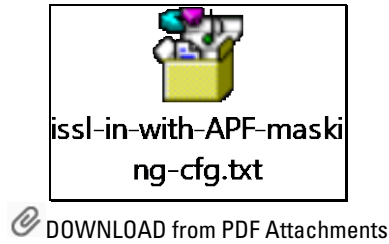
7. Inline SSL session runtime statistics

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


```
▷ Frame 14: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits)
▷ Ethernet II, Src: Cisco_38:72:c6 (00:d7:8f:38:72:c6), Dst: Vmware_0a:f0:47 (00:0c:29:0a:f0:47)
▷ Internet Protocol Version 4, Src: 192.168.100.2, Dst: 192.168.200.246
▷ Transmission Control Protocol, Src Port: 45970, Dst Port: 80, Seq: 1, Ack: 1, Len: 601
▷ Hypertext Transfer Protocol
◢ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▷ Form item: "firstName" = "Harry"
  ▷ Form item: "lastName" = "Potter"
  ▷ Form item: "gender" = "****"
  ▷ Form item: "age" = "**"
  ▷ Form item: "email" = "***********************"
  ▷ Form item: "creditCard" = "*************"
  ▷ Form item: "userName" = "hpotter"
  ▷ Form item: "password" = "********"
```

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.
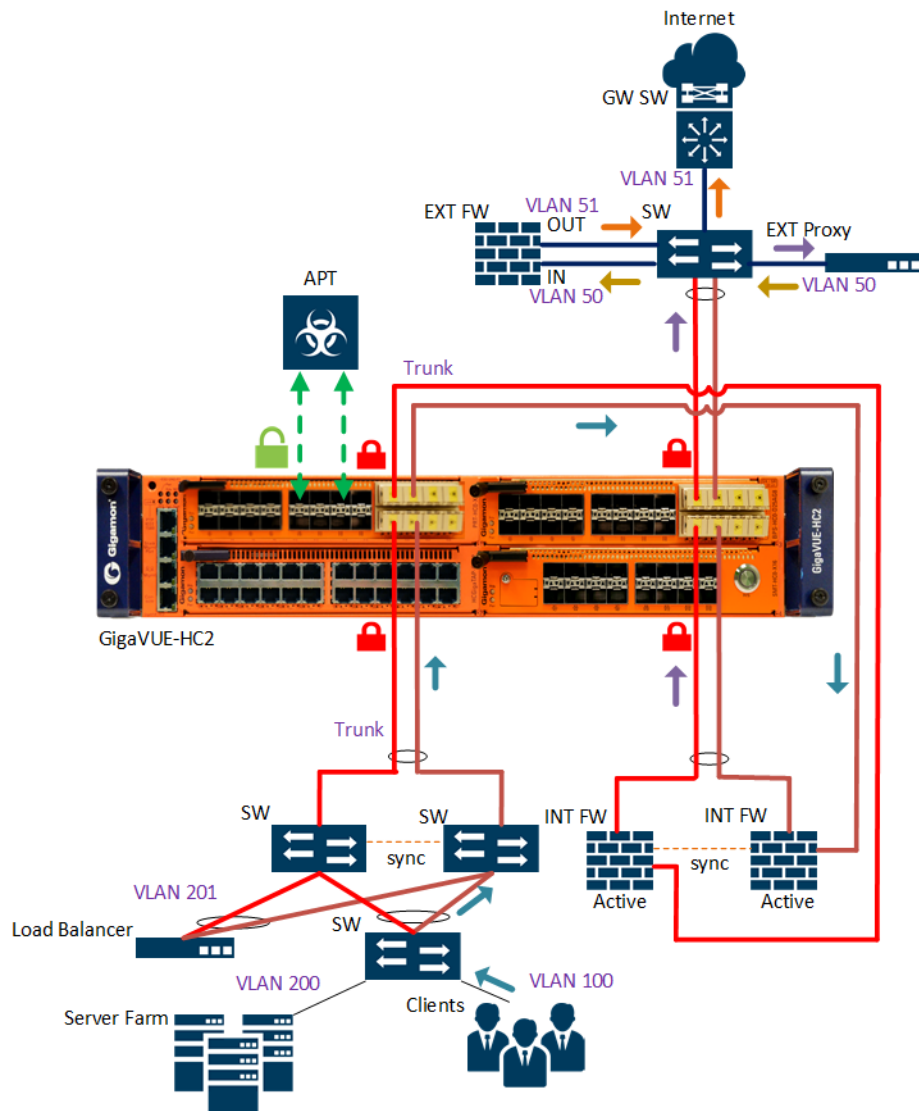
Figure 12   GigaSECURE® Inline SSL Solution with explicit proxy.

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.
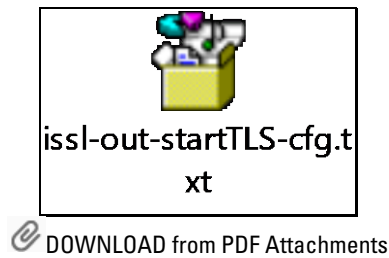
To launch the workflow:

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

2. From the device navigation pane, select: **Workflows > Inline GigaSMART Operations**.

3. 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**.

3. 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:

issl-out-startTLS-cfg.t
xt

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.
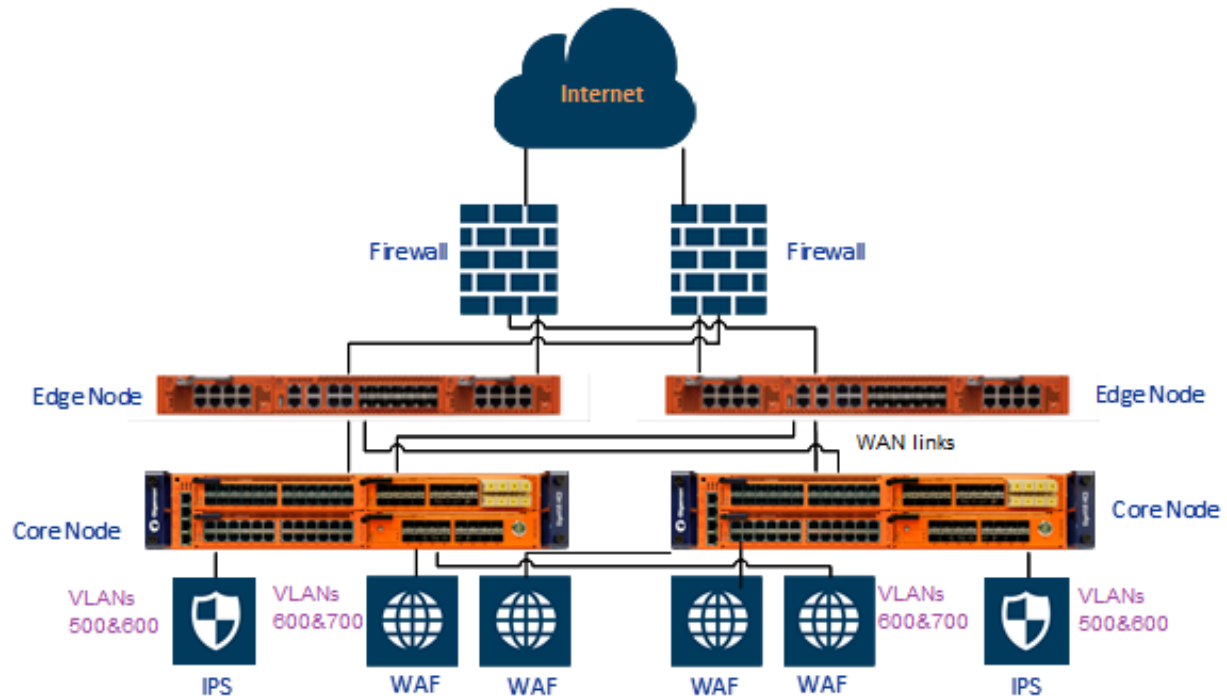
Figure 13   Two-tier hierarchical deployment of GigaSECURE® Security Delivery Platform
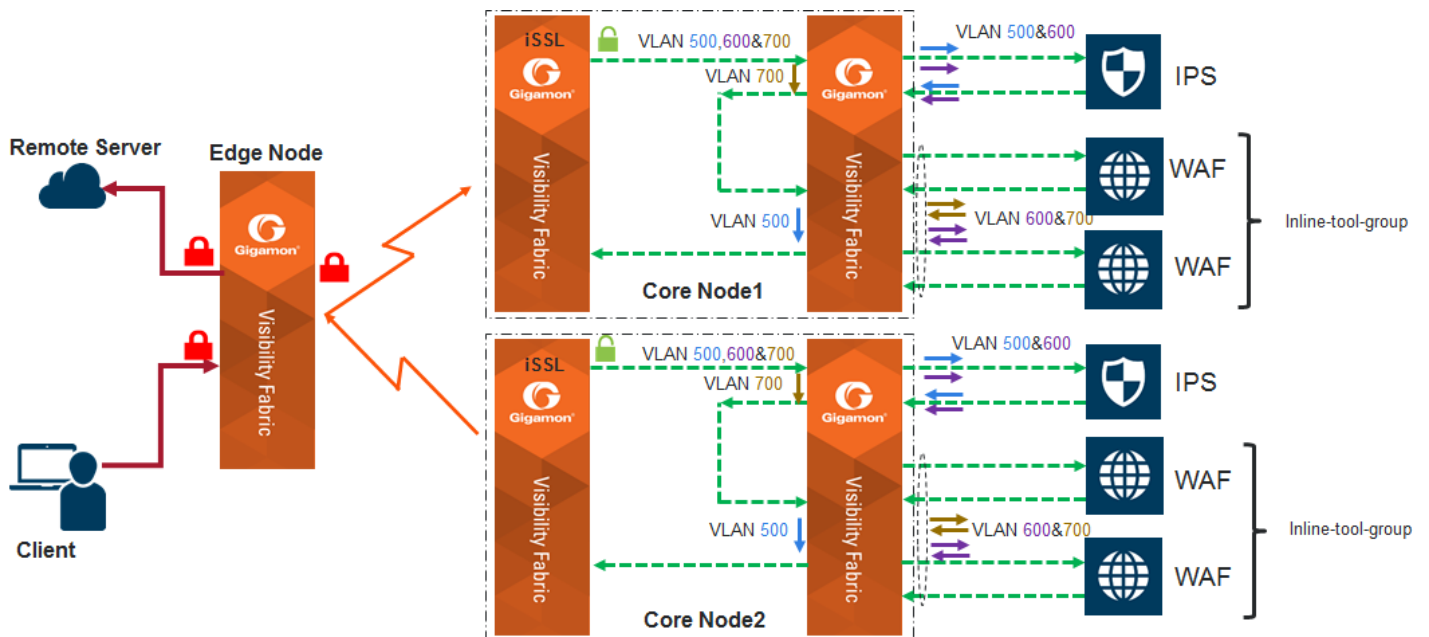
Figure 14   Logical topology of the two-tier hierarchical architecture

Edge Layer Device Configuration

To configure the Edge layer devices:

1. Configure the inline network ports as illustrated below:

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:

Figure 16   Configuring Inline Network

3. Configure the inline network groups as illustrated below:

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.

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.

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.

Figure 20   *Configuring Rule Based Inline Map*

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

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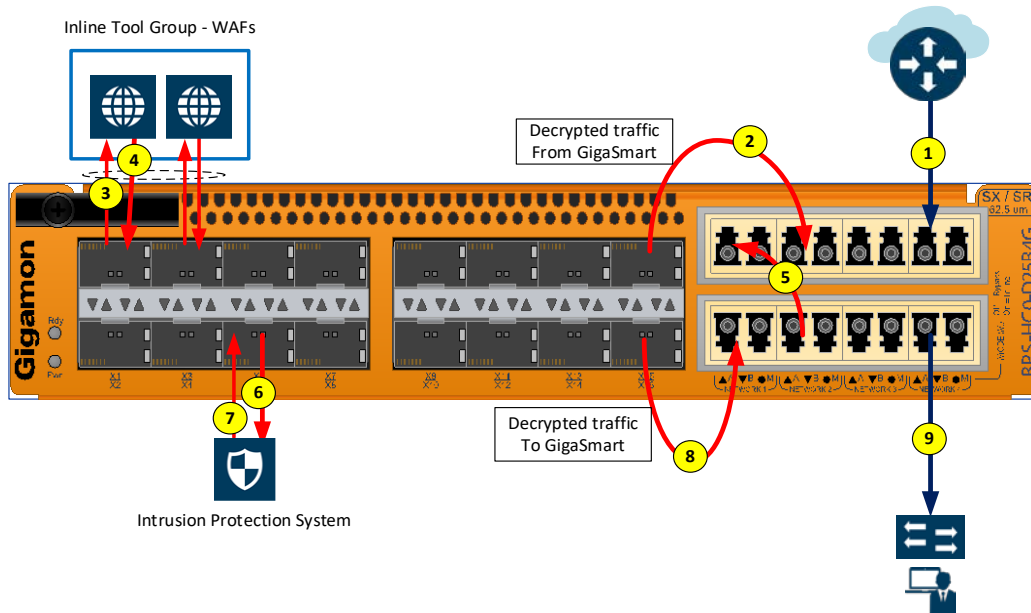
Figure 22   Traffic steering at a Gigamon device in the Core layer.

To configure the Core layer devices:

1.   Configure inline network ports.

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.

Figure 24   Configuring Inline Network

3. Configure the inline network groups as illustrated below.

Figure 25   Configuring Inline Network Group

4. Configure the inline tools as illustrated below.

Inline Tool ISSL_IT

Inline Tool Info

Alias	ISSL_IT
Comment	comment

Ports

Port Editor

Port A	1/4/x11 (ISSL_ITA)
Port B	1/4/x12 (ISSL_ITB)

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

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.

Figure 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.

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.

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

Figure 30   Configuring Classic Inline Map for bypassing all other traffic

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

Gigamon device's CLI configuration:

PDF issl-high-density-dc -CoreDevice1.cfg.pd	PDF issl-high-density-dc -CoreDevice2.cfg.pd	PDF issl-high-density-dc -EdgeDevice1.cfg.pc	PDF issl-high-density-dc -EdgeDevice2.cfg.pc

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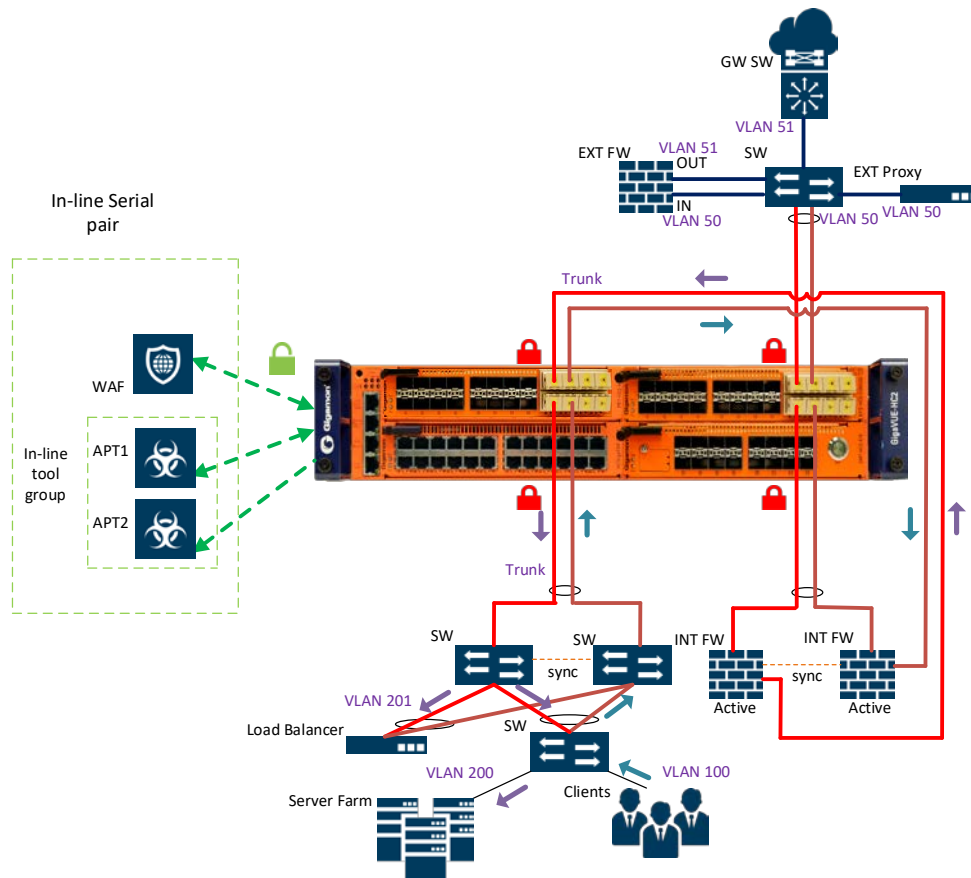
Figure 31   *GigaSECURE® inbound Inline SSL Solution multiple tool in series.*

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:

Inline_serial.pdf

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 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 .
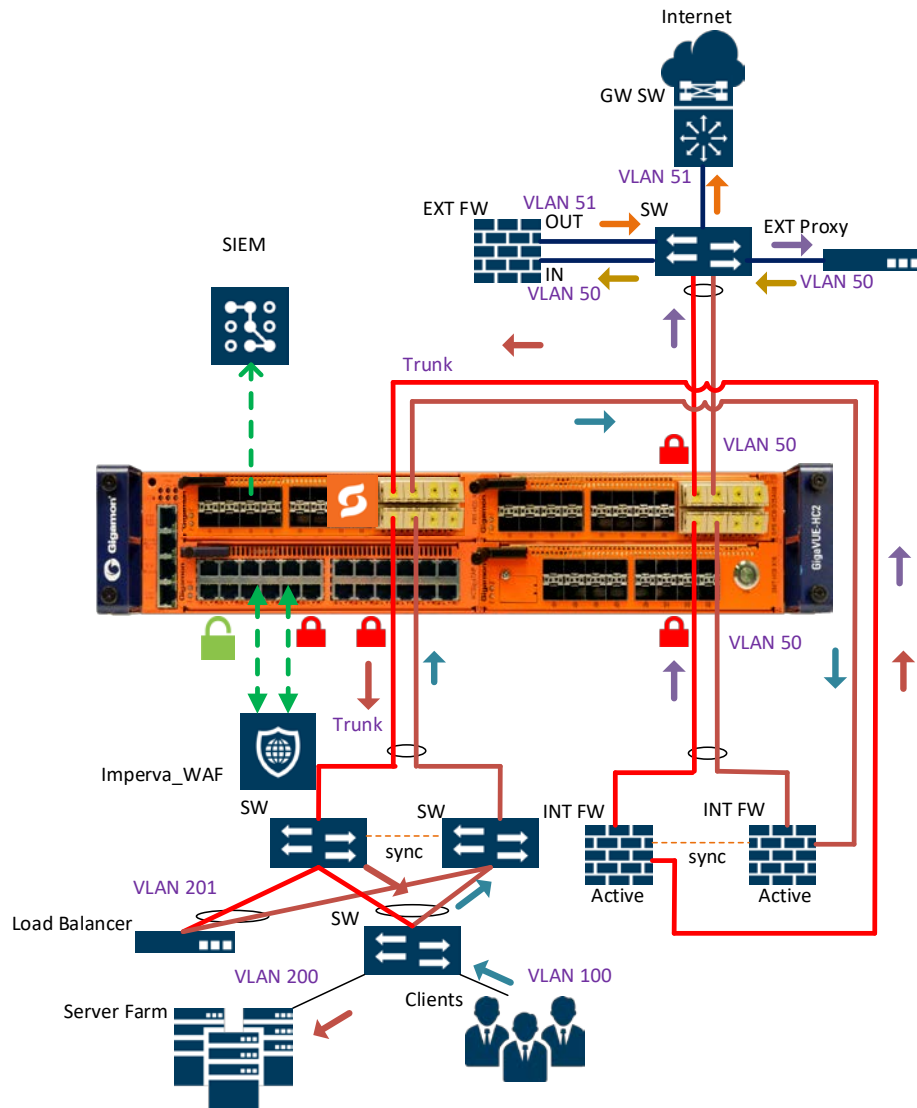
Figure 32   *GigaSECURE® inbound Inline SSL Solution with SIEM*

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-of-band 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:

Inline_SIEM.pdf

📎 DOWNLOAD 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 .
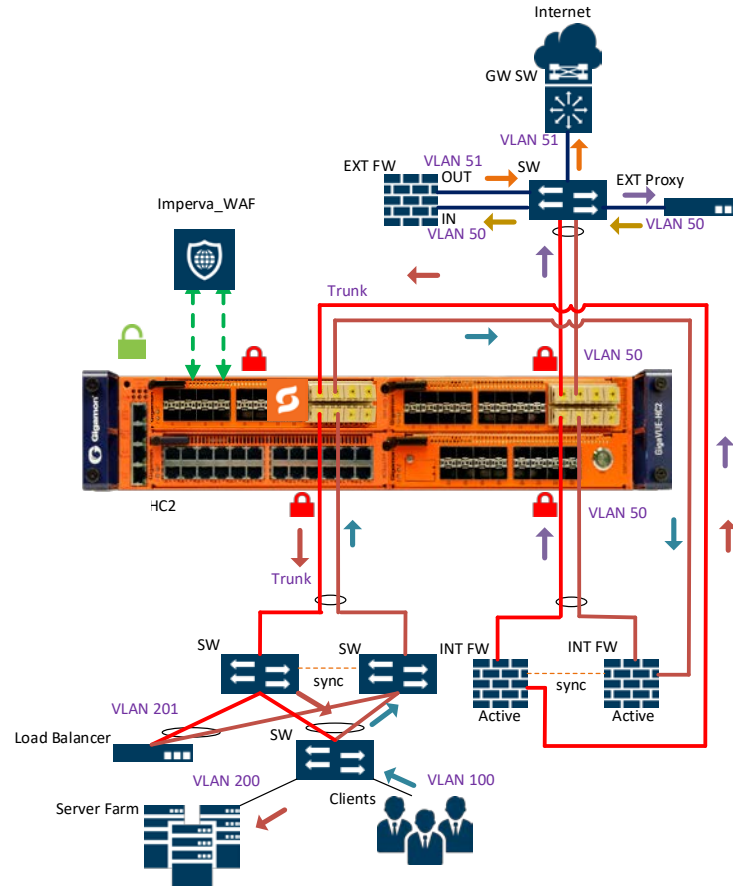
Figure 33   GigaSECURE® inbound and outbound Inline SSL deployment using the same GigaSMART

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:

Inline_single GS.pdf

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, 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**.
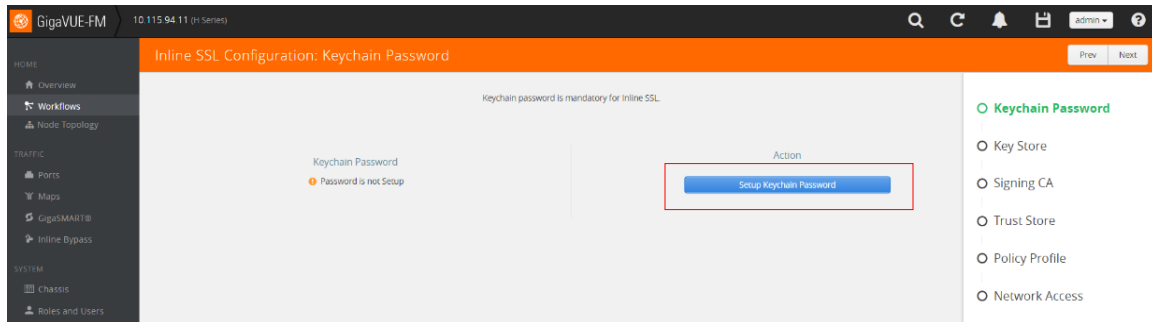
Figure 34   *Inline SSL Configuration Workflow: Keychain Password*

   b. Set the password and click **Submit** from the top menu.
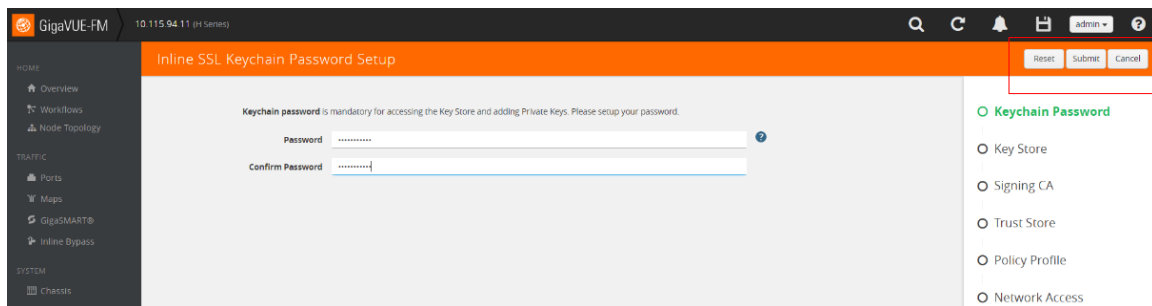
Figure 35   *Inline SSL Configuration Workflow: Configuring Keychain Password*

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**.
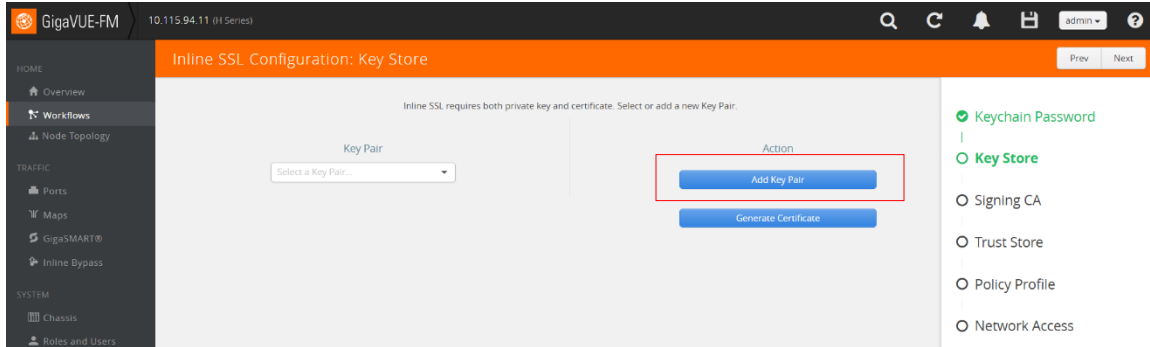
Figure 36   Inline SSL Configuration Workflow: Key Store

    b. Provide relevant details as illustrated below.

    c. Click **OK** from the top menu to install the key pair.
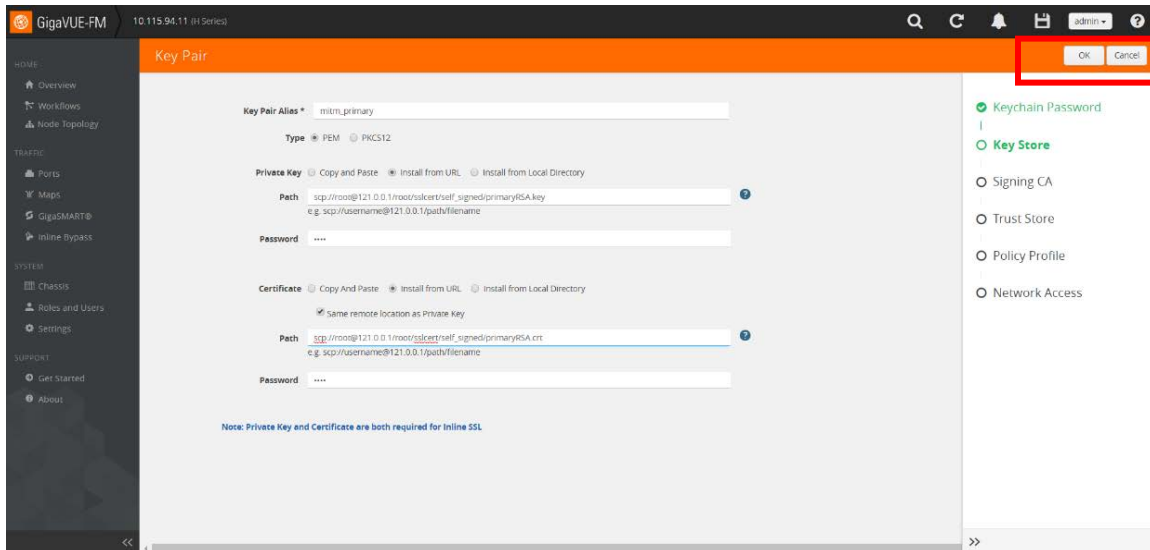
Figure 37   Inline SSL Configuration Workflow: Updating the Key Store

    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**.
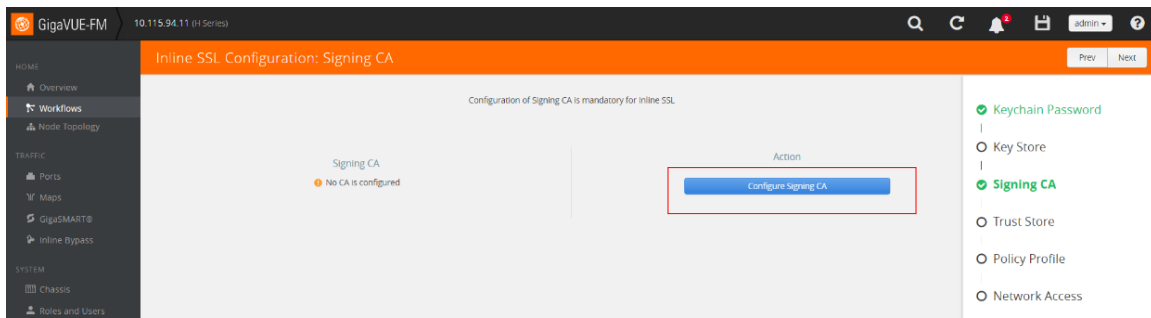
Figure 38   Inline SSL Configuration Workflow: Signing CA

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

c.   Click **OK** from the top menu to configure the mapping.
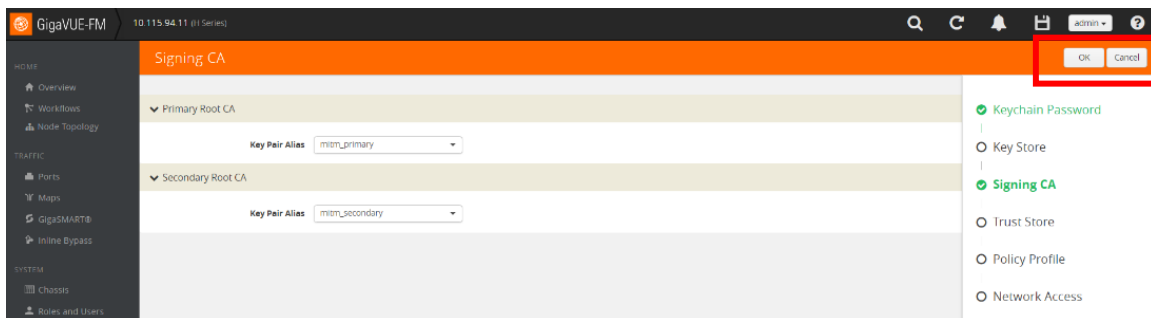
Figure 39   Inline SSL Configuration Workflow: Configuring Signing CA

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.
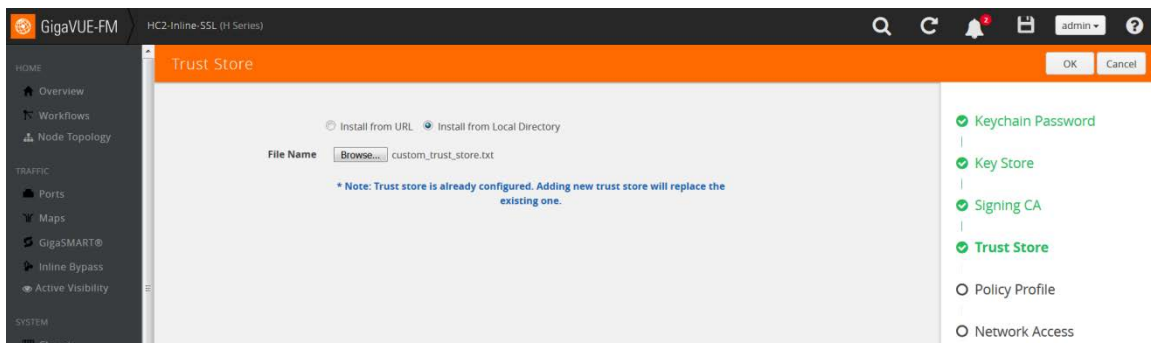
Figure 40   Inline SSL Configuration Workflow: Updating the Trust Store

5.   Configure the Inline SSL profile

a.   Click **Create**.
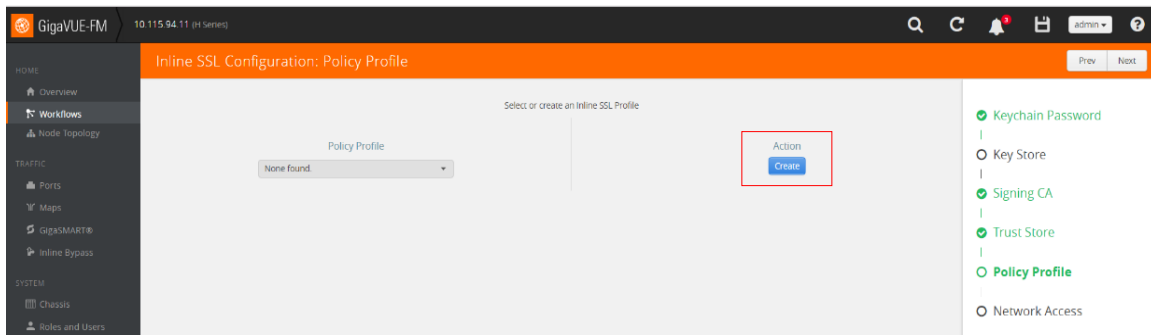
Figure 41   Inline SSL Configuration Workflow: Policy Profile

b.   Select the **Policy Configuration** and the **Security Exceptions** as illustrated below.
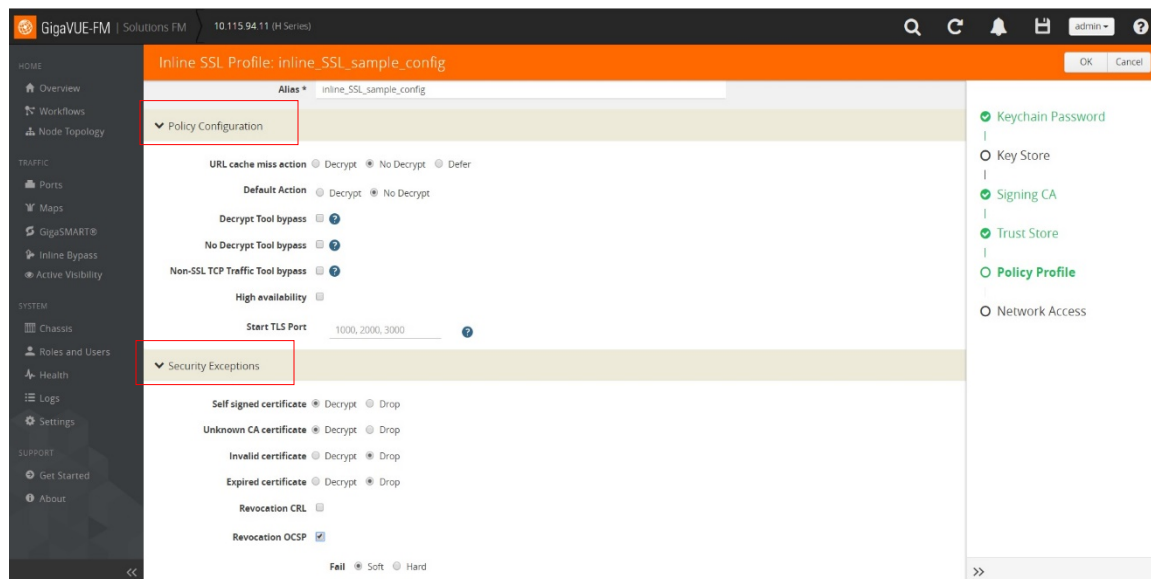
Figure 42   Inline SSL Configuration Workflow: Configuring Policy configuration & Security Exceptions in the Policy Profile

c.   Upload Whitelist and/or Blacklist as illustrated below

NOTE: Skip this step if it is not applicable.
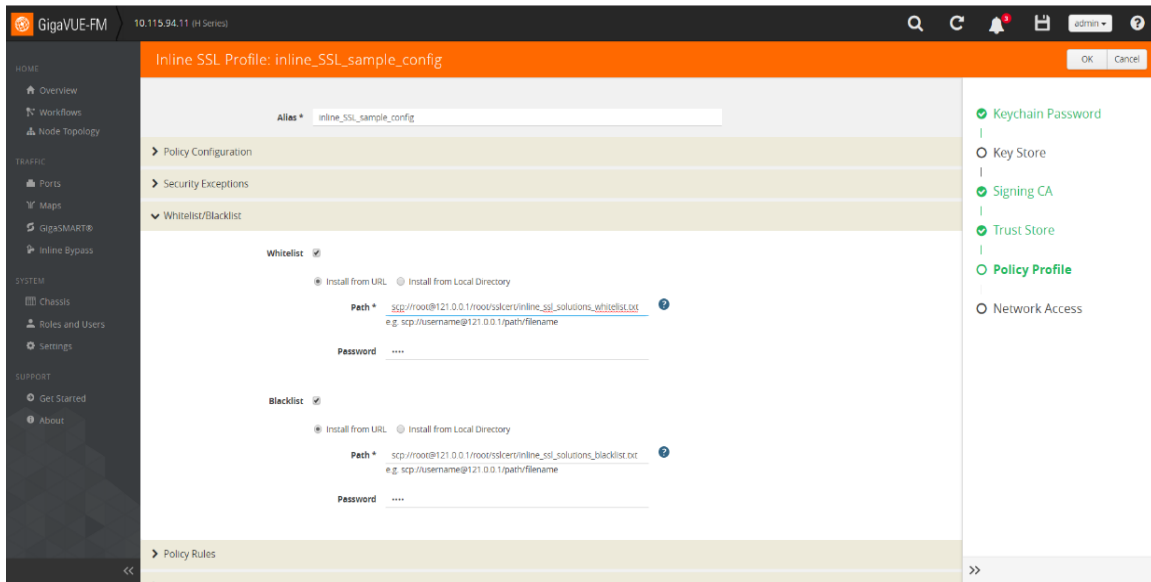
Figure 43   *Inline SSL Configuration Workflow: Configuring Whitelist/Blacklist in the Policy Profile*

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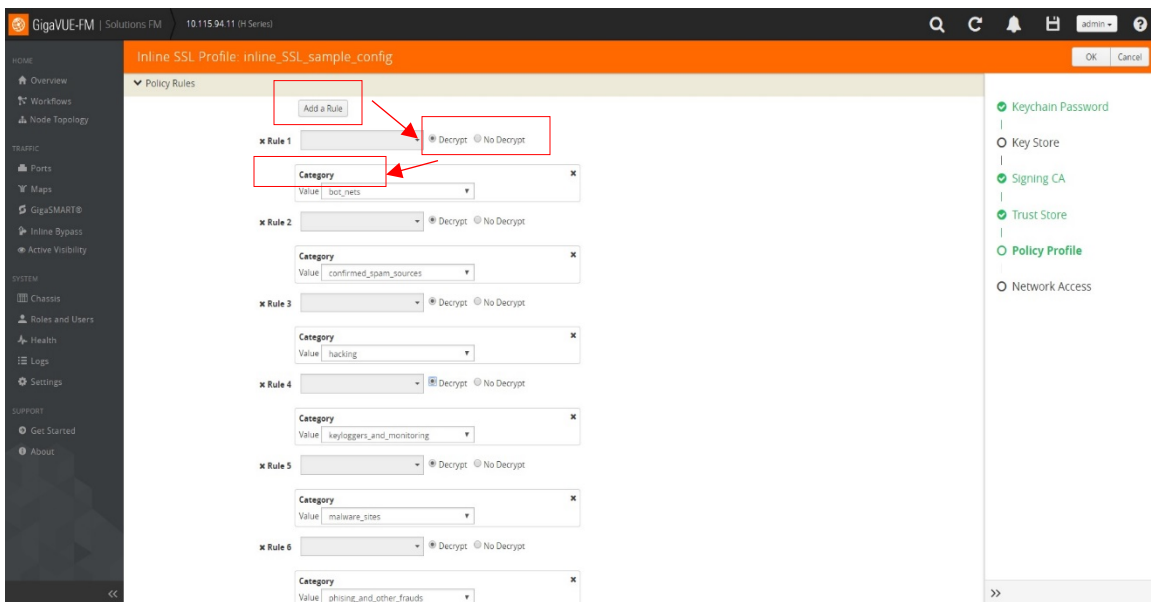
Figure 44   *Inline SSL Configuration Workflow: Configuring Policy Rules in the Policy Profile*

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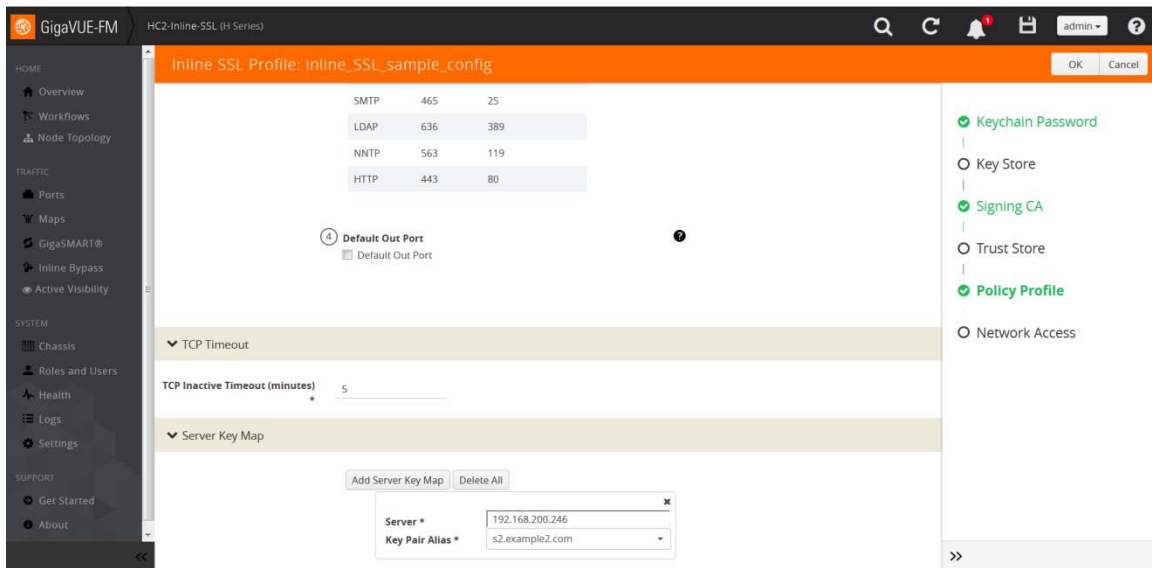
Figure 45   Inline SSL Configuration Workflow: Configuring Key Map in the Policy Profile

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**.
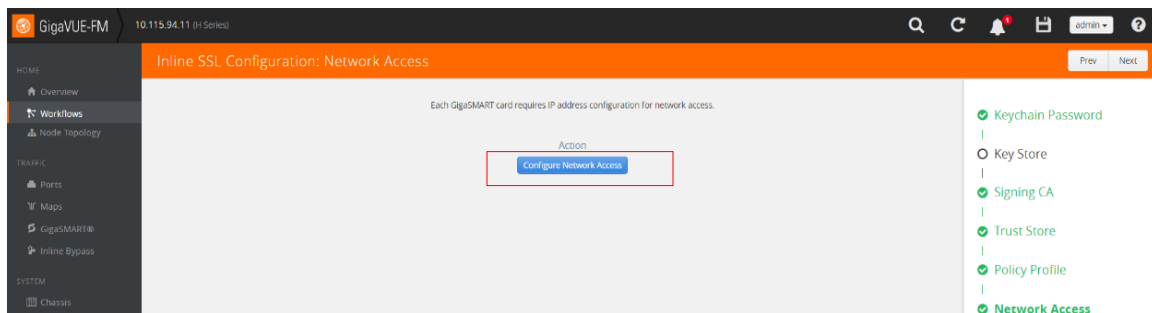
Figure 46   Inline SSL Configuration Workflow: Network Access step

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

Configuration Tasks   *53*

i.   Click **OK** from the top menu; exit the workflow.
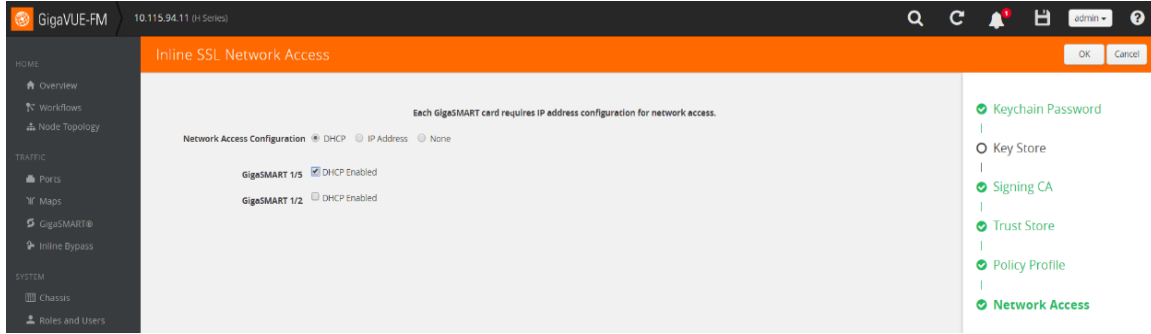
Figure 47   *Inline SSL Configuration Workflow: Configuring Network Access*

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.
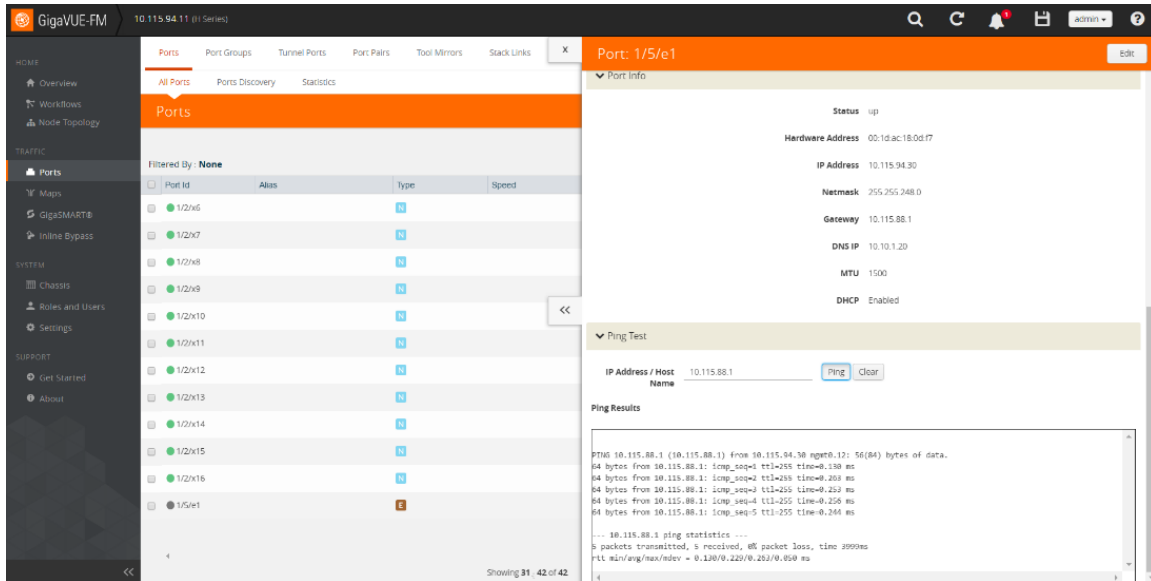
Figure 48   *GigaSMART engine interface Quick View window*

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.
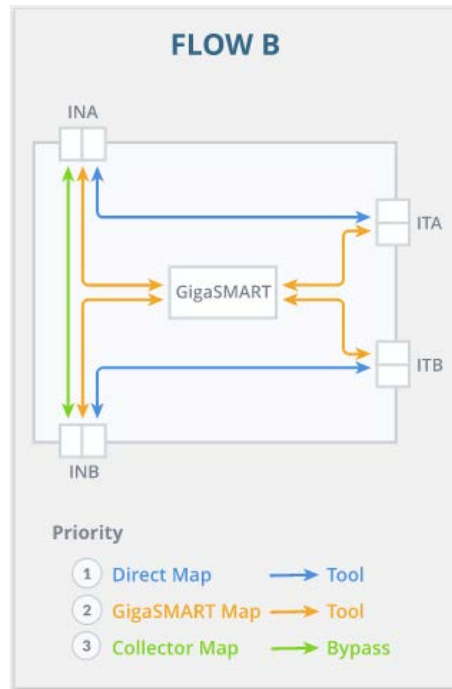
Figure 49   Inline SSL Map Workflow: Flow B

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**.
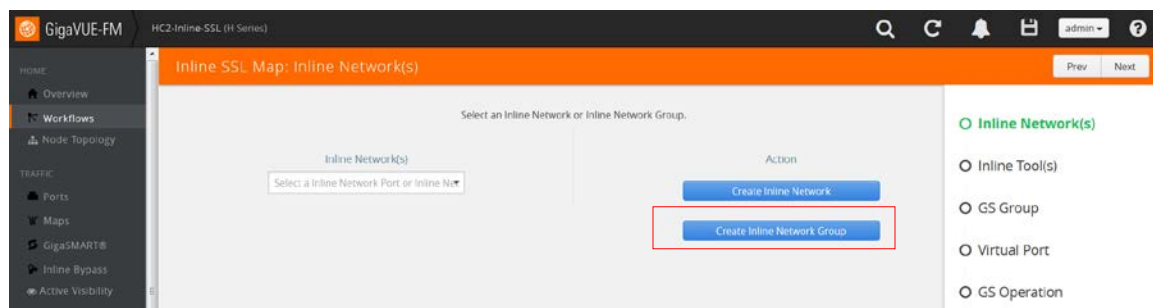
Figure 50   Inline SSL Map Workflow: Inline Network

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

Figure 51   Inline SSL Map Workflow: Creating inline network group

2.   Configure Inline Tool

a.   Click **Create Inline Tool**.

Figure 52   Inline SSL Map Workflow: Creating inline tool

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

Figure 53   Inline SSL Map Workflow: Creating inline tool ports
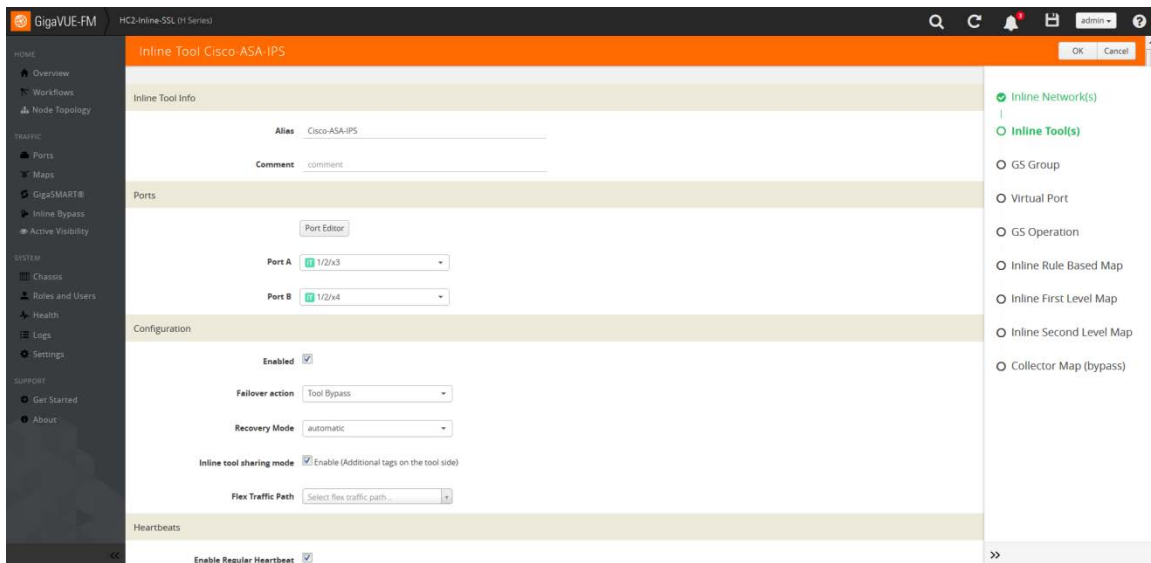
c.   Configure the inline tool as illustrated below.

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.
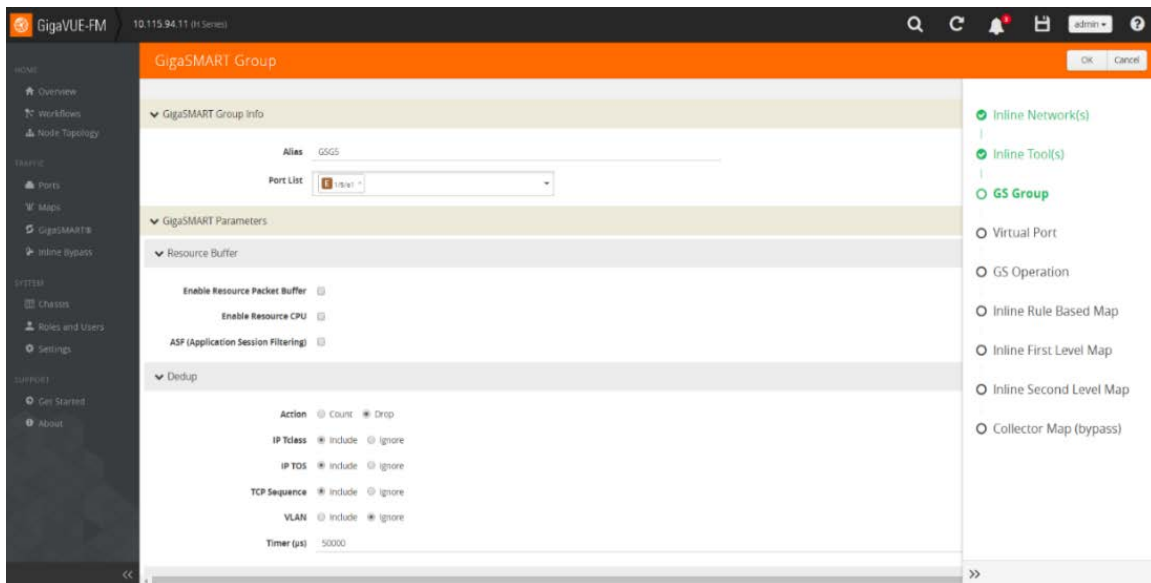
Figure 55 Inline SSL Map workflow: Creating new GigaSMART Group

4. Configure Virtual Port:

 a. Select **Create**.

 b. Enter an alias name and click **OK** from the top menu.
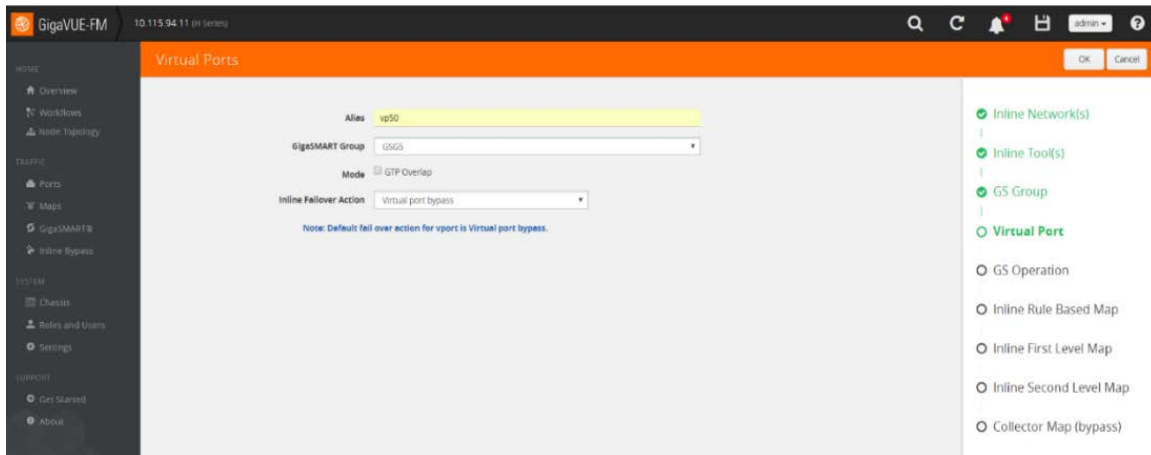
Figure 56   Inline SSL Map workflow: Creating new Virtual Port

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.
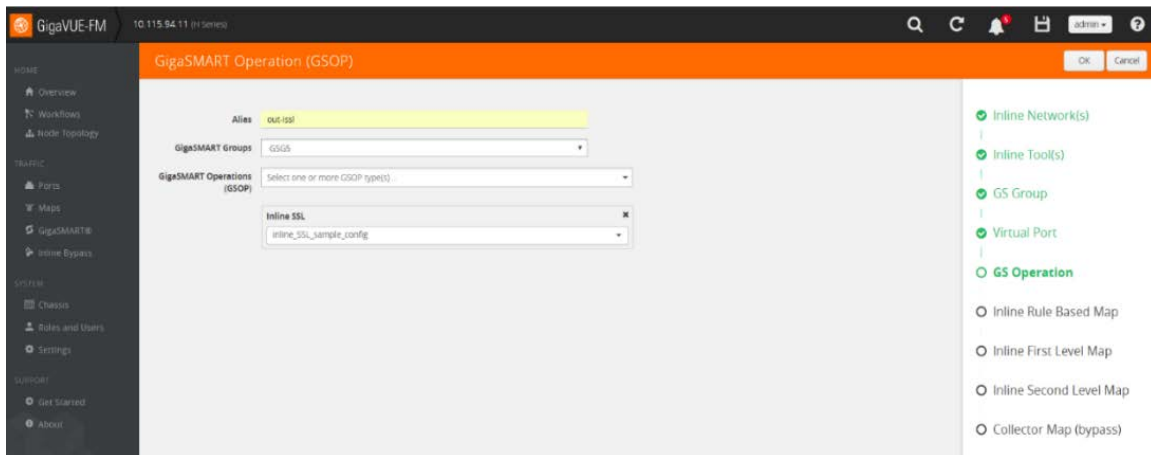
Figure 57   Inline SSL Map workflow: Creating GigaSMART Operation

6.   Configure the Inline Rule Based Map

a.   Provide details as illustrated below and click **OK**.
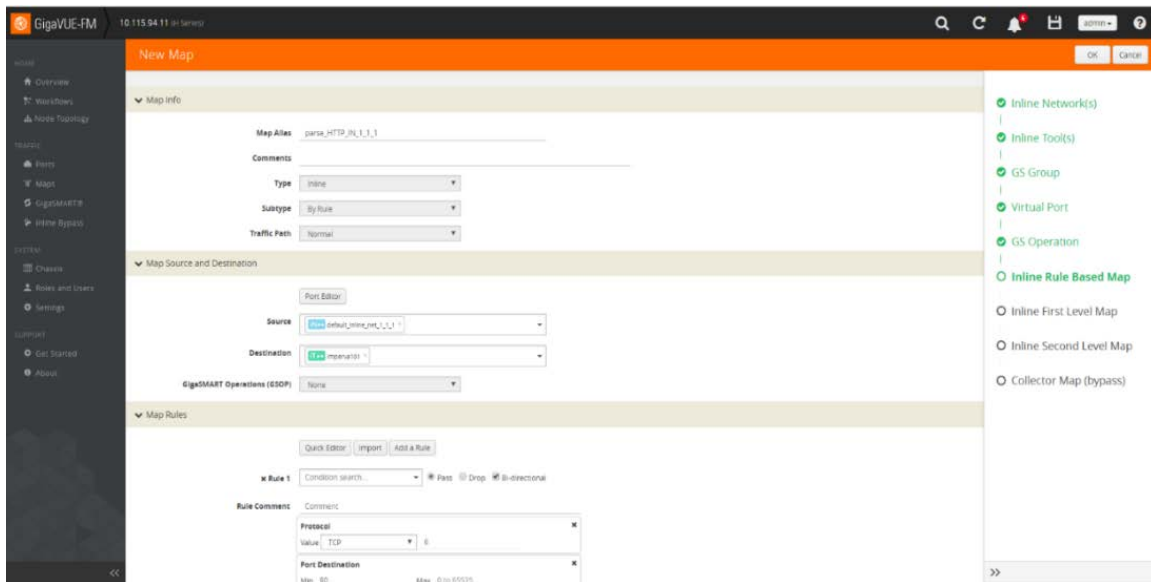
Figure 58   Inline SSL Map workflow: Creating Classic Inline Map

7.   Configure the Inline First Level Map:

a.   Provide details as illustrated below and click **OK**.
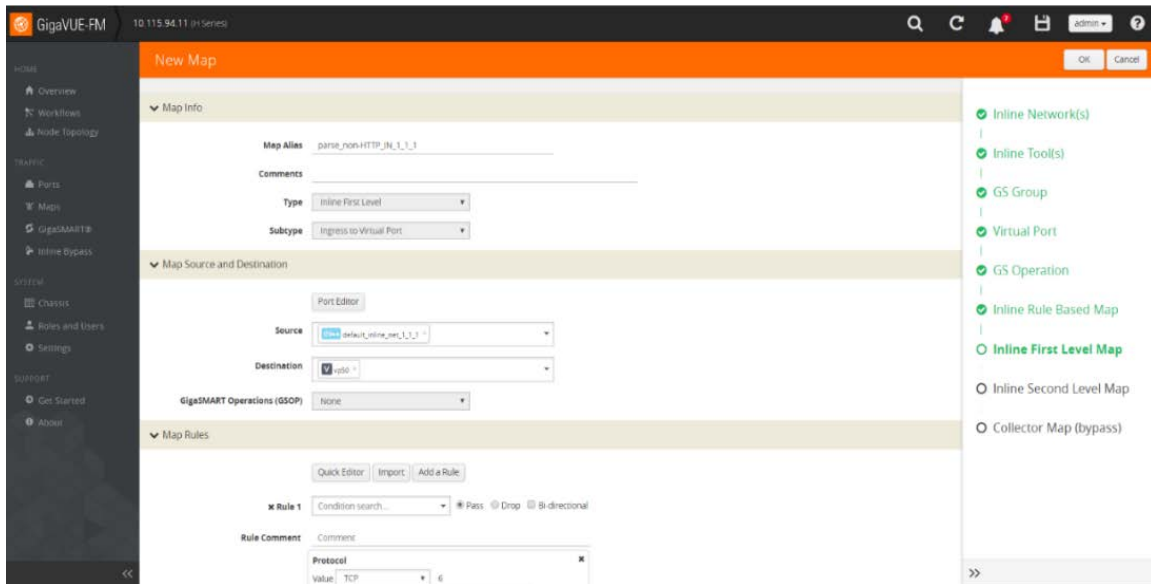
Figure 59   Inline SSL Map workflow: Creating Inline First Level Map

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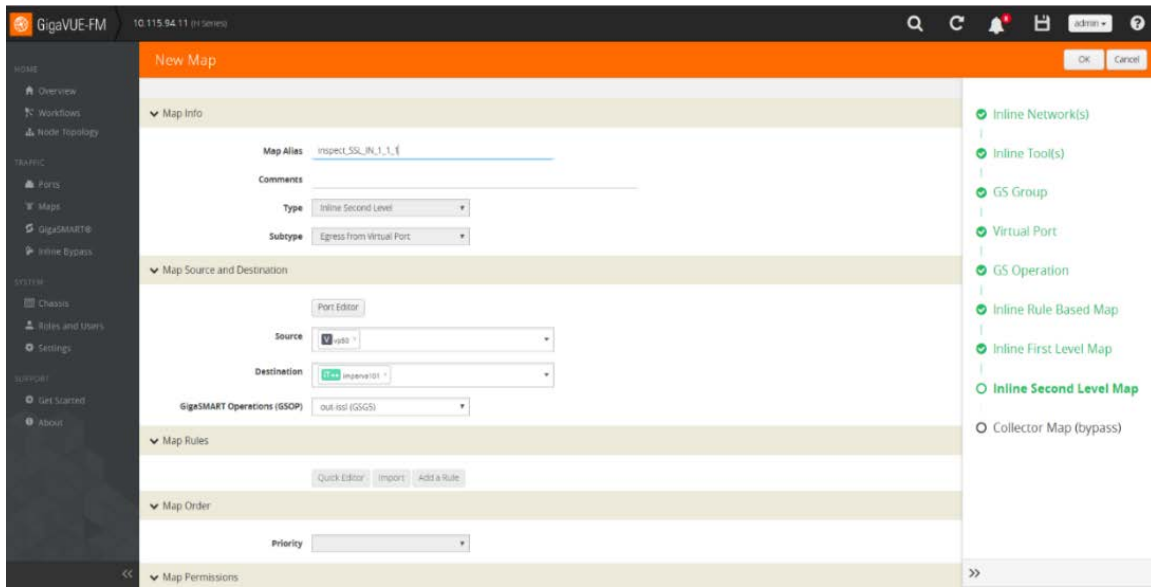
a.   Enter an alias name and click **OK**.

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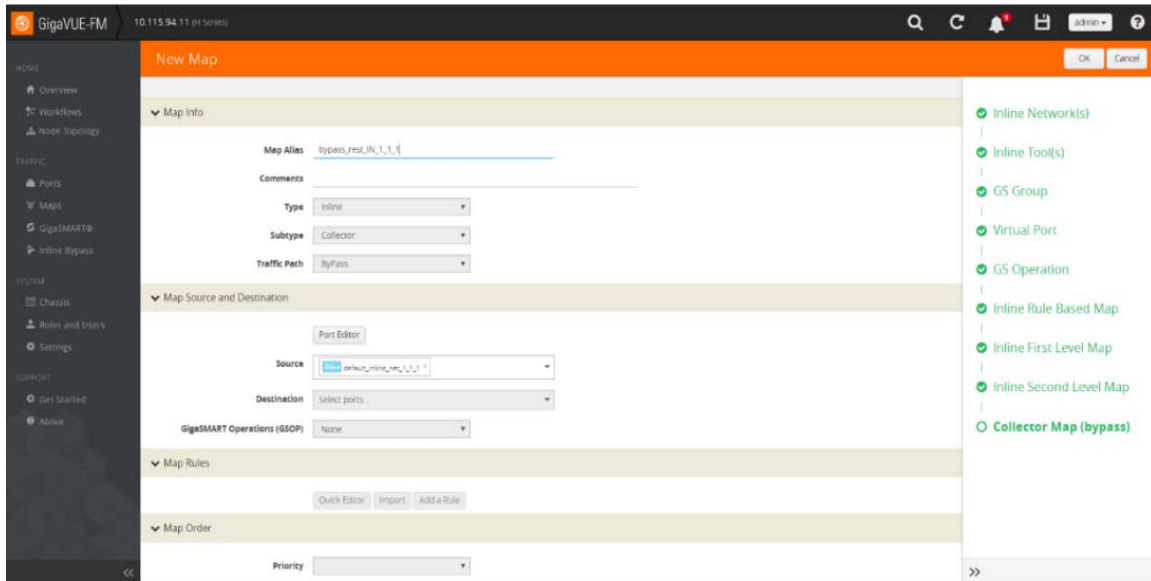
Figure 61   Inline SSL Map workflow: Creating the Shared Collector Map

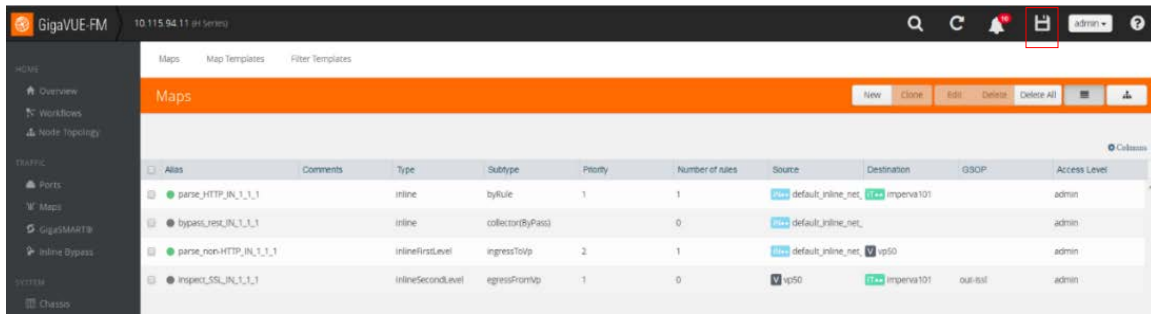   c.   Review the maps created by the workflow.

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.
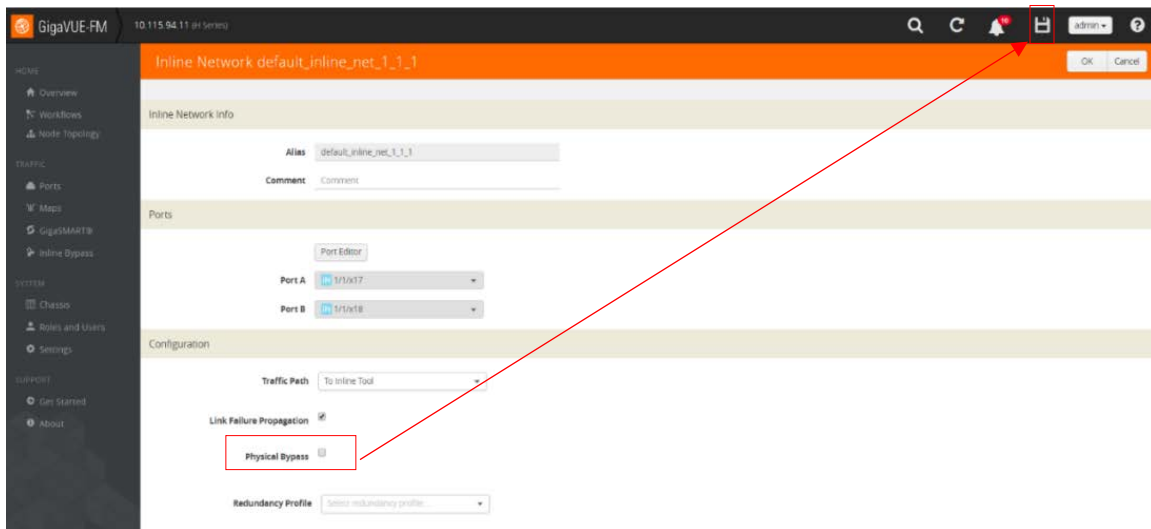
Figure 63   Updating Inline Network

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**.

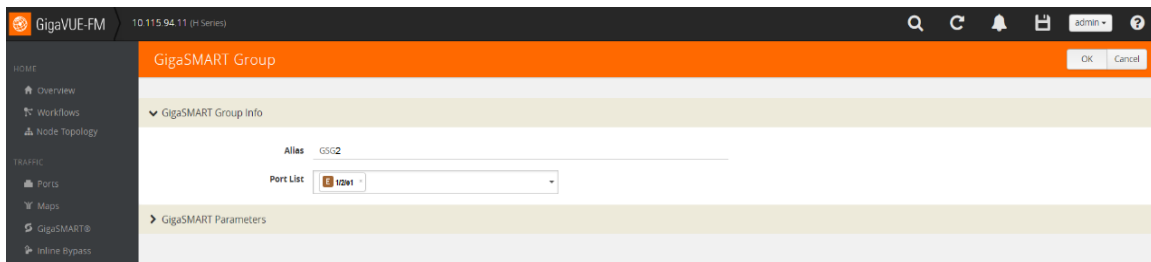   b. Provide details as illustrated below and click **OK**.

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**.

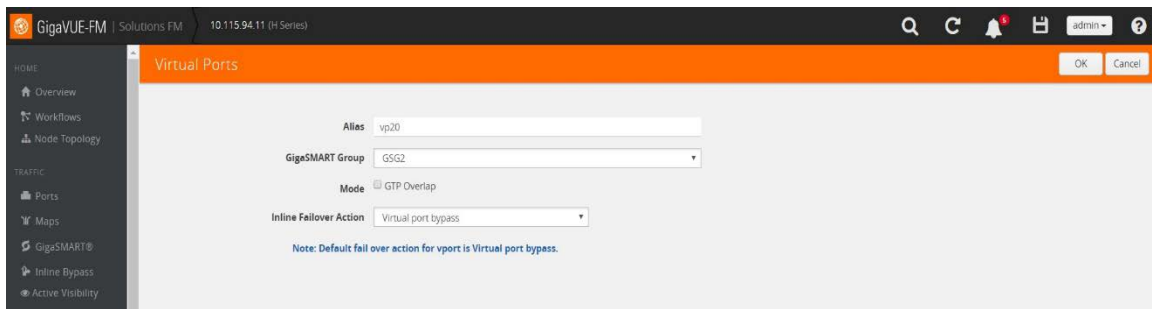   b. Provide details as illustrated below and click **OK**.

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.

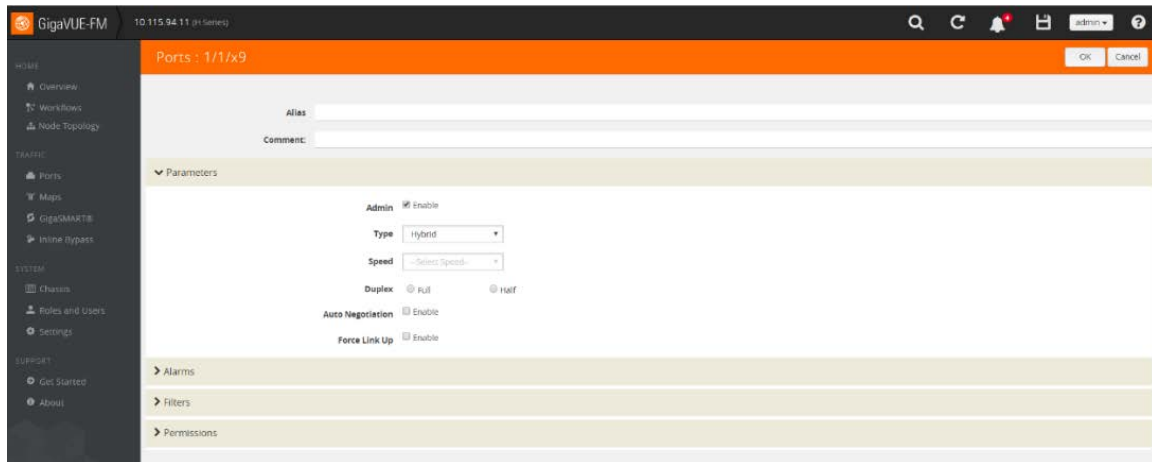   b.   Provide details as illustrated below and click **OK**.

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.

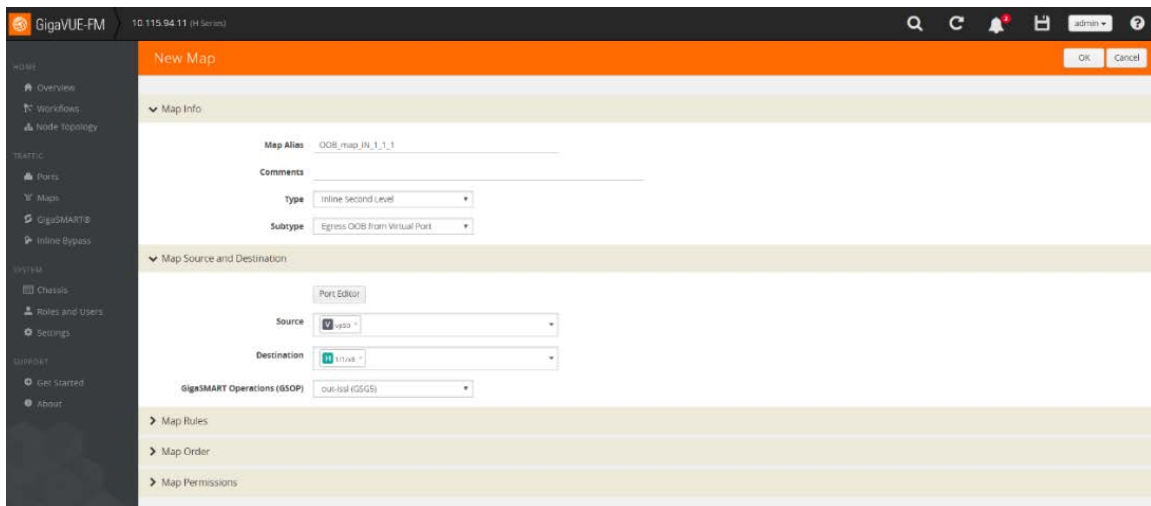   c.   Provide details as illustrated below and click **OK**.

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**.

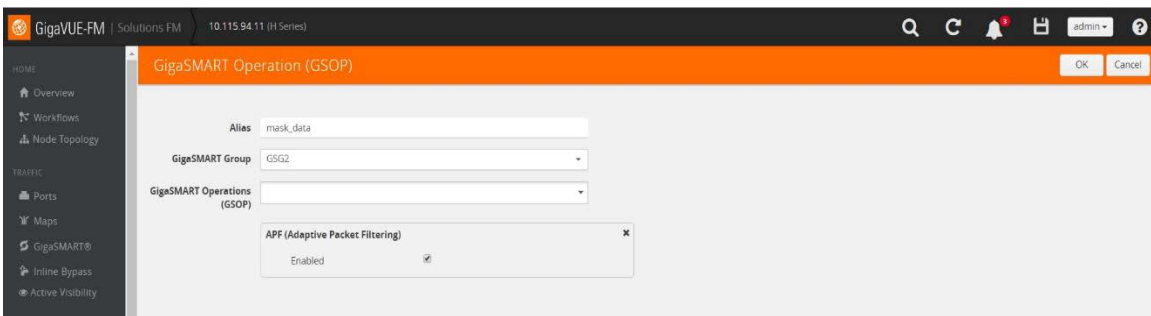   b. Provide details as illustrated below and click **OK**.

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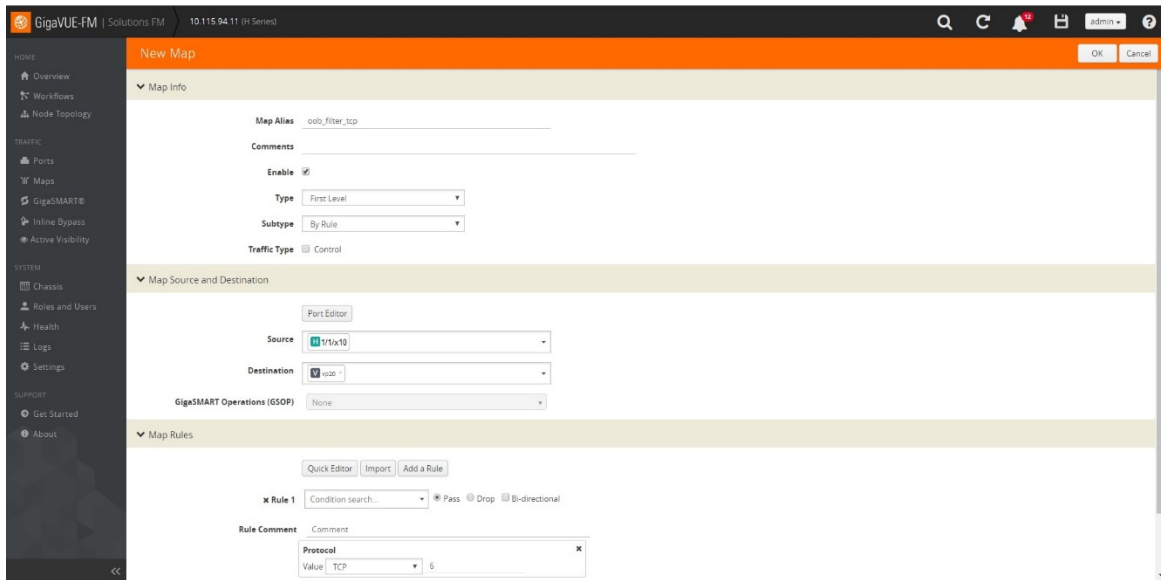
Figure 69   Configuring rule-based first-level map for filtering in intended traffic for masking.

8.   Configure regular shared collector map with the hybrid port and the tool port connected to the out-of-band 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**.
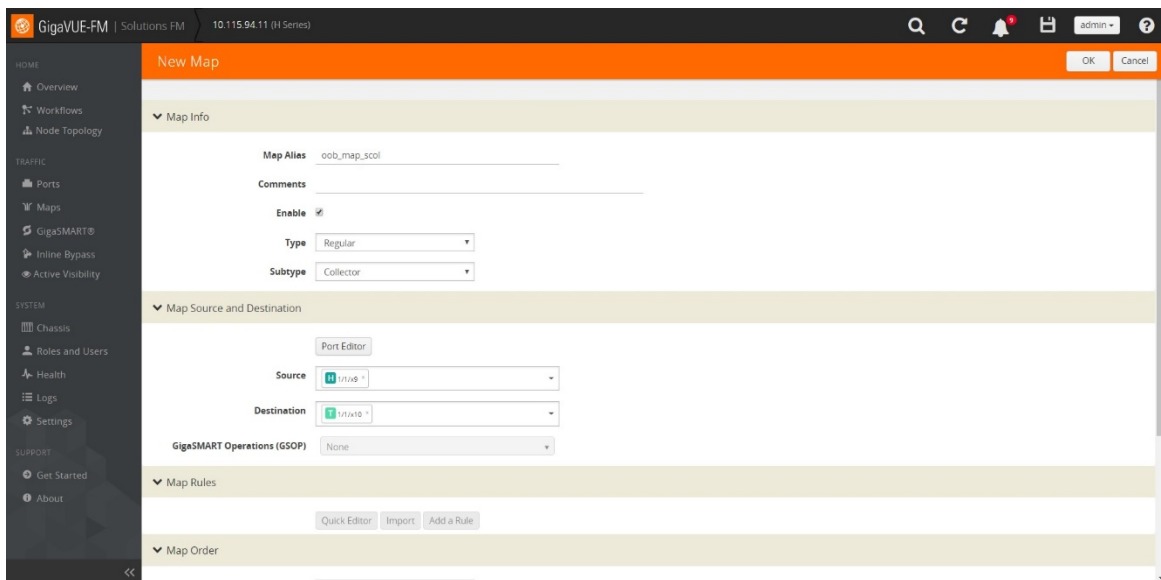

Figure 70   Configuring regular shared collector map.

9.   Configure rule-based Second Level map with the virtual port and the tool port connected to the out-of-band 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**.

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.

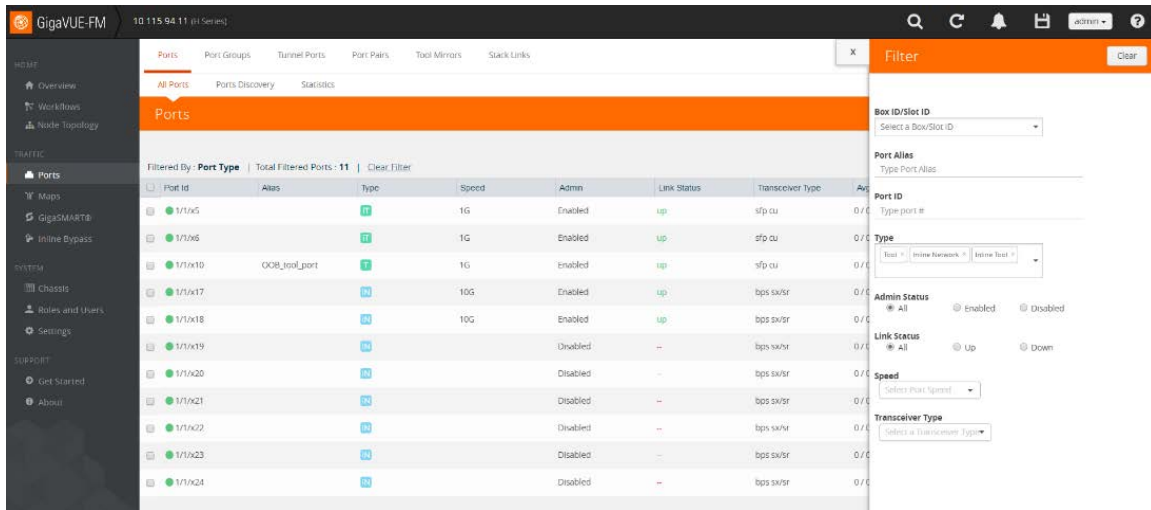3. All ports should be **Enabled** and their **Link Status** must be **Up**.

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".

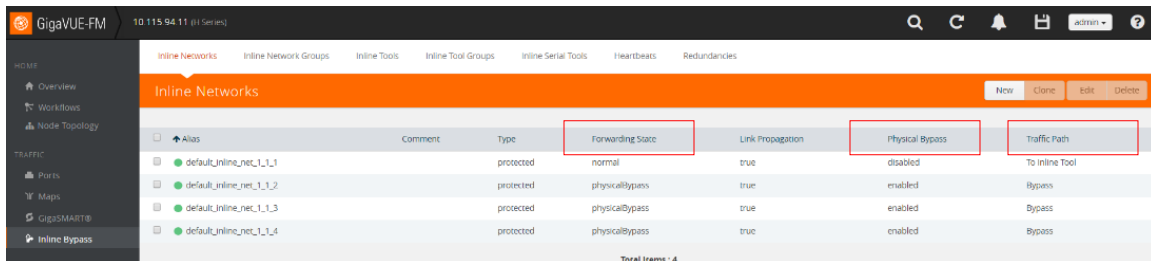*Figure 73   Viewing Inline Network status*

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.
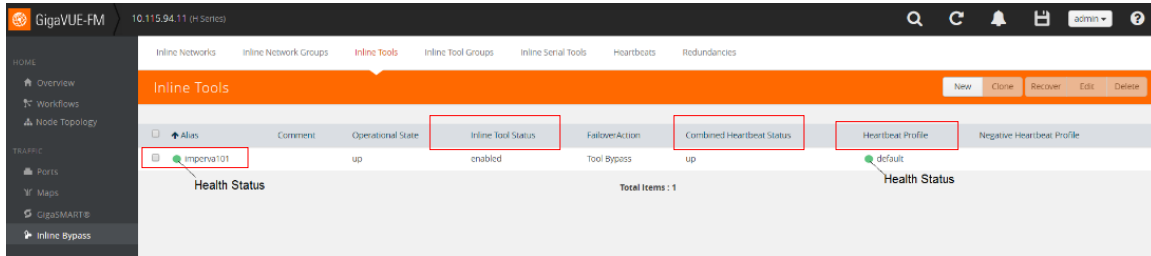

Figure 74   Viewing Inline Tool status

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.
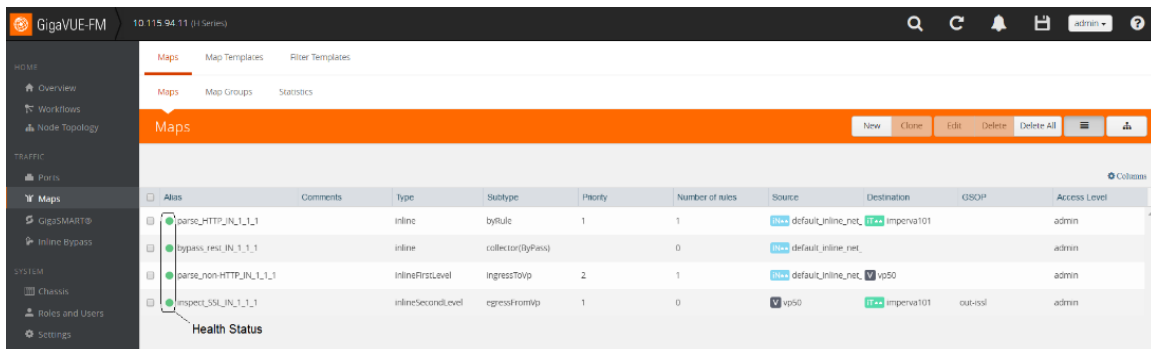

Figure 75   Viewing Maps status

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.
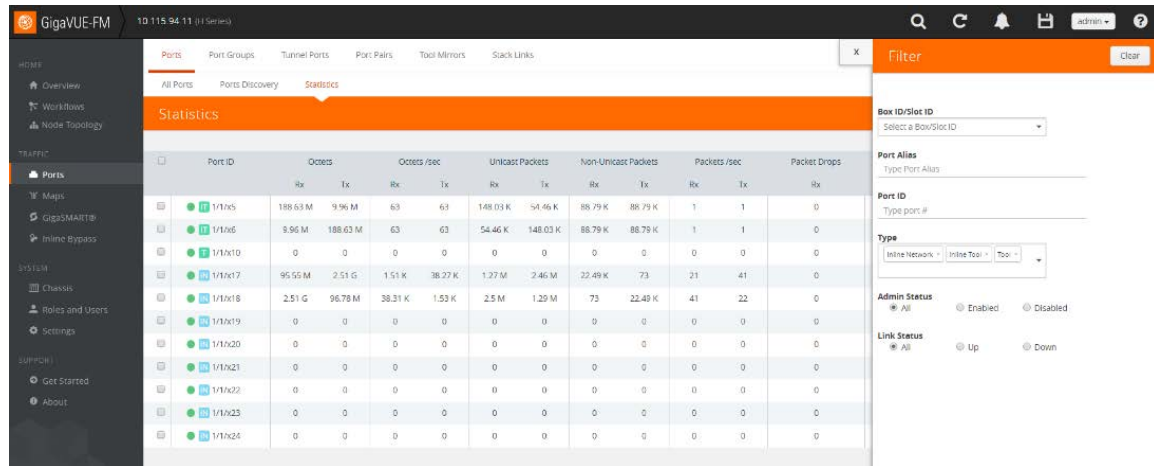

Figure 76   Viewing Ports statistics

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.
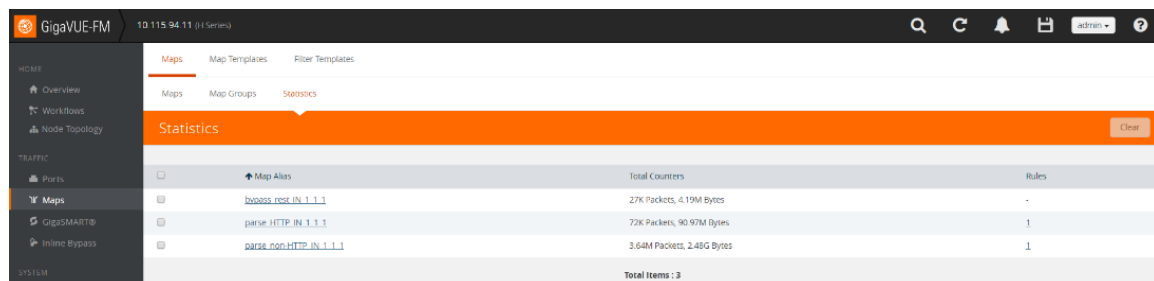

Figure 77   Viewing Map statistics

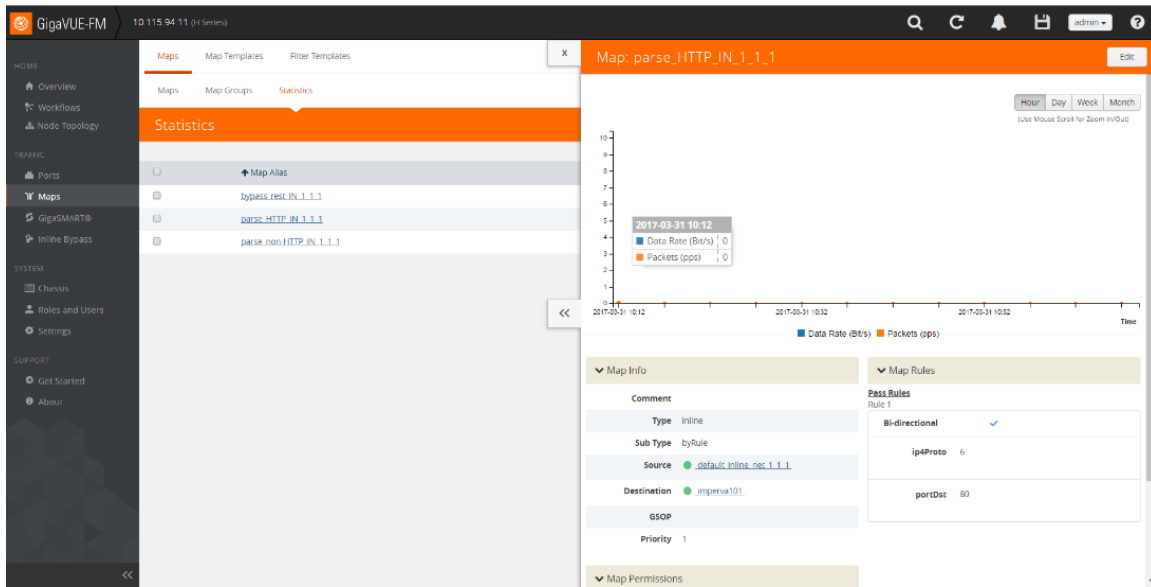2. Click on a map to check its trending statistics.

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**.
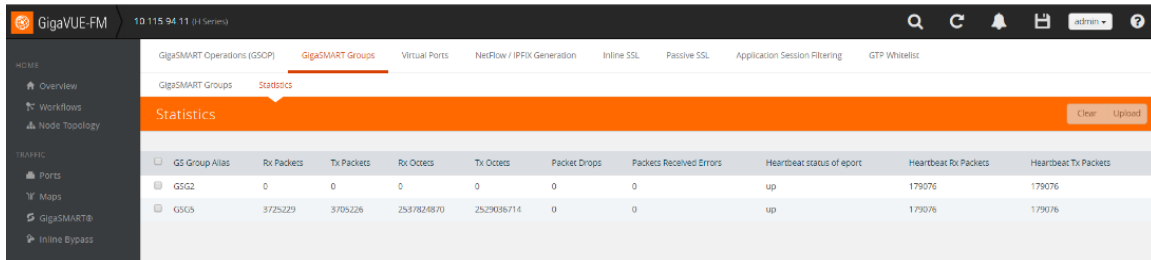

Figure 79   Viewing GigaSMART Group statistics

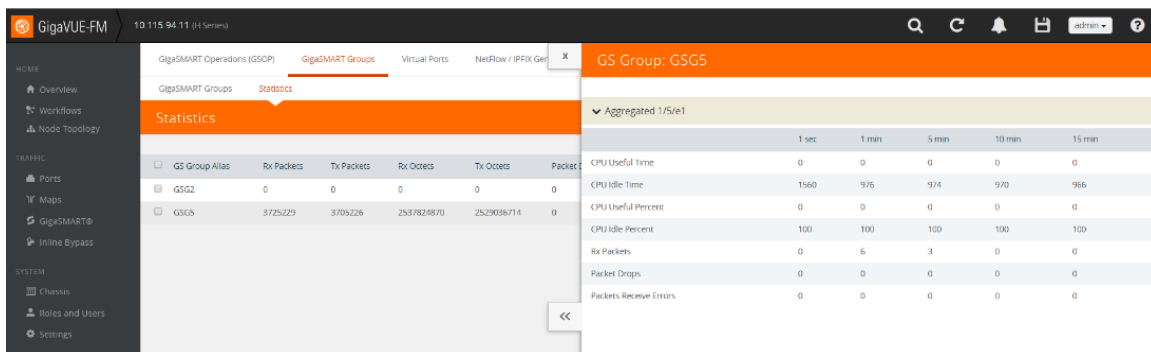2. Click the GigaSMART Group Alias name to view the historical statistics.

Figure 80   Viewing historical statistics of GigaSMART Group

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.

Figure 81   Viewing GigaSMART Operation statistics

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**.
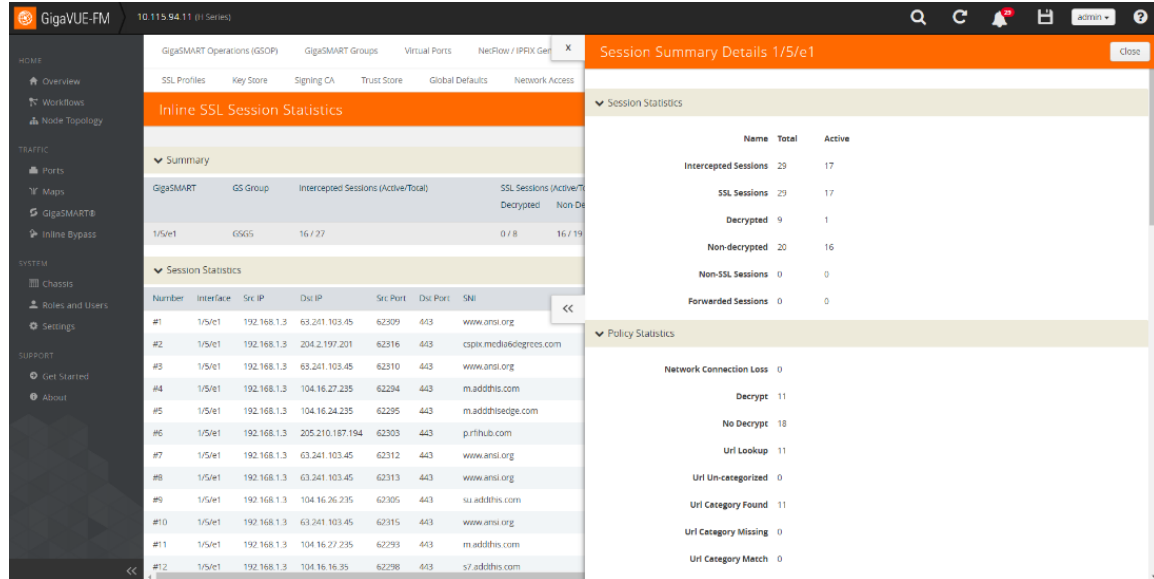

Figure 83   Viewing Inline SSL session summary
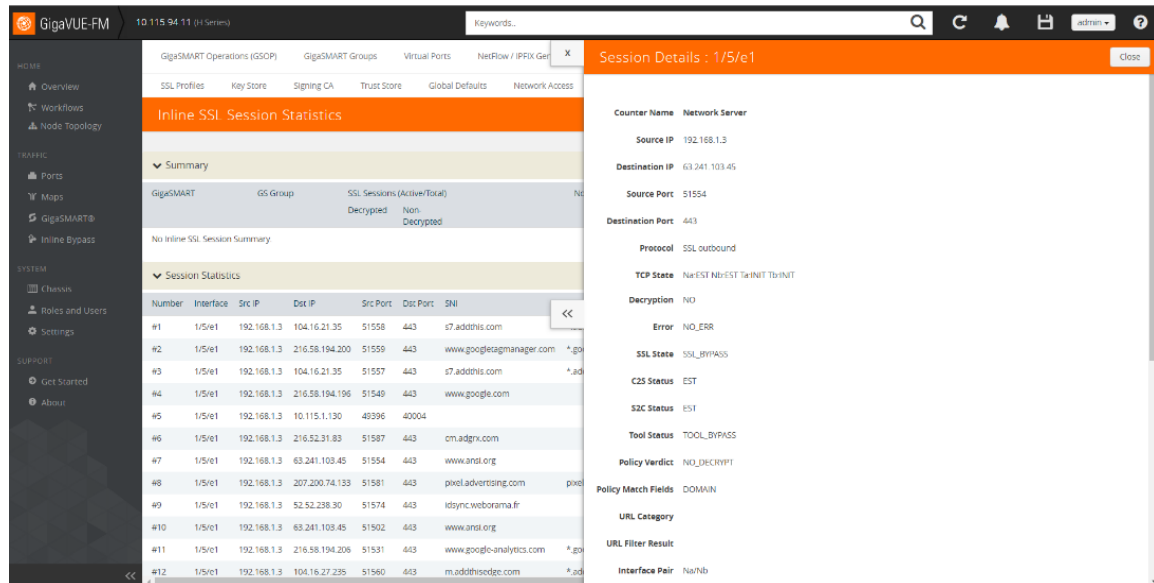
2. Click **Show Details** to view more details.

Figure 84   Viewing Inline SSL session detail statistics

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.
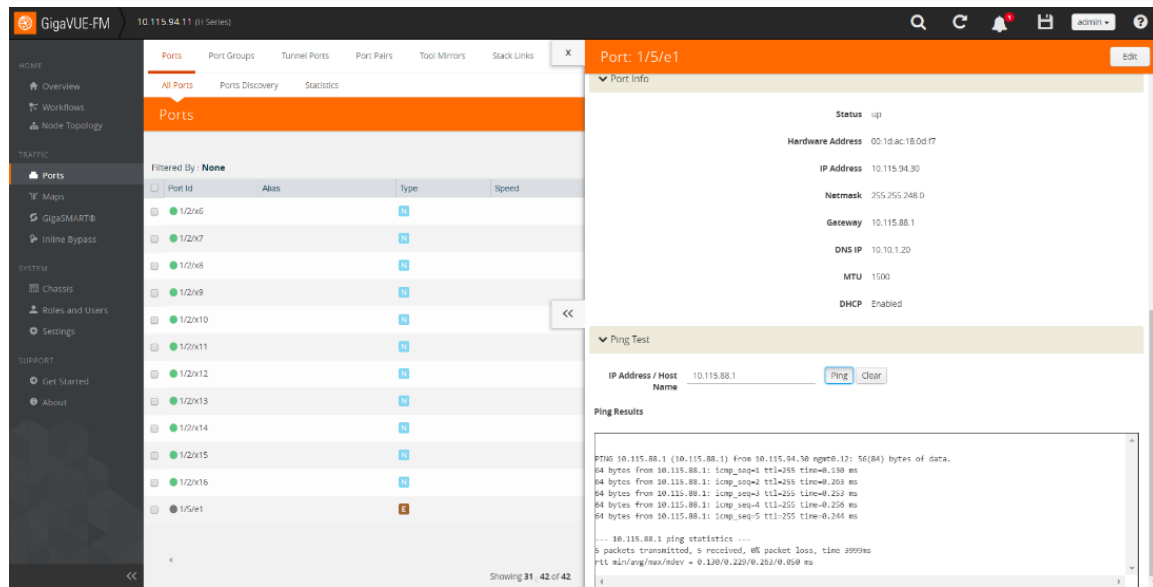
GigaSMART engine interface Quick View window

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 No-decrypt** 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 (1s/max/10ms
burst/limit)

        CPU usage               = 0 %/0 % (1s/5s)

        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
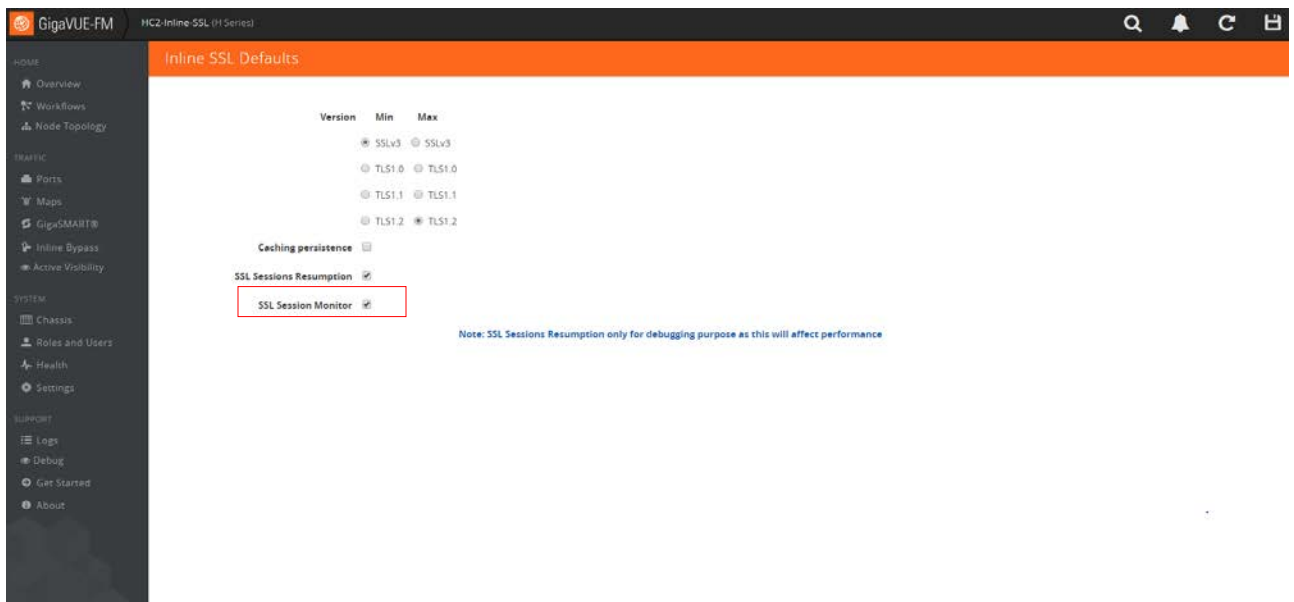- Totals SYN/SYNACK

Per session info

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

- VLAN ID used in the session

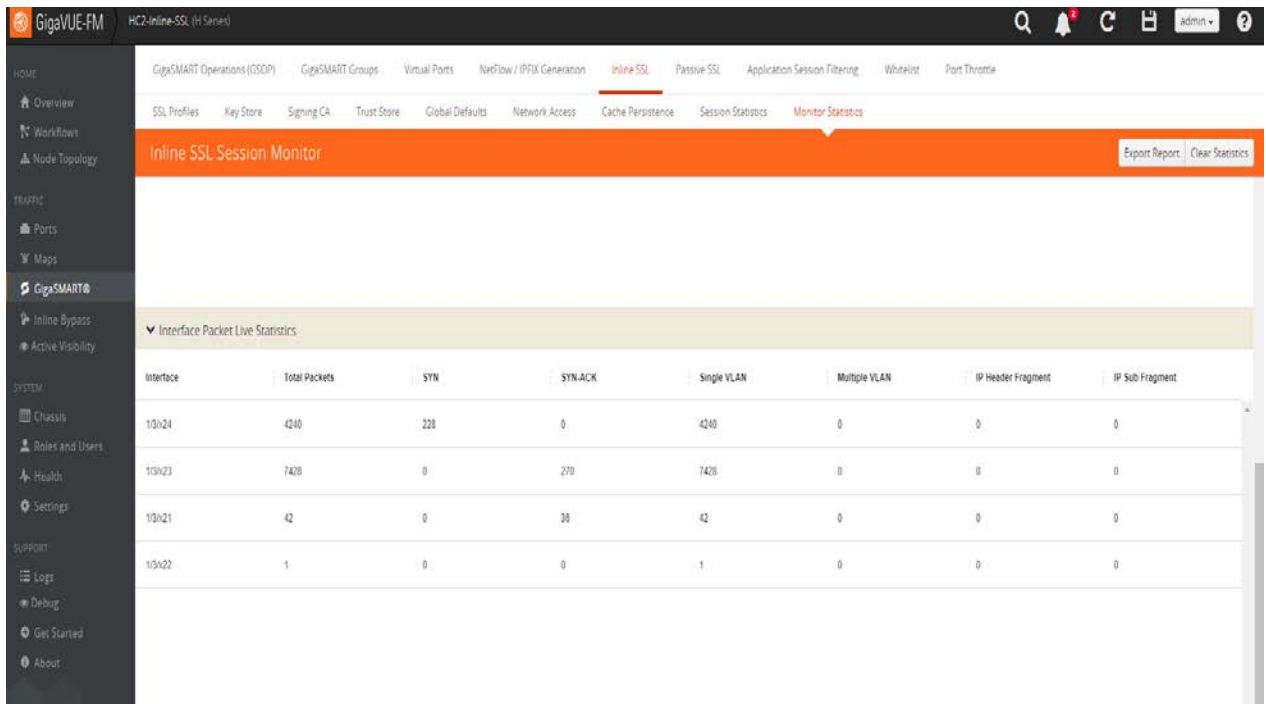- Network interface used in this session

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 → Navigate to GigaSMART → Inline Bypass → Global Defaults → check the checkbox on "Enable SSL session monitor".**

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

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> | l4port-src <sport> | l4port-dst <dport>`

See Inside Your Network™