



GigaVUE Inline Solutions Guide

GigaVUE-FM

Product Version: 6.13

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc.

Trademark Attributions

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

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.14	1.0	02/25/2026	The original release of this document with 6.14.00 GA.

Contents

GigaVUE Inline Solutions Guide	1
Change Notes	2
Contents	3
GigaVUE Inline Solutions	13
Software Constructs for Inline Solutions	13
Inline Network and Inline Network Ports	14
Physical Bypass Parameter	17
Resiliency Features	18
Network Port Link Status Propagation Parameter	18
Heartbeat Support Between GigaVUE Nodes	18
Heartbeats in a Multi-Layer Inline Topology	19
Display Current State of Inline Bypass Solution	20
IP Interface	25
Inline Network Link Aggregation Group (LAG)	25
Inline Network Link Aggregation Group— Rules and Notes	26
Inline Network Bundle	26
Inline Tool Ports and Inline Tools	27
Inline Tool Recovery Modes	28
Inline Tool Group	29
Inline Bypass Restriction	31
Forwarding	32
Failover	32
Out-of-Band and Inline Tools	33
Service Chaining of Decrypted Traffic	34
Packet Flows	34
Modules Matrix	36
Inline Single VLAN Tag	36
Flexible Inline Maps	37
Types of Flexible Inline Maps	38
Types of Inline Networks	39
Unprotected Inline Network	39

Resilient Inline Arrangement	40
Resilient Inline Arrangement— Classic	41
Resilient Inline Arrangement With Single VLAN Tag	41
Inter-broker Pathway (IB-P)	42
Resilient Inline Arrangement—Rules and Notes	43
Hardware Security Modules (HSM)	43
Why HSM	44
How HSM Solution Works	44
HSM - Supported Platforms	45
Internet Content Adaptation Protocol (ICAP)	45
How ICAP Solution works	46
ICAP - Supported Platforms	47
ICAP - Rules, Notes, and Limitations	47
ICAP - Supported GigaSMART Engine Ports	48
Gigamon Resiliency for Inline Protection	48
GRIP in Classic Inline Bypass	49
GRIP in Flexible Inline (Redundancy)	49
GRIP Scenarios	49
Traffic Flows Through Node with Primary Role	50
Traffic Flows Through Node with Secondary Role after Primary is Lost	50
Both Nodes Go Down and Only Secondary Comes Up	51
Both Nodes Fail; No Traffic Monitoring	51
Both Nodes are in Suspended State	52
How to Handle Recovery	52
How to Cable GigaVUE-FM,GigaVUE HC Series Nodes	53
Redundancy Profile	53
Rules and Notes	53
Limitations	54
Inline TLS/SSL Decryption	54
Why Decrypt TLS/SSL Traffic	54
Inline vs. Passive Decryption	55
How Inline TLS/SSL Decryption Works	55
Mutual TLS (mTLS) with Inline TLS/SSL Decryption	55
Privacy and Sensitive Data Handling	56
What Applications Use TLS/SSL	57
	57
Supportability and Compatibility for Inline TLS/SSL Decryption	57
Supported Platforms	57

Mutual TLS (mTLS) Support and Limitations	58
Supported platforms for mTLS	58
Limitations of mTLS functionality	58
GigaSMART Licensing	58
Inline Bypass Requirements	59
Port Requirements	60
GigaSMART Compatibility	60
Supported Ciphers	60
Post-Quantum Cryptography (PQC) Cipher Support	63
Supported Algorithms	63
Supported Key File Types	64
Limitations	64
Attributes of Inline TLS/SSL Decryption Solution	64
TLS/SSL Sessions	65
TLS/SSL Handshake	65
TLS/SSL Handshake Steps:	65
TCP Transition States during TLS/SSL Session	66
TLS/SSL Session Resumption	66
TLS/SSL Session Search	66
StartTLS and HTTP CONNECT	66
Behavior with StartTLS	67
TLS/SSL Keys and Certificates	67
Key Store	67
Trust Store	68
Client Trust Store (for mTLS)	68
Certificate Validation	68
Types of Certificate Validation Errors	69
Client Authentication	69
Client Authentication with mTLS enabled	69
Re-Signed Certificates	70
Certificate Revocation Status	70
Methods to Check Certificate Revocation Status	71
Policy Profile	71
Types of Policy Rules	72
Scale and Flexibility	72
Policy Evaluation	72
Network Phase	72
SNI Phase	73
Certificate Validation	73
Certificate Phase	74
Policy Profile Options	74
Inline TLS/SSL Decryption Port Map	74

Enable or Disable Tool Bypass	75
High Availability Active Standby	75
Inline Network Group Multiple Entry	76
Inline TLS/SSL – Multiple Entry Behavior	77
Tool Early Engage	77
One-Arm Mode	78
Failover Support	79
One-Arm Mode — Rules and Notes	79
Tool Early Inspect	80
Inline TLS/SSL L3 Tool NAT/PAT Support	81
HTTP 2.0 Downgrade	81
Decryption Port Mapping	82
Cache Server Certificate Timeout	82
Cache Persistence	83
GigaSMART Overload Bypass	83
CPU Overload Threshold	84
Inline TLS/SSL Monitor Mode	85
Inline TLS/SSL Traffic Filtering	85
No-decrypt Listing Policy	86
Decrypt Listing Policy	86
No-Decrypt/Decrypt List Policy — Rules and Notes	86
IP Address Subnet with Longest Prefix Match(LPM)	87
URL Categorization	87
URL Category Look-ups and Caching	88
Inline SSL URL categories	89
Proxy Server Profile for URL Categorization and Certificate Revocation status	95
Inline TLS/SSL Decryption Deployments	96
Inbound Deployment	96
Inbound Deployment with Client Certificate Authentication (mTLS) ...	96
Outbound Deployment	97
Basic Deployments for Inline TLS/SSL Decryption Solution	98
Inline TLS/SSL Decryption Solution with Layer 2 Transparent Tools	98
Rules and Notes	100
Inline TLS/SSL Decryption Solution with Layer 3 Tools (NAT-PAT)	101
Architecture of an L3 Tool based Inline TLS/SSL Decryption Solution ...	102
Rules and Notes	102

Differences Between Layer 2 and Layer 3 Tools	
Deployments	104
Advanced Features for Inline TLS/SSL Decryption	
Solution	104
Inline TLS/SSL Decryption Solution with RIA	104
Symmetric Traffic in RIA	106
Asymmetric Traffic in RIA	106
VLAN Tagging Behavior for Decrypted Traffic	108
VLAN Tagging Behavior for Non-Decrypted Traffic	108
Entrust nShield and Thales- Luna HSM for TLS/SSL	
Decryption for iSSL	109
HSM - Supported Solutions	110
HSM Configuration Rules, Notes, and Limitations	110
Inline TLS/SSL Decryption Solution with ICAP Client	111
ICAP - Limitations	112
TLS/SSL Terminology and Acronyms	113
Inline Solutions Configuration Using Flexible Inline	
Arrangement Canvas	114
What is a Flexible Inline Arrangement	115
Flexible Inline Maps	116
Types of Flexible Inline Maps	117
Supported Platforms, License, and Software Version	118
Flexible Inline Solution Supported in Clustered Nodes	119
Limitations	120

Flexible Inline TLS/SSL Decryption Solution—Rules and Notes	120
Configure Software Constructs Using Flexible Inline Arrangement Canvas	122
Configure Inline Network Ports and an Inline Network	122
Configure IP Interface	123
Configure Inline Network LAG	124
Configure Inline Network Bundle	126
Configure Inline Tool Ports and Inline Tools	127
Configure Inline Tool Group	129
Configure Inline Single VLAN Tag	132
Configure Flexible Inline Maps	134
Configure Resilient Inline Arrangement Solution	135
Create Inter-broker Pathway	135
Configure Resilient Inline Arrangement	137
Configure ICAP Client	139
ICAP Client—Field References	141
Configure GRIP Solution	142
Configure Synchronization	142
Example: Gigamon Resiliency for Inline Protection	143
Redundancy Control State	147
How to Use Suspended Role for Maintenance	147
How to Upgrade GigaVUE Nodes in GRIP Deployment	148
Troubleshoot	149
Signaling Ports Down	149
Traffic outage in Inline Tool	149
Network Traffic Outage	149
Configure TLS/SSL Decryption Solutions	150
Inline SSL App—Field References	150
Configure Inline TLS/SSL Decryption Solution with Layer 2 Tools	157
Prerequisites	157
Access Flexible Inline Canvas	157
Configure Inline Network	157
Configure Inline Tool	158
Create an Inline SSL APP	159
Deploy Inline TLS/SSL Decryption Solution	160
Verify the Solution	160

What to Do Next	160
Configure Inline TLS/SSL Decryption Solution with Layer 3 Tools	161
Prerequisites	161
Access Flexible Inline Canvas	161
Configure Inline Network	161
Configure Inline Network Bundle	162
Configure Inline Tool	162
Create an Inline SSL APP	163
Deploy Inline TLS/SSL Decryption Solution	164
Verify the Solution	164
What to Do Next	165
Configure Inbound mTLS for Inline TLS/SSL Decryption ..	165
Prerequisites	165
Create a Client Trust store	165
Access Flexible Inline Canvas	165
Create an Inline SSL APP	165
Deploy the solution	167
Verify the Solution	167
What to Do Next	167
Configure Inline TLS/SSL Decryption Solution with RIA ..	168
Prerequisites	168
Access Flexible Inline Canvas	168
Configure Inline Network	168
Configure Inline Tool	169
Create Inter-broker Pathway	170
Configure Resilient Inline Arrangement	170
Create an Inline SSL APP	172
Deploy Inline TLS/SSL Decryption Solution	173
Verify the Solution	174
What to Do Next	174
Configure Thales-Luna HSM for TLS/SSL Decryption	174
Prerequisites	174
Access Flexible Inline Canvas	175
Configure Inline Network	175
Configure Inline Tool	175
Create HSM Group	176
Add Thales -Luna HSM Appliance to the HSM Group	177
Create an Inline SSL APP and Attach the HSM Group	178
Deploy the Inline SSL Solution	180
Register GigaSMART Engine on Thales Luna HSM Server	181

Verify the Solution	181
What to Do Next	182
Modify an HSM Deployment for Inline TLS/SSL	
Decryption	182
Configure ICAP Client for Inline TLS/SSL Decryption	
Solution	183
Prerequisites	183
Access Flexible Inline Canvas	183
Configure Inline Network	183
Configure Inline Tool	184
Configure IP Interface	185
Configure ICAP Client	185
Create an Inline SSL APP	186
Deploy the Inline SSL Solution	187
Verify the Solution	188
What to Do Next	189
View Inline Solution Status and Statistics	189
View Inline Solution Status	189
Rules and Notes	190
View the Forwarding States of Inline Networks	191
View Inline TLS/SSL Session Statistics	197
View Inline TLS/SSL Monitor Statistics	198
View Inline TLS/SSL Certificate Statistics	200
View HSM Statistics	201
View ICAP Statistics	202
View Inline TLS/SSL Dashboards	204
Access TLS/SSL Dashboards	204
Basic Dashboards	205
Advanced Dashboards	208
System Requirements to configure Inline TLS/SSL Advanced	
Dashboards	208
Rules and Notes	209
Configure Advanced dashboard	209
View Advanced Dashboards	210
	211
Import and Export Flexible Inline Solution — Rules and Notes	212
Import and Export a Flexible Inline Solution	212
Backup and Restore Flexible Inline Flows	213
Troubleshoot Inline TLS/SSL Decryption Solution Issues	213
Example: Troubleshoot Traffic Issues Between Side A and Side B	214

Inline Configurations using Inline Bypass Solutions	
(Classic)	215
Inline Bypass Solutions	215
Introduction to Inline Bypass Solutions	216
Capabilities of Inline Bypass Solutions	216
Logical Bypass and Physical Bypass	217
Simple and Complex Inline Bypass Solutions	219
Typical Configuration	220
Distribution to Multiple Inline Tools	220
Inline Tools in a Series	221
Multiple Inline Networks	222
Inline Flow Mapping®	223
Send Traffic to Out-of-Band Tools	224
Types of Inline Networks	224
Unprotected Inline Network	224
Inline Network Groups	225
Inline Tool Sharing	226
Configurable VLAN Tagging	227
Add VLAN Tag	227
Tools in Bridge Mode	227
Inline Tools	228
Inline Tool Failover Action	229
Inline Tool Failover Action with Inline Flow Mapping®	230
Inline Tool Recovery Mode	230
Inline Tool Sharing Mode	232
How to Use SNMP Polling to Obtain Inline Tool State	233
Heartbeats	233
Rules and Notes	234
Heartbeat Profiles	234
Standard Heartbeat	236
Standard or Custom Heartbeat Packet	236
Detect Inline Tool Failure	236
Negative Heartbeat Profiles	237
Heartbeat Support Between GigaVUE Nodes	238
Troubleshoot Heartbeat Failures	240
Configure a Heartbeat Profile	240
View Heartbeat Profile Statistics	241
Heartbeat Status after System Reload	242

Inline Tool Groups	242
Inline Tool Group Failover Action	245
Inline Tool Group Spare Inline Tool	246
Symmetrical and Asymmetrical Hashing	246
Asymmetrical Hashing Restrictions	248
Resilient Weighted Hashing	249
Inline Serial Tools	249
Inline Serial Tools Global Failover Action	252
Inline Tool Series Local Failover Action	254
Inline Tool Series Per-Direction Order	256
Associate Inline Networks with Inline Tools Using Inline Maps	258
Inline Map Passall	259
Inline Map	259
Inline Map Shared Collector	260
Inline Maps to Individual Members of an Inline Tool Group	260
Map, Inline Tool, and Inline Tool Group Configuration Restrictions	262
Inline Tool Failures and Failover Actions	263
Maps That May Lead to Selective Traffic Drops	264
Out-of-Band (OOB) Map	264
Symmetric and Asymmetric Maps	266
Configure Inline Bypass	266
Configuration Step Details	267
Configure Inline Network Ports	267
Configure Inline Network (Unprotected)	268
Configure Inline Network Group	268
Create Heartbeat Profile	269
Create Negative Heartbeat Profile	270
Configure Inline Tool Ports	271
Configure Inline Tool	271
Create Inline Tool Group	272
Configure Inline Tool Series	273
Configure When GigaVUE-FM,GigaVUE HC Series® HC Series Modules are Operationally Up	274
Avoid Over subscription	274
Inline Bypass Solution Examples	275
Example 1: Unprotected Inline Bypass with an Inline Tool Group	275
Example 2: Unprotected Inline Bypass with Default Heartbeat	277
Example 3: Protected Inline Bypass Using Combo Modules	279
Glossary	282

GigaVUE Inline Solutions

A GigaVUE inline solution refers to network configuration where a GigaVUE node is placed directly in the data path ("inline") between two network segments, allowing it to capture and analyze live network traffic while simultaneously directing traffic to security tools like firewalls or intrusion prevention systems (IPS) for inspection, all while maintaining network connectivity and minimizing disruption; essentially acting as a "traffic broker" for inline security tools with fail-safe bypass capabilities in case the security appliance fails.

The various solutions are:

- [Resilient Inline Arrangement](#) - Resilient inline arrangement is a method of configuring and deploying inline threat prevention tools for dual-path, redundant network architectures
- [Hardware Security Modules \(HSM\)](#) - Hardware Security Modules (HSMs) with its Inline SSL (iSSL) decryption solution enhances the security and management of cryptographic keys used for decrypting SSL/TLS traffic.
- [Internet Content Adaptation Protocol \(ICAP\)](#) - The ICAP protocol, integrates with DLP systems for enhanced security by allowing inline inspection of decrypted TLS/SSL traffic.
- [Gigamon Resiliency for Inline Protection](#) - GRIP is an Inline Bypass solution that connects two GigaVUE-FM, GigaVUE HC Series nodes together so that one node provides high availability to the other node when there is a loss of power. This redundant arrangement of two GigaVUE-FM, GigaVUE HC Series nodes maintains traffic monitoring by inline tools when one of the nodes is down.
- [Inline TLS/SSL Decryption](#) - Inline TLS/SSL decryption detects, intercepts, filters, decrypts, analyzes, and re-encrypts encrypted traffic for security purposes. The various Inline TLS/SSL Decryption solutions are as follows:
 - [Inline TLS/SSL Decryption Solution with Layer 2 Transparent Tools](#)
 - [Inline TLS/SSL Decryption Solution with Layer 3 Tools \(NAT-PAT\)](#)
 - [Inline TLS/SSL Decryption Solution with RIA](#)
 - [Entrust nShield and Thales- Luna HSM for TLS/SSL Decryption for iSSL](#)
 - [Inline TLS/SSL Decryption Solution with ICAP Client](#)

Software Constructs for Inline Solutions

In Gigamon Inline solutions, a software construct is a configuration element that helps manage network traffic. These constructs include things like inline networks, inline tools, inline tool groups, and inline network groups. They are not physical devices; rather, they

represent logical groupings of ports and tools that dictate how traffic is processed and inspected within the system.

For instance, an "inline tool" is formed by a pair of ports, along with the inline tool connected to those ports. This setup is configured on the GigaVUE HC Series node and includes specific attributes. An "inline network" consists of two network ports designed for inline monitoring.

Administrators can configure these constructs via a management interface or command-line interface (CLI). They play a crucial role in creating and managing inline bypass and other flexible arrangements within Gigamon deployments. These constructs allow for the definition of traffic flows, inspection policies, and failover behaviors, independent of the actual physical hardware in use.

Below is the list of software components used in Gigamon Inline solutions:

- [Inline Network and Inline Network Ports](#)
- [IP Interface](#)
- [Inline Network Link Aggregation Group \(LAG\)](#)
- [Inline Network Bundle](#)
- [Inline Tool Ports and Inline Tools](#)
- [Inline Tool Group](#)
- [Inline Single VLAN Tag](#)

Inline Network and Inline Network Ports

An inline network forms a logical connection between two inline network ports—Port A and Port B—that carry live production traffic. These ports operate at the same speed, use the same medium (fiber or copper), and reside on the same node. Traffic entering one port exits through the other, enabling packets to be inspected or modified by inline tools without disrupting service.

Inline networks can be configured as protected or unprotected, depending on whether failover protection is required:

- *Protected* inline networks provide high availability by automatically redirecting traffic through a bypass path if a tool or link fails.
- *Unprotected* inline networks do not offer automatic failover; traffic stops if a link or tool fails until manual intervention restores service.
- *Mixed* inline networks is a combination of protected and unprotected inline networks supported in Inline Bypass solutions (Classic).

When an inline network connects directly to inline tools, traffic continues to flow based on the configured failover action.

- **Drop**—All traffic through the inline network is stopped. No packets are exchanged between the inline network ports or with the inline tools. Traffic entering Port A or Port B is dropped.

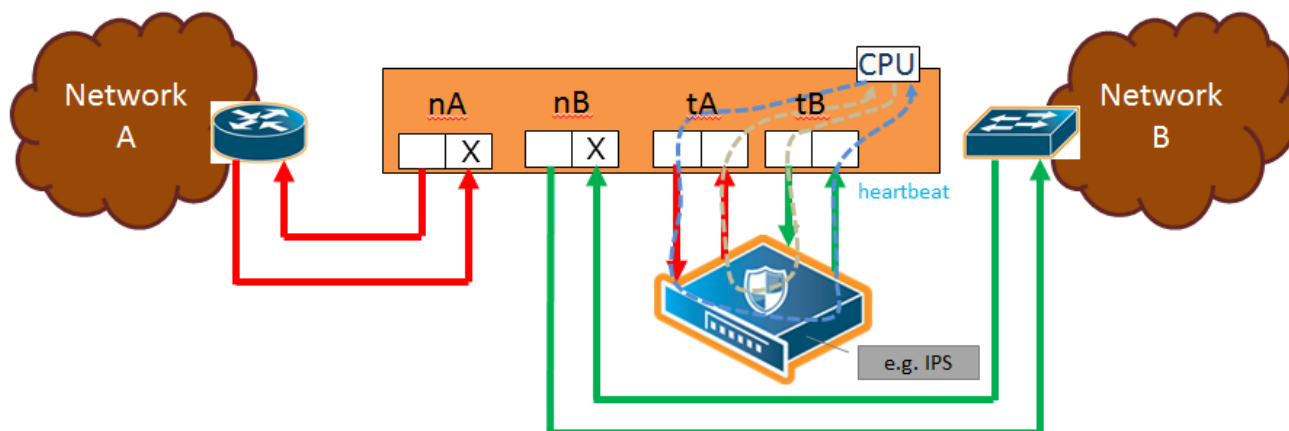


Figure 1 Traffic Path of Drop

- **ByPass**—Traffic is forwarded directly between the inline network ports, depending on how inline maps are configured:
 - **No maps or pass-all maps:** All traffic entering Port A is forwarded to Port B, and traffic entering Port B is forwarded to Port A through a logical bypass.
 - **Maps with drop conditions:** Only traffic that would have been forwarded in To Inline Tool mode is passed through. Packets that were dropped in that mode remain dropped here as well.

In both cases, no traffic is sent to the inline tools.

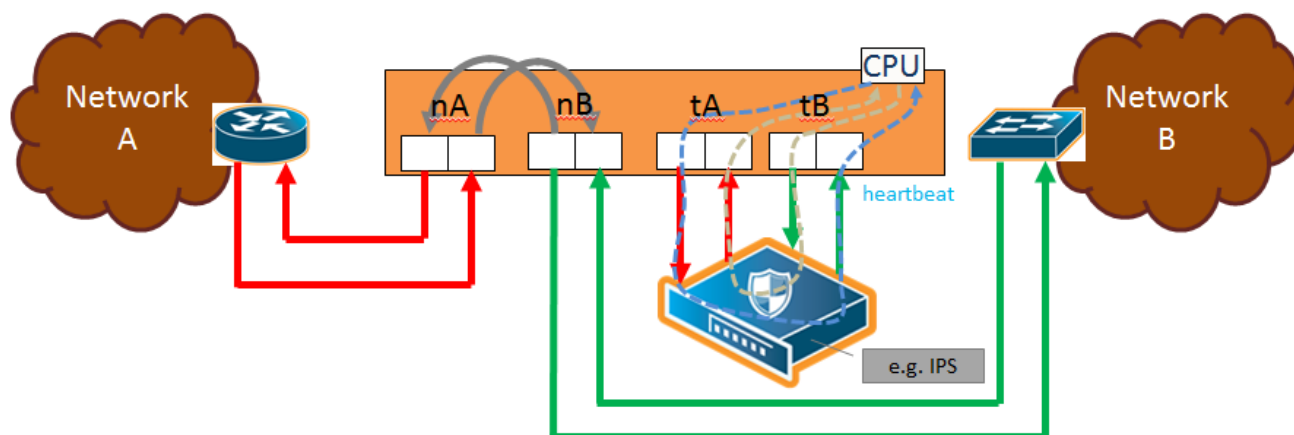


Figure 2 Traffic Path of Bypass

- **ByPass with Monitoring**—This mode behaves like standard bypass but also sends a copy of the traffic to the inline tools:
 - **No maps or pass-all maps:** All traffic is forwarded as in bypass mode, while a copy is sent to the inline tools for monitoring.
 - **Maps with drop conditions:** Only traffic that would not have been dropped in To Inline Tool mode is forwarded and copied for monitoring.

In both monitoring cases, no packets are received from the inline tools.

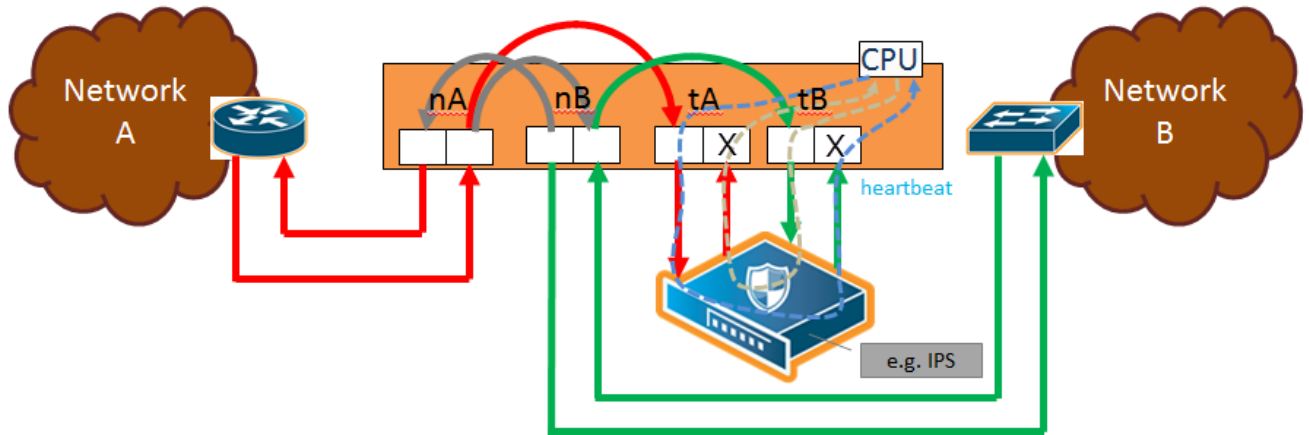


Figure 3 Traffic Path of Monitoring

- **To Inline Tool**—traffic received at the inline network ports is forwarded according to the following factors:
 - the configured maps between the inline network and the inline tools
 - the failover actions of the inline tool or tools
 - the health state of the inline tool or tools

The default is **Bypass**. This avoids any traffic loss when first configuring an unprotected inline network or when disabling physical bypass on a protected inline network.

Figure 1Traffic Path of Drop to Figure 4Traffic Path of To-Inline-Tool show the traffic path for a simple inline bypass solution with inline network ports (nA and nB), inline tool ports (tA and tB), and a map passall.

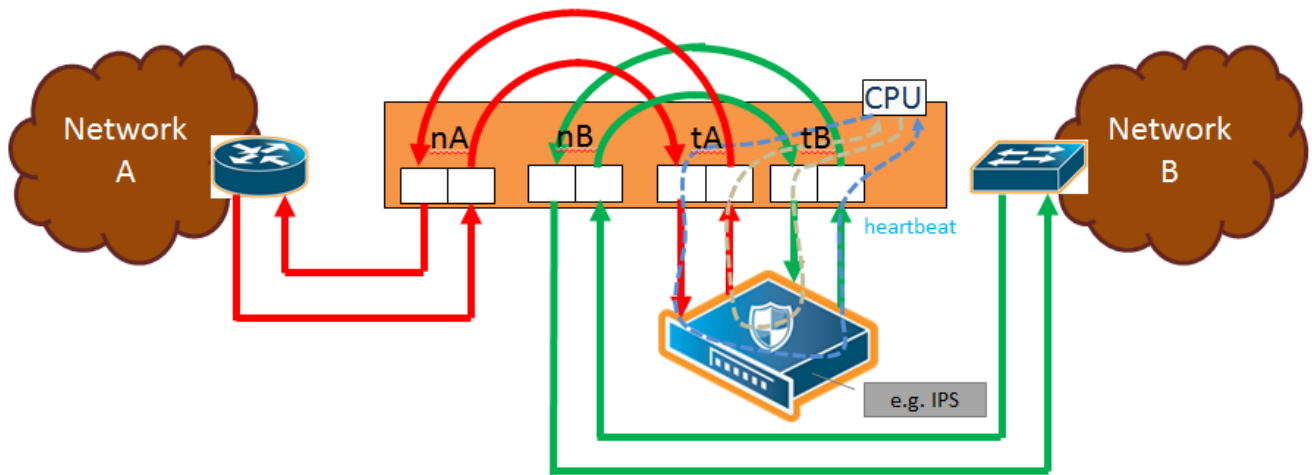


Figure 4 Traffic Path of To-Inline-Tool

Physical Bypass Parameter

One of the parameters of inline networks is physical bypass, which controls the state of the optical protection switch on the bypass combo module or copper TAP module when the module is powered on. The optical protection switch can have one of the following states:

- close—the fiber connected to the side A network port is passively coupled with the fiber connected to the side B port without any transceivers or switching fabric. Therefore, any traffic coming in on these fibers is exchanged between the two inline network ports without being noticed by the system.
- open—the fiber connected to the inline network ports is coupled through transceivers with the switching fabric that is under software control. Therefore, 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.

When the bypass combo module or copper TAP modules is powered off, the optical protection switch is always in the close state.

When the bypass combo module or copper TAP modules is powered on, the state of the optical protection switch is as follows:

- the close state if **Physical Bypass** is set to enable (that is, selected on the configuration page)
- the open state if physical bypass is set to disable (that is, not selected on the configuration page)

Physical Bypass is enabled by default.

NOTE: Physical bypass only applies to protected inline networks.

Resiliency Features

Inline Networks include resiliency mechanisms to handle failures gracefully:

Network Port Link Status Propagation Parameter

Link status propagation controls how the link state is handled for inline network ports. It is enabled by default.

- When enabled, if one side of the inline network fails, the failure is also applied to the other side. For example, if traffic stops on one port and cannot reach the inline tools, the opposite port is also marked down.
- When the original link comes back up, the opposite side is restored as well.
- The node will not forward packets to inline tools until both sides of the link are active.

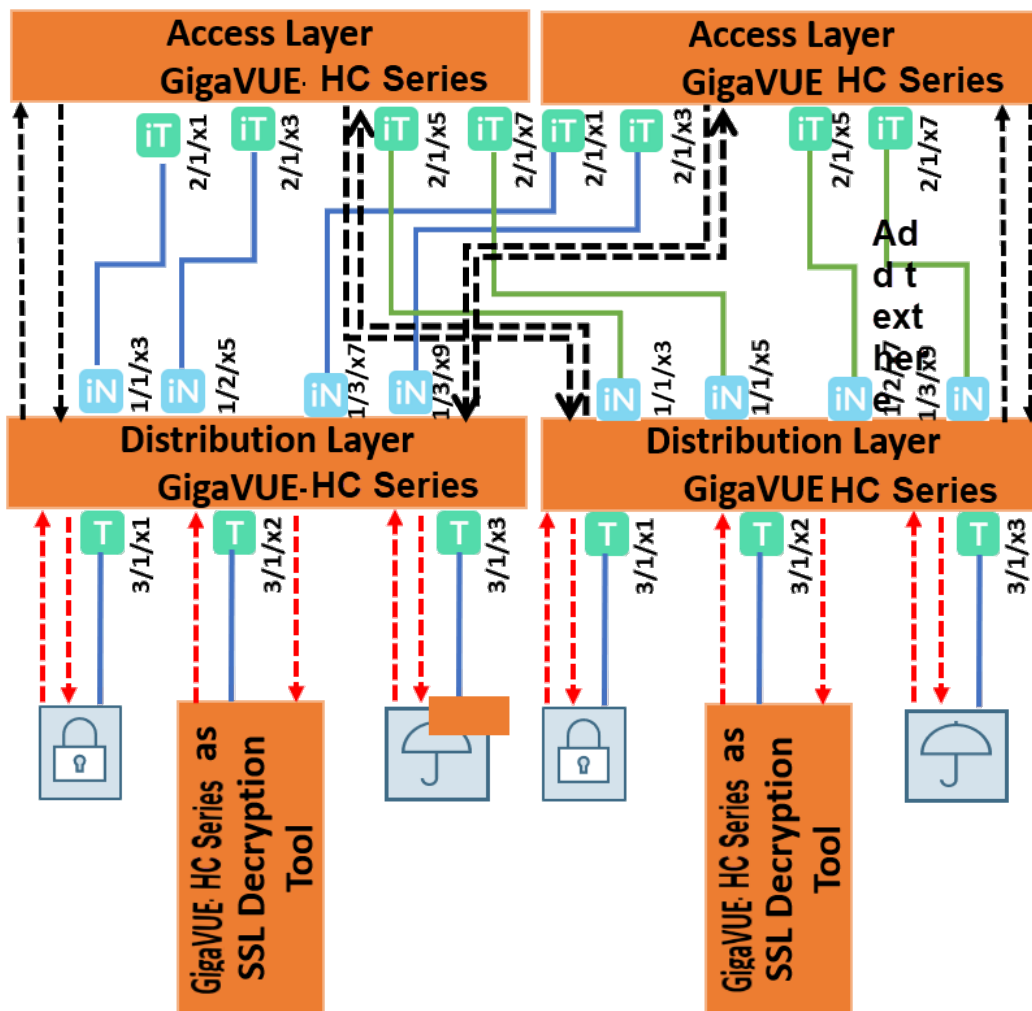
You can enable or disable this feature by selecting **Link Failure Propagation** when configuring an inline network port.

Heartbeat Support Between GigaVUE Nodes

Heartbeat packets are lightweight health-check signals exchanged between inline nodes and inline tools. They verify that traffic flows correctly through the inline path. If heartbeats stop, the system assumes a failure and automatically switches traffic to bypass mode, preventing packet loss.

When heartbeats resume, traffic again passes through the inline tools. This feature quickly detects tool or link failures and protects live traffic.

Following figure illustrates an example of a topology with GigaVUE nodes placed at three different layers.



-----> Heartbeat (Access Layer -> Distribution Layer -> Access Layer)

-----> Heartbeat (Distribution Layer -> Tool -> Distribution Layer)

——— Traffic

GigaVUE HC Series means it can be either GigaVUE-HC3, GigaVUE-HC1 or GigaVUE-HC1-PLUS

Heartbeats in a Multi-Layer Inline Topology

In a multi-layer setup, heartbeat packets help maintain traffic integrity and support automatic failover.

- The access layer node captures live traffic, sends it to the tool layer for processing, and then returns it to the network.
- The distribution layer node sits between the access and tool layers, distributing and managing traffic flows.

In this example, the tool layer node performs TLS/SSL decryption. Heartbeats monitor link health between each layer.

At the access layer, ports facing the distribution layer are configured as inline tool ports. At the distribution layer, ports facing the access layer are configured as inline network ports.

Heartbeat packets flow from the inline tool port pair (access layer) to the inline network port pair (distribution layer). If the distribution layer is in a healthy forwarding state, the heartbeat is returned; otherwise, it is dropped to signal a fault. The same principle applies between the distribution and tool layers.

Here, the distribution layer ports facing the tool layer are inline tool ports, while the tool layer ports facing back are inline network ports.

Heartbeats confirm the availability of both the tool devices and their processing engines.

Display Current State of Inline Bypass Solution

Inline networks, inline tools, and inline maps work together to form an inline bypass solution. The inline bypass solution has an overall state, which can change in response to hardware conditions and user configuration.

Several factors make up the overall state of an inline bypass solution, as follows:

- The physical bypass configuration of the inline network is protected.
- The inline network configuration, in particular, if physical bypass is enabled or disabled, what traffic path is configured, and if link failure propagation is enabled or disabled.
- The inline tool configuration, in particular, if the state of the inline tool is enabled or disabled, if there is a heartbeat profile configured and if the heartbeat is enabled or disabled, and what failover actions are configured.
- The inline tool group configuration, in particular, if the state of the inline tool group is enabled or disabled, what failover mode is configured, what failover action is configured, and what number of minimum healthy tools is configured.
- The status of the links attached to the inline network ports and inline tool ports.

[Forwarding States and Determining Factors](#) describes each forwarding state and the factors determining that state.

Whenever link failure propagation is configured as false (disabled), the inline network port status reflects the status of the respective far-end ports. Only when link failure propagation is configured as true (enabled) does this behavior change. Refer to the note under the Forwarding states for DISABLED and DISCONNECTED in [Forwarding States and Determining Factors](#).

Table 1: Forwarding States and Determining Factors

physical-bypass	traffic-path	Status of far-end ports connected to inline network ports	Status of inline tool side	Description
enable	drop, bypass, monitoring, or to-inline-tool	any status	any status	Forwarding state—PHYSICAL BYPASS If physical bypass is enabled, all traffic is exchanged directly between side A network and side B network without any monitoring by the GigaVUE-FM, GigaVUE HC Series node. Only applies to protected inline networks.
disable	drop	any status	any status	Forwarding state—DISABLED If the inline network is configured with a traffic path of drop, no traffic is exchanged between side A network and side B network because all packets coming to the inline network ports are dropped. Note: If the inline network is configured with link failure propagation set to true (enabled), the status of the inline network ports will be determined by the status of the far-end ports connected to the inline network ports. If both far-end ports are up, then both inline network ports will be up. If any far-end ports are down, then both inline network ports will be down.
disable	bypass, monitoring, or to-inline-tool	at least one far-end port is down	any status	Forwarding state—DISCONNECTED When one of the inline network ports is down due to a link down caused by a far-end device, no traffic is exchanged between side A network

physical-bypass	traffic-path	Status of far-end ports connected to inline network ports	Status of inline tool side	Description
				and side B network. Note: If the inline network is configured with link failure propagation enable as true, the status of both inline network ports will be down. That is, if only one inline network port is down, the other will be brought down.
disable	bypass	both far-end ports are up	any status	Forwarding state—FORCED BYPASS If the inline network is configured with a traffic path of bypass, all traffic that would not have been dropped when the traffic path is set to to-inline-tool is exchanged directly between side A network and side B network through the switching fabric.
disable	monitoring	both far-end ports are up	any status	Forwarding state—FORCED BYPASS WITH MONITORING If the inline network is configured with a traffic path of monitoring, all traffic that would not have been dropped when the traffic path is set to to-inline-tool is exchanged directly between side A network and side B network through the switching fabric. If there is any inline map configured for the inline network, a copy of the respective traffic is directed to the respective inline tools according to the configured inline maps.
disable	to-inline-tool	both far-end ports are up	all inline tools involved in the inline bypass solution are operating as expected	Forwarding state—NORMAL If all inline tools involved in the inline bypass solution are enabled, all inline tool ports are up, and the inline tools operating with heartbeat protocol enabled have a heartbeat status of up, traffic flows as desired according to the configuration of the inline maps.

physical-bypass	traffic-path	Status of far-end ports connected to inline network ports	Status of inline tool side	Description
				Note: If there are no inline maps, setting the traffic path of a protected fiber inline network to to-inline-tool results in a NORMAL forwarding state, but the traffic sent to the source inline network ports will be dropped because there are no inline maps specifying destination tool ports to which to forward the traffic.
disable	to-inline-tool	both far-end ports are up	at least one inline tool involved in the inline bypass solution is disabled or associated with any inline tool port that is down or associated with the heartbeat protocol in a down state	Forwarding state—FAILURE-INTRODUCED BYPASS All traffic is exchanged directly between side A network and side B network through the switching fabric as a result of an inline tool port failure or heartbeat failure or inline tool being disabled that led to the network-level bypass due to the configured failover actions.

physical-bypass	traffic-path	Status of far-end ports connected to inline network ports	Status of inline tool side	Description
disable	to-inline-tool	both far-end ports are up	at least one inline tool involved in the inline bypass solution is disabled or associated with any inline tool port that is down or associated with the heartbeat protocol in a down state	Forwarding state—FAILURE-INTRODUCED DROP No traffic is exchanged between side A network and side B network. All packets coming to the inline network ports are dropped as a result of an inline tool port failure or heartbeat failure or inline tool being disabled that led to the network-level drop due to the configured failover actions.
disable	to-inline-tool	both far-end ports are up	at least one inline tool involved in the inline bypass solution is disabled or associated with any inline tool port that is down or associated with the heartbeat protocol in a down state	Forwarding state—NETWORK PORTS FORCED DOWN No traffic is exchanged between side A network and side B network. The inline network ports are forced down as a result of an inline tool port failure or heartbeat failure or inline tool being disabled that led to the network ports being forced down due to the configured failover actions.
disable	to-inline-tool	both far-end ports are up	at least one inline tool involved in the inline bypass solution is disabled or associated with any inline tool port that is down or associated with the heartbeat protocol in a down state	Forwarding state—ABNORMAL Any condition of the inline bypass solution that does not meet the criteria of the forwarding states listed in this table. At least one inline tool passes traffic as desired. There are many scenarios that can lead to the abnormal forwarding state, for example, when one inline tool member of an inline tool group has failed, but the number of remaining healthy tools is still above the minimum required number of healthy tools.

IP Interface

An IP interface acts as a logical network interface that enables communication between devices using Internet Protocol (IP) addresses. It connects to a single IP peer within the local subnet and can reach destinations outside the subnet through the configured default gateway. Each IP interface associates an IPv4 or IPv6 address with a physical port—either a network or tool port—on a GigaVUE device.

IP interfaces are essential for GigaSMART operations such as encapsulation, decapsulation, tunnel initiation or termination, and NetFlow export. They are configured with attributes such as IP address, subnet mask, gateway, and MTU, and can be associated with GigaSMART groups and NetFlow exporters.

These interfaces handle the sending and receiving of traffic for advanced packet processing features including GigaSMART tunnels, NetFlow generation, and inline SSL decryption. Administrators can monitor interface status and performance metrics to ensure proper operation and simplify troubleshooting in visibility workflows.

NOTE: IP interfaces are supported on GigaVUE HC Series nodes but are not supported on TA Series nodes.

Inline Network Link Aggregation Group (LAG)

A Link Aggregation Group (LAG) combines multiple physical ports to act as one logical, high-bandwidth path. This approach improves throughput, distributes traffic across ports, and ensures link redundancy—so if one port fails, traffic continues through others.

When inspection or processing is required on aggregated links, the Flexible Inline Network LAG feature allows you to treat multiple inline networks as a single logical entity. Instead of configuring each inline network individually, you can manage them together.

This unified configuration makes it possible to:

- Apply consistent traffic forwarding and monitoring policies across all member links.
- Simplify load balancing and failover handling within inline deployments.
- Use the inline network LAG as a source in flexible inline maps for traffic orchestration.

Traffic entering a LAG is grouped and delivered to inline tools with the same VLAN ID. The response traffic is hashed and returned through the appropriate member links, ensuring bidirectional consistency and high availability.

Inline Network Link Aggregation Group— Rules and Notes

When configuring or using an inline network LAG, keep the following in mind:

1. Do not mix protected and unprotected inline networks or networks with different speeds within the same LAG.
2. Inline TLS/SSL Decryption is not supported with inline network LAG. Use an Inline Network Bundle instead.
3. It is strongly recommended that the first flexible inline map bypasses the LACP/PagP protocols between the inline network peers.
4. When Bypass LACP and LLDP is enabled, all protocol packets with MAC Destination 01-80-C2-XX-XX-XX are bypassed.
5. When CDP/LLDP Bypass is enabled, neighborhood discovery will not be established on the corresponding inline networks.

NOTE: Inline Network LAGs are only supported in Flexible Inline Arrangements. Classic Inline Bypass does not support the grouping of inline networks into LAGs. Classic deployments can monitor or protect individual inline networks, but they cannot aggregate them into a single logical link.

Inline Network Bundle

The Flexible Inline Network Bundle feature lets you group several inline networks into one bundle. You can then use this bundle as the source in a flexible inline map. The system automatically creates separate inline maps for each inline network in the bundle. These maps are built using the Tool Side VLAN tags and the rules you set when creating the bundle.

NOTE: This feature is only available in Flexible Inline Arrangements. It is not supported in Classic Inline Bypass.

Inline Tool Ports and Inline Tools

An **inline tool** is a device or a sequence of tools placed directly in the live traffic path between inline network ports for inspection, security, or optimization. Each inline tool is built from a pair of inline tool ports (Port A and Port B) that operate at the same speed, use the same medium (fiber or copper), and reside on the same node as the associated inline network ports. The paired ports and connected tool form a logical inline entity that processes packets passing through it.

One of the parameters of inline tools is failover action, which controls the action taken when a tool is unhealthy or in response to a failure of an inline tool. You can configure one of the following failover actions:

- **ToolBypass:** When an inline tool fails, traffic that would normally pass through it is redirected to the bypass path between side A and side B of the inline network. Use this mode for configurations that involve multiple inline tools associated with an inline network or inline network group using rule-based maps. In Flexible Inline, the same action applies to the failed tool instance in the flow sequence. For configurations using map pass-all, ToolBypass behaves the same as NetworkBypass.
- **NetworkBypass:** When an inline tool fails, all traffic that would normally pass through the inline network in a normal forwarding state is redirected to the bypass path. Traffic arriving at side A is forwarded to side B, and vice-versa, ensuring minimal disruption. This behavior is identical in both Classic and Flexible Inline modes.
- **ToolDrop:** When an inline tool fails, only the traffic mapped to that specific tool is dropped. Use this option when multiple inline tools share a network or tool group through rule-based or sequence maps. For map pass-all configurations, ToolDrop behaves the same as NetworkDrop.
- **NetworkDrop:** When an inline tool fails, all traffic associated with that inline network or group is dropped. Use this mode when you need to stop all packet forwarding after a failure.
- **NetworkPortForcedDown:** When an inline tool fails, the inline network ports are forced down. After a device reload, these ports become operationally up even if the tool remains down. To maintain correct behavior, manually force the inline network ports down again.

NOTE: The default failover action is **ToolBypass**. The bypass path operates between the side A and side B ports of the inline network.

When Flexible Inline Flow Mapping is used, failover actions apply to each tool within the defined sequence:

- **ToolBypass:** Traffic mapped to the failed tool is redirected to the bypass path. Other tools in the sequence continue to process their assigned traffic.

- **ToolDrop:** Traffic mapped to the failed tool is dropped, while traffic for healthy tools remains unaffected.

This model ensures that the failure of one tool does not interrupt traffic for other inline tools in the same sequence or map.

Inline Tool Recovery Modes

Inline tools detect traffic path failures between their port pairs and divert traffic as needed. After recovery, you can control how traffic returns to the inline tool using recovery modes. The Recovery Modes are as follows:

- **Automatic:** When the tool returns to a healthy state, traffic automatically resumes through it without user intervention. This is the default recovery mode.
- **Manual:** When recovery mode is set to manual, the failover action (for example, Bypass) remains active even after the tool is restored.

By selecting the tool and selecting the Recover button, users can set the recovery of the inline tools to manual or automatic.

Refer to [Figure 5Automatic and Manual Inline Tool Recovery from Failover](#) for automatic and manual inline tool recovery from failover.

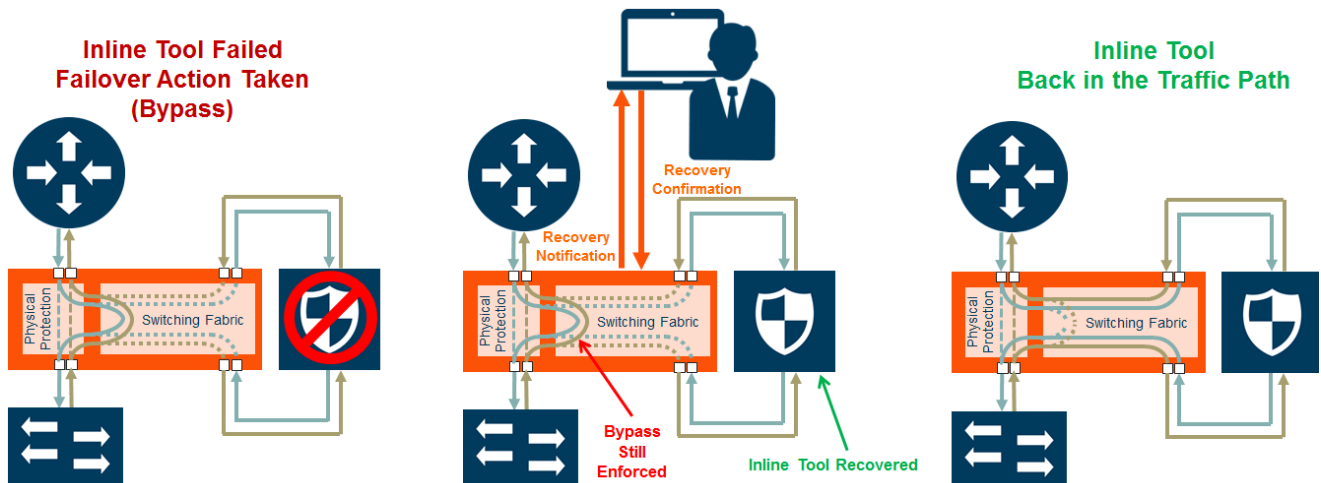


Figure 5 Automatic and Manual Inline Tool Recovery from Failover

The left side of [Figure 5Automatic and Manual Inline Tool Recovery from Failover](#) shows an inline tool that has failed and the bypass failover action has been executed.

Automatic recovery is shown on the right side of [Figure 5Automatic and Manual Inline Tool Recovery from Failover](#). When the inline tool recovers, traffic is automatically directed back to it.

Manual recovery is shown in the center of [Figure 5Automatic and Manual Inline Tool Recovery from Failover](#). When the recovery mode is configured as manual, an SNMP notification, if enabled, will send a notification when the inline tool is ready to be put back into service. The failover action, in this case, bypass, will be enforced until you manually put the inline tool back into service.

When the recovery mode is configured as manual, an SNMP notification, when enabled, will notify you when the inline tool is ready to be put back into service.

Inline Tool Group

NOTE: Resilient weighted hashing, single VLAN tag, and shared mode flexibility are supported only in Flexible Inline TLS/SSL deployments.

An inline tool group is a configuration that combines multiple inline tools into a single logical entity. Traffic is distributed among the tools using hardware-calculated hash values, and if one tool fails, the remaining tools in the group continue processing traffic. The ports of tools in a group must run at the same speed and medium and reside on the same node as the inline network ports.

In a clustered environment, the group must be configured on the cluster leader and cannot span multiple nodes. Resilient weighted hashing allows you to assign equal, relative or percentage-based weights to tools so traffic shifts appropriately when a tool fails, provided the group meets its Minimum Healthy Group Size.

If the group size falls below that threshold, traffic is handled according to the configured Failover Action: **Tool Bypass, Network Bypass, Tool Drop, Network Drop or Network Port Forced Down**. When configuring the tool group, you choose the traffic path mode (Drop, Bypass, Monitoring or To Inline Tool) and select options such as Enable, Release Spare if Possible, Minimum Healthy Group Size, Hash algorithm and spare tool assignments.

Inline tools connect to the GigaVUE-FM,GigaVUE HC Series node through inline bypass (BPS) modules, available on the GigaVUE-HC1, GigaVUE-HC3.

The inline bypass arrangements supported by inline TLS/SSL decryption are as follows:

- single inline network. The inline network ports can be protected, unprotected, or a mix of protected and unprotected.
- inline network group, consisting of multiple inline networks
- single inline tool
- inline tool group, consisting of multiple inline tools over which traffic is distributed

- inline tool group with a spare inline tool, in which the failure of one tool in the inline tool group will trigger a failover to the spare
- inline series, in which traffic is guided through inline tools in a particular order

In summary, inline TLS/SSL decryption can be deployed in any combination of inline network and inline network group with any inline tool, inline tool group, or inline series.

NOTE: The TLS/SSL sessions will fail, if a BPS card is shut down and brought back up with an Inline TLS/SSL configuration.

Inline tool ports can be configured in shared mode. When an inline tool is shared (true), the decrypted traffic will be VLAN tagged. The connected inline tool is expected to receive VLAN tagged packets instead of untagged packets. There is an extra outer VLAN tag added to the packet, which the connected inline device needs to see. When an inline tool is not shared (false), the extra VLAN tag is not added. This allows untagged traffic to be sent to the tool ports. Use false for inline tools that are not able to handle more than one VLAN tag, such as Q-in-Q tagged packets. For tagless mode, if an inline tool is involved in an inline TLS/SSL map, the inline tool cannot be used in any other classic inline map.

Refer to [Figure 6Simple Inline Tool Arrangement](#) to [Figure 8Serial Inline Tool Arrangement](#) for inline tool arrangements. Encrypted traffic is shown in solid lines, decrypted traffic is shown in dotted lines.

[Figure 6Simple Inline Tool Arrangement](#) shows a simple inline tool arrangement with one inline tool connected to the GigaVUE-FM,GigaVUE HC Series node. Traffic is decrypted and sent to the inline tool.

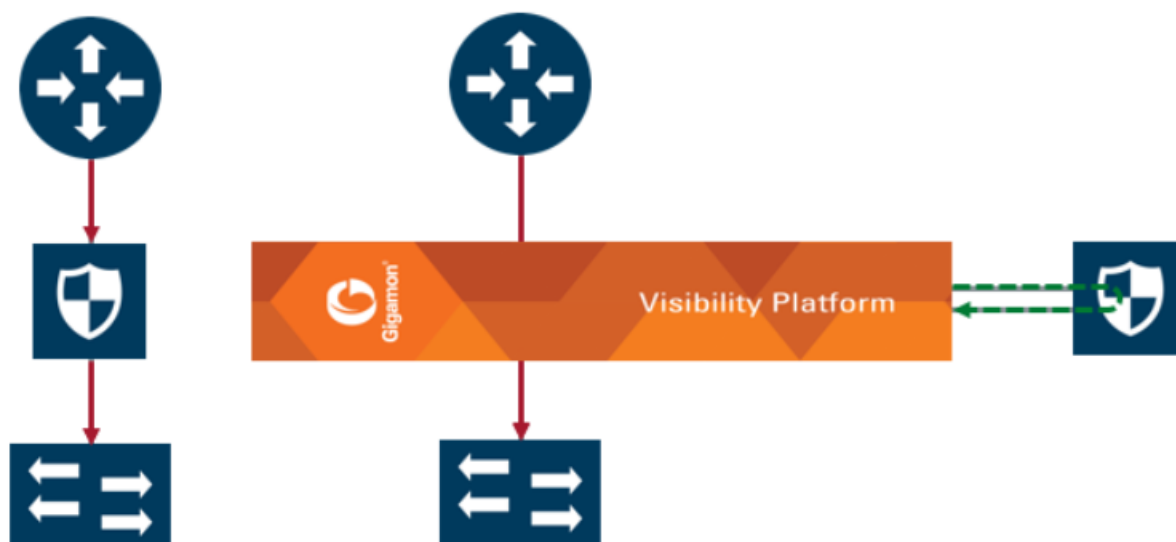


Figure 6 Simple Inline Tool Arrangement

Figure 7 Multiple Inline Tool Arrangement shows a multiple inline tool arrangement with three inline tools connected to the GigaVUE-FM, GigaVUE HC Series node. Decrypted traffic is distributed across the tools.

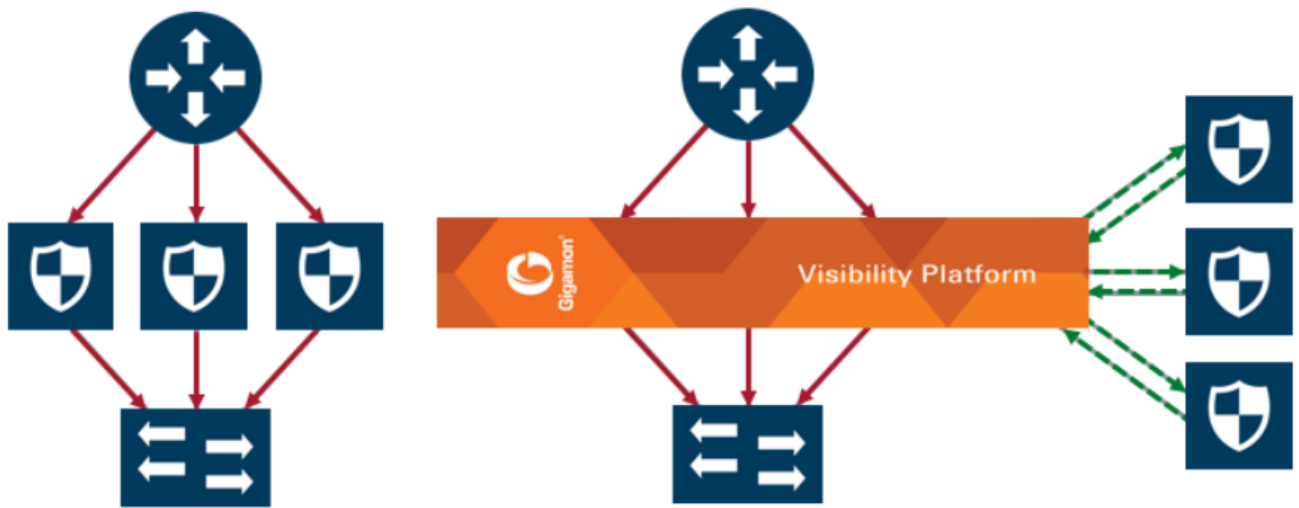


Figure 7 Multiple Inline Tool Arrangement

Figure 8 Serial Inline Tool Arrangement shows a serial inline tool arrangement in which traffic is decrypted on the GigaVUE-FM, GigaVUE HC Series node, sent serially through the inline tool, and then re-encrypted on the GigaVUE-FM, GigaVUE HC Series node.

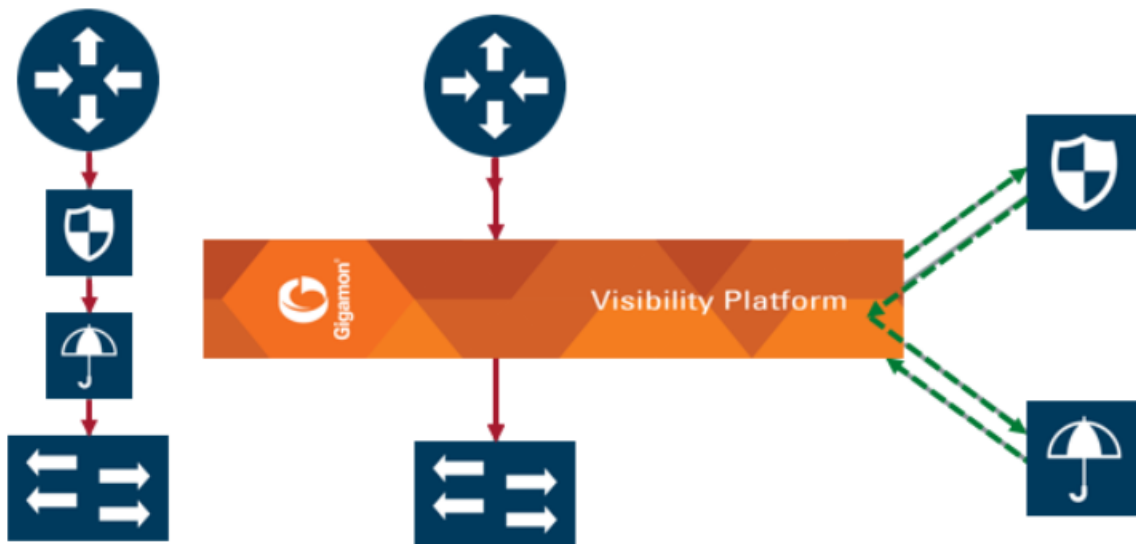


Figure 8 Serial Inline Tool Arrangement

Inline Bypass Restriction

The inline bypass arrangements supported by inline TLS/SSL decryption have the following restriction:

- inline network group does not support ingress VLAN tagging on the member links

Forwarding

Inline TLS/SSL decryption supports the following kinds of forwarding:

- inline forwarding—Packets can be forwarded from the inline network or inline network group to the inline tool, inline tool group, or inline series. The IPv6 traffic received from the inline network is forwarded as IPv6 traffic in tool-port. The translation from IPv6 packet in network-port to IPv4 packet in tool port will not be supported.
- inline out-of-band forwarding—Packets from inline ports can be sent to regular tool ports.
- inline bypassing—Packets can be put in loopback between two ports of an inline network.
- TLS/SSL forwarding—Packets from an inline network or inline network group can be sent to GigaSMART, then from GigaSMART to an inline tool, inline tool group, or inline series.
- GigaSMART out-of-band forwarding—Packets from GigaSMART can be copied to tool ports.

Failover

The inline bypass module detects failure either through link loss or tool heartbeat failure.

The inline bypass module supports the following failover actions:

- inline tool failover action—Specifies the failover action taken in response to a failure of an inline tool.
- inline tool group failover actions—Specifies the failover action taken in response to a failure of an inline tool group, when the number of healthy inline tools in the inline tool group (including the spare inline tool, if configured) falls below the configured minimum.
- inline tool series failover actions—Specifies the failover action taken in response to a failure of an inline tool series as a whole. An inline tool series is declared to be in a failure condition as soon as any of its member inline tools goes into a failure condition. An inline tool series recovers from a failure condition after all the member inline tools recover from their failure conditions. The failover-action attributes of the individual inline tools participating in an inline tool series are ignored. Instead, the failover-action configured for the inline tool series is respected.

The inline bypass failover actions are configurable. Refer to the *GigaVUE-OS CLI Reference Guide* for the actions and default values of the inline-tool, inline-tool-group, and inline-series commands.

The virtual port also has configurable failover actions. Refer to the *GigaVUE-OS CLI Reference Guide* for the actions and default value of the vport command.

The GigaSMART module might also have events such as port down or card down. These failover actions are not configurable but are triggered by events. These events should not impact traffic.

Out-of-Band and Inline Tools

After decryption, traffic can be sent to multiple tools. The tools can be either inline or out-of-band.

Out-of-band tools process the decrypted packets offline. The tools are connected to the GigaVUE-FM, GigaVUE HC Series node through tool or hybrid ports, GigaStream, or port groups with tool or hybrid ports. The out-of-band tools receive a copy of the decrypted packets from the GigaSMART module. This is referred to as GigaSMART out-of-band forwarding.

Inline tools process the decrypted packets inline. Inline tools are connected to the GigaVUE-FM, GigaVUE HC Series node through inline bypass (BPS) modules.

An out-of-band tool might be an Intrusion Detection System (IDS) examining decrypted packets:

- If it detects a threat, the IDS will send a notification back, but does not have the ability to act.

An inline tool might be an Intrusion Prevention System (IPS) examining decrypted packets:

- If it does not detect a threat in the decrypted packets, the traffic comes out of the inline tool and goes back to the GigaSMART module to be re-encrypted and sent to the server.
- If it detects a threat, the IPS can act. The action depends on the tools' behavior. It can either terminate the connection or modify packets
- If the IPS terminates the connection, then GigaVUE-FM, GigaVUE HC Series node will terminate the connection between the client and the server.
- If the IPS modifies packets, then the modified packets will come out of the inline tool, go to the GigaSMART module to be re-encrypted, and sent to the server.

When an inline tool is shared, you must:

- configure the inline second level out-of-band map to forward proxy traffic from GigaSMART to the out-of-band tool port.

When an inline tool is not shared, you must configure only the inline second level out-of-band map to forward proxy and non-proxy traffic from GigaSMART to the out-of-band tool port.

NOTE: When OOB-copy is configured in a non-shared inline-tool with the tag set as “inline”, both proxy and non-proxy out-of-band traffic will be copied with the proxy map VLAN tag.

Service Chaining of Decrypted Traffic

Service chaining of decrypted traffic may be required for compliance purposes.

This is done by directing the decrypted traffic to a hybrid port and applying the required GigaSMART operations on the traffic that is looped back from the hybrid port, before forwarding the traffic to the out-of-band tool.

The GigaSMART operations must be configured on a different GigaSMART engine than the one used for inline TLS/SSL decryption.

Packet Flows

Normally, a client and server talk directly to each other, such as when you are using a browser to go to a bank website, a health care provider, or a search engine.

As shown in figure below , the GigaVUE-FM,GigaVUE HC Series node is placed in the middle between the client and the server. All traffic from the Internet goes through the GigaVUE-FM,GigaVUE HC Series node.

Incoming traffic arrives on an ingress inline network port on the inline bypass module.

SSL traffic, which is TCP traffic, is directed to the GigaSMART module. Until the traffic is processed by the GigaSMART module, it is not known if it is SSL traffic or not.

The GigaSMART module decides what traffic is bypassed, what traffic is sent to tools without decryption, and what traffic is decrypted and then sent to tools. So, there are three types of decisions as follows:

- to bypass or not
- to decrypt or not
- to send to tools or not

[Figure 9Packet Flow for Inline SSL Decryption](#) shows the flow for a configuration consisting of a single inline network, a single inline tool, and a single out-of-band tool.

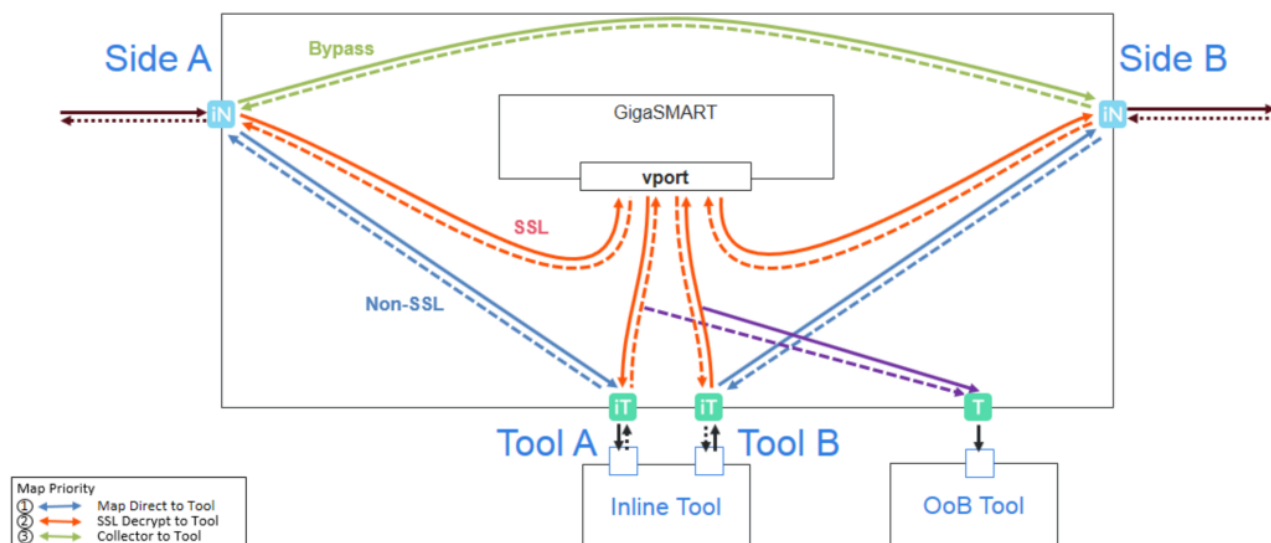


Figure 9 Packet Flow for Inline SSL Decryption

Traffic enters the inline SSL decryption solution at the side A inline network port on the inline bypass module.

Some traffic can be bypassed. That traffic goes from the side A inline network port to the side B inline network port on the inline bypass module as shown in the solid green line in [Figure 9Packet Flow for Inline SSL Decryption](#). Bidirectional traffic is shown by dotted lines.

Traffic that is not encrypted (non-SSL) can be sent to tools for inspection. That traffic goes from the side A inline network port to the inline tool A port, to the inline tool, and from the inline tool to the inline tool B port and the side B inline network port on the inline bypass module without going through the GigaSMART module as shown in the solid blue lines in [Figure 9Packet Flow for Inline SSL Decryption](#).

Traffic that is encrypted (SSL) goes from the side A inline network port on the inline bypass module to the GigaSMART module. That traffic goes to a virtual port (vport) that directs traffic to an inline SSL GigaSMART operation as shown by the red line on the left in [Figure 9Packet Flow for Inline SSL Decryption](#). The traffic is decrypted in the GigaSMART module based on policy configuration, sent to the inline tool A port to the inline tool and from the inline tool to the inline tool B port, then back to the GigaSMART module for re-encryption as shown in the solid red lines in the center of [Figure 9Packet Flow for Inline SSL Decryption](#). Finally, the re-encrypted traffic is sent from the GigaSMART module to the side B inline network port on the inline bypass module as shown by the red line on the right in [Figure 9Packet Flow for Inline SSL Decryption](#).

The out-of-band tool can also receive the traffic as shown by the purple line on the right in [Figure 9Packet Flow for Inline SSL Decryption](#).

An out-of-band map from a virtual port to a single tool port and to multiple tool ports is supported. The ports can be tool, hybrid, or GigaStream. Out-of-band maps from a vport to port groups are also supported when the ports in the group are tool or hybrid.

Modules Matrix

For traffic that is encrypted, there is a question as to whether or not it needs to be decrypted. For example, is there a policy for or against decrypting that traffic? There might be a policy, such as do not decrypt financial or health care traffic, or there might be a decrypt list that states that traffic from a particular site should always be decrypted, or there might be a no-decrypt list that states that traffic from a particular site should always be bypassed. So encrypted packets need to be filtered because some packets will not be decrypted, while others will be decrypted.

The following table is a matrix of the GigaVUE-FM, GigaVUE HC Series module used for different types of traffic.

Table 2: GigaVUE-FM, GigaVUE HC Series Modules Used for Type of Traffic

Type of Traffic	GigaSMART	Inline Bypass	GigaSMART
Bypassing GigaSMART	No	Yes - to network	No
Not encrypted (non-SSL)	Yes	Yes - to tools then to network	Yes, depending on the configuration
Encrypted (SSL), and to be decrypted	Yes	Yes - to tools	Yes - to be re-encrypted, then to network

The GigaSMART module does the decryption as well as handling policies, no-decrypt lists, and decrypt lists. The decision to decrypt or not is made in the GigaSMART module.

Inline Single VLAN Tag

During flexible inline bypass operations, network traffic sent to inline tools carries an additional VLAN tag. This tag helps distinguish return traffic from inline tools and ensures correct routing between inline networks. However, these extra tags can cause compatibility issues with certain tools. The Inline Single Tag feature resolves this by replacing the additional VLAN tag on incoming traffic. It enables mapping between network-side VLANs and tool-side VLANs, ensuring traffic reaches the inline tools with only one defined VLAN tag.

In flexible inline arrangements, VLAN tags are linked to each inline map rather than to inline network ports, as seen in classic inline bypass. A single inline network port can therefore host multiple inline maps, each with a separate VLAN tag. VLAN tags are added to traffic before it is sent to tools and removed before it returns to the network.

NOTE: The **OOB Copy** tag attribute **none** is invalid for single-tag maps; use the **original** or **as-inline** attribute instead. When configuring inline maps with a single VLAN tag, ensure that the map rules use the same VLAN tag as specified in the `from` parameter.

Flexible Inline Maps

Traffic flows are the building blocks of flexible inline arrangements. Flows can be based on any flow mapping criteria, such as TCP port, IP subnet, or VLAN. There is a one-to-one correspondence between a traffic flow and a flexible inline map.

A flexible inline map is a new map type. Flexible inline arrangements allow inline maps from inline networks to arbitrary sequences of shared (overlapping) sequences of inline tools and inline tool groups.

Using flexible inline maps, you can identify specific flows of traffic using Layer 2 (L2) to Layer 4 (L4) rules, then designate the tools that will inspect the traffic, and specify the order of traffic to the tools.

You can configure a flexible inline map with a specific inline tool that is part of an inline tool group, which is associated with another flexible inline map. For example, you have created an inline tool group, ITG1 in which inline tools, IT1, IT2, and IT3 are grouped together. You can configure a flexible inline map, Map1 with inline network, IN1 as the source and ITG1 as the destination. You can configure a second flexible inline map, Map2 with IN1 as source and IT1 as destination. Such configuration is useful to guide specific traffic to a particular inline tool and the rest of the traffic to the inline tool group in which the inline tool is associated.

To properly guide traffic through the inline tools, each flow of traffic is assigned a VLAN tag. VLAN tags can be automatically assigned or can be user-defined. You can use flexible inline single tags to map incoming VLANs on the network side to the outgoing VLANs on the tool side.

With flexible inline arrangements, VLAN tags are associated with each inline map, not with each inline network port as in the case of classic Inline Bypass. A single inline network port can have multiple inline maps, each with a separate VLAN tag.

A VLAN tag automatically assigned to an inline map can be manually added to another inline map. For example, if an inline map is given the VLAN tag 2000, the same VLAN tag can be manually added to another inline map. Here, the system would prioritize the manually added VLAN tag and modify the auto-assigned VLAN Tag. This is not applicable for VLAN's assigned to internal inline maps such as import/export maps and inner non-proxy maps configured by GigaVUE-FM for Resilient Inline Arrangement (RIA) and RIA SSL solutions.

For example, traffic flows can be defined with the following VLAN tags:

- Unspecified traffic—VLAN 101
- Web traffic—VLAN 102
- Email traffic—VLAN 103
- Database traffic—VLAN 104

NOTE: The VLAN tags are added to the traffic before it is sent to the tools and are removed before it is sent back to the network.

Types of Flexible Inline Maps

To define a traffic flow, you must configure a flexible inline map. Following are the two types of flexible inline maps:

- **byRule**—Use the byRule map type to define a flow using map rules. Any standard L2-L4 mapping rules can be specified in the map, such as, IPv4, IPv6, L4 port, or UDA.
- **collector**—Use the collector map type for all other traffic. A collector is the lowest priority of map and does not have a map rule definition. Use a collector to catch any traffic that does not go to any other map. You can define a flexible inline collector map without any other maps in place. This provides a map passall, provided there are no rule-based maps. If you want all the traffic to go to the same tools, you only need to configure a collector.

Flexible inline arrangements guide rule-based or collector-based inline traffic flows through unidirectional or bidirectional sequences of inline tools or inline tool groups. The traffic path can be set up independently for side A to side B and side B to side A directions, meaning that the traffic flow can be either symmetrical or asymmetrical.

You specify the ordered list of inline tools or inline tool groups that will inspect a particular flow of traffic. Additionally, you can specify if the A-to-B and B-to-A directions have the same order or the reverse order. Reverse order is the order of inline tools as they are wired in a physical network if a Gigamon network packet broker was not present.

For example, in the A-to-B direction, if the tools are specified in the following order: T1, T2, T3, the same order in the B-to-A direction will be: T1, T2, T3, while the reverse order in the B-to-A direction will be: T3, T2, T1. Or, you can specify the order of the tools explicitly, for example, the B-to-A direction can be: T2, T1, T3.

You can create separate flexible inline maps for each flow of traffic to be inspected by a sequence of inline tools. Create maps until you have accounted for all the flows of traffic. Any unspecified traffic will go to the collector. You can also specify map priorities for the flexible inline maps.

Types of Inline Networks

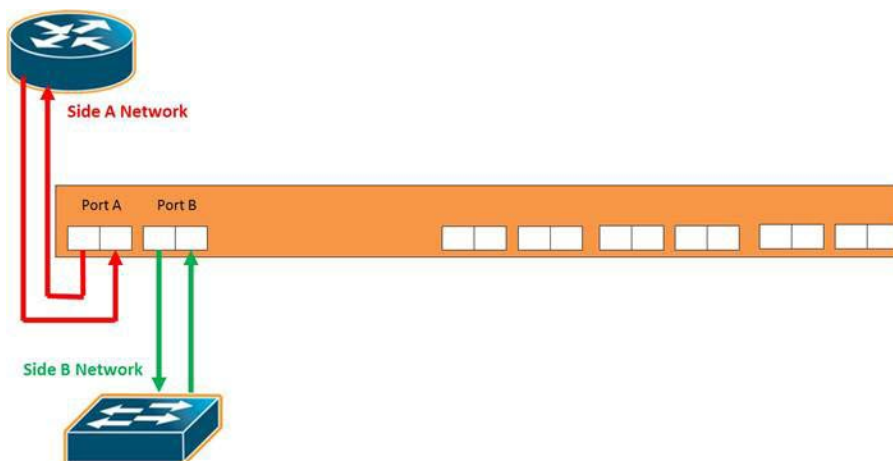
The types of inline networks are described in the following sections:

- [Unprotected Inline Network](#)
- [Protected Inline Network](#)
- [Mix of Protected and Unprotected](#)

Unprotected Inline Network

An unprotected inline network consists of two ports of the inline-network type, which facilitate access to a bidirectional link between two networks (or more precisely, two far-end network devices).

Any available network type ports on a GigaVUE-FM, GigaVUE HC Series HC Series node can be configured to inline-network type ports and combined to form an unprotected inline network. An unprotected inline network is shown in the following figure.



Resilient Inline Arrangement

Resilient inline arrangement is a method of configuring and deploying inline threat prevention tools for dual-path, redundant network architectures. A successful deployment of resilient inline arrangements provides traffic management for dual-path high availability environments.

NOTE: Resilient inline arrangement is not supported in GigaVUE-HCT devices, GigaVUE-TA400, and GigaVUE-TA400E.

The following figure illustrates the resilient inline arrangement.

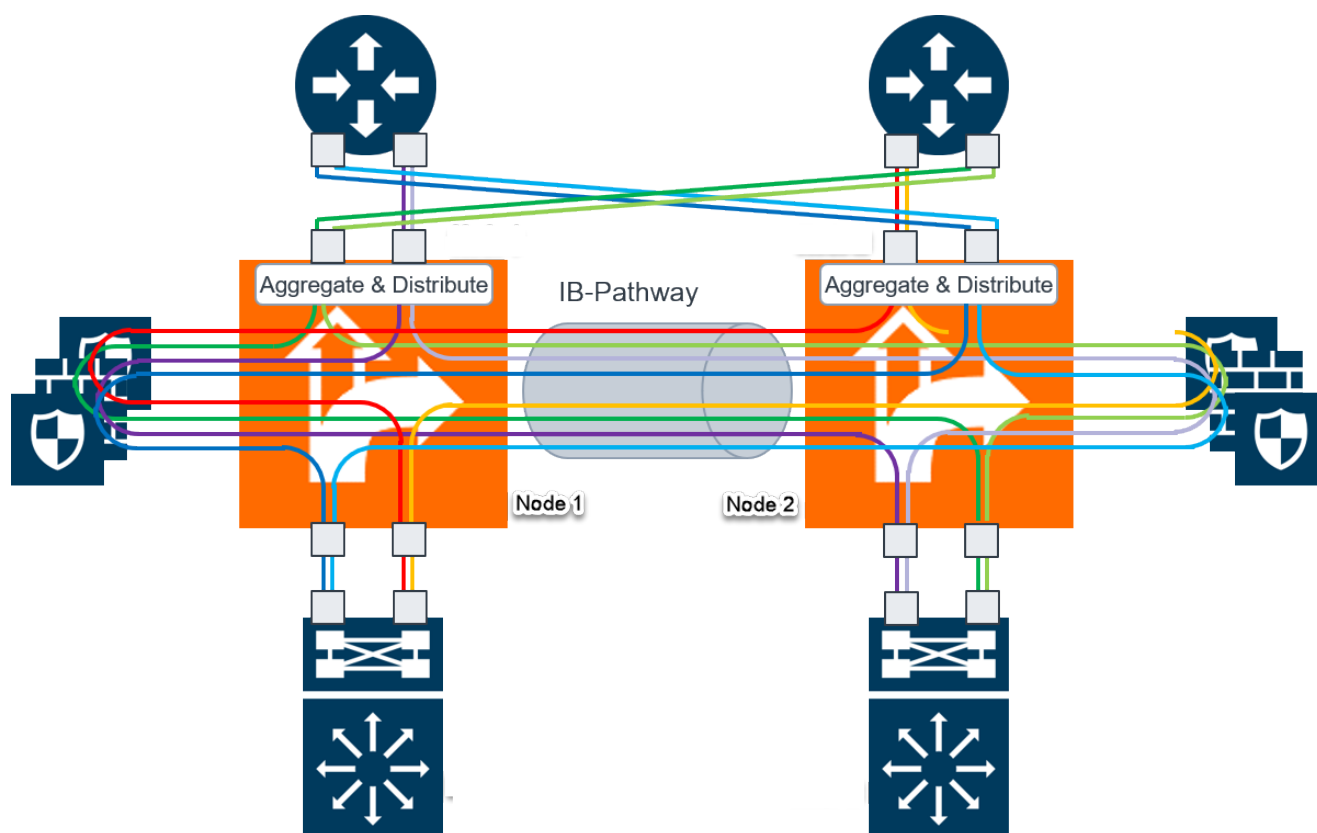


Figure 10 *Resilient Inline Arrangement*

The resilient inline arrangement shows the Gigamon devices, which consolidate the traffic from multiple intercepted links before routing the traffic to inline tools. To protect such an inspection arrangement from any failure of the Gigamon devices, a redundant arrangement of inline packet broker is shown. Both the inline packet brokers are interconnected by an Inter-broker Pathway (IB-P).

Each inline packet broker is attached to a set of inline tools that are identical to each other, that is, both inline packet brokers must have equal number of inline tools. Moreover, the inline tools on both sides must be of the same type, port speed, and processing capacity.

Resilient inline arrangement is based on an aggregation and distribution principle that divides the packets received by an inline packet broker, between Node 1 and Node 2. The inline packet broker on the left, guides the Node 1 class of packets through its local tools and Node 2 class of packets through the remote tools that are reachable by a resilient inter-broker pathway. Similarly, the inline packet broker on the right, guides the Node 2 class of packets through its local tools and Node 1 class of packets through the remote tools.

Each link intercepted by the inline packet broker must be configured with the following component maps:

- either a bidirectional original component map or two unidirectional original component maps,
- two unidirectional export component maps, and
- two unidirectional import component maps.

GigaVUE-FM configures the required export and import component maps for all the links that are intercepted by both the inline packet brokers. GigaVUE-FM configures the maps based on the tool side VLAN tags and the rules that you specified when configuring the flexible inline map.

The component maps use VLAN tags to transfer the traffic from inline network to inline tools and back through the inter-broker pathway. Refer to the following sections:

- [Resilient Inline Arrangement— Classic](#)
- [Resilient Inline Arrangement With Single VLAN Tag](#)

Resilient Inline Arrangement— Classic

When a packet is received from an inline network, an additional VLAN tag is added to the packet before guiding it to the inline tools. The additional VLAN tag is useful when the inline tools are shared by multiple traffic flows. It helps to distinguish the traffic coming from inline-tools and to make sure the traffic is routed to the right inline networks. You can configure the additional VLAN tags when you create the flexible inline maps.

Resilient Inline Arrangement With Single VLAN Tag

You can choose to deploy a resilient inline arrangement with a single VLAN tag in which a packet received from an inline network is guided to the inline tool using a single VLAN tag, which you can configure when creating a flexible inline map. You must configure the

packet's original VLAN tag as the network side VLAN tag and provide the required tool side VLAN tag when you create the flexible inline maps. The single VLAN tag is useful when your inline tools do not support Q-in-Q VLAN tags.

You can configure a Flexible Inline SSL and RIA iSSL solution with Single VLAN Tagging (SVT).

The following table explains the compatibility matrix between single VLAN tag enabled and disabled maps. Symbol (√) denotes the engine ports that are supported, and symbol (X) denotes the engine ports that are not supported.

Maps	SVT enabled RIA iSSL map	
	same gs_engine	different gs_engine in different maps
RIA	√	X
RIA + SVT	√	X
RIA + iSSL	√	X

NOTE: The **OOB Copy** tag attribute **none** is invalid for single-tag maps; use the **as-inline** attribute instead.

Inter-broker Pathway (IB-P)

The inter-broker pathway provides link aggregation and distribution and is responsible for moving traffic between Node 1 and Node 2. You must configure tool ports in the inter-broker pathway. Following are the IB-P states:

- inter-broker pathway-up—the traffic is handled as follows:
 - If the traffic is governed by the original component maps in which the traffic path is set to Bypass, the traffic bypasses the sequence of inline tools and inline tool groups and is re-directed to the inline network port that is configured on the opposite-side.
 - If the traffic is governed by the export component maps in which the traffic path is set to any value other than Bypass, the traffic is routed through the inter-broker pathway based on the tag value defined in the map. If the tag value matches the VLAN attribute configured in the import component map, the traffic is sent to the inline packet broker on the opposite side. The traffic is then routed through the inline tools or inline tool groups based on the sequence defined in the import component map. After inspection, the traffic is sent back to the inter-broker pathway with the same tag value. Finally, the traffic is intercepted by the export component map and is guided to the respective exit inline network port.

- inter-broker pathway-down—the traffic is handled based on the failover action selected for the inline map configured, as follows:
 - If the failover is set to 'bypass', the traffic is passed directly between the respective inline network ports.
 - If the failover is set to 'original-map', the traffic is passed through the path that is defined by the respective original map.

NOTE: Traffic can be moved from 'bypass' to 'original-map' and vice-versa, when the inter-broker pathway is in 'down' state.

The failover-action set for an inline tool or an inline tool group that is configured on Node 2 will affect the inter-broker pathway as follows:

- If the failover-action for the inline tools on Node 2 is set to 'network-bypass', all traffic received on the Node 2 will be by-passed and referred back to Node 1.
- If the failover-action is set to 'network-drop', all traffic received on Node 2 of the inter-broker pathway will be dropped.
- If the fail over-action is set to 'network-port-forced-down', all ports on Node 2 of the inter-broker pathway will be brought down.

Resilient Inline Arrangement—Rules and Notes

Keep in mind the following rules and notes when working with Resilient Inline Arrangement:

- In GEN2 GigaSMART card, a maximum of 14 VLANs will be supported for a single inline- network per GS Group. In the case of multiple inline-network ports (number of inline- network ports x number of VLANs), the number should not exceed 14 per GS Group.
- In GEN3 GigaSMART card, a maximum of 16 VLANs will be supported for a single inline- network per GS Group. In the case of multiple inline-network ports (number of inline- network ports x number of VLANs), the number should not exceed 16 per GS Group.

To configure, refer to [Configure Resilient Inline Arrangement Solution](#).

Hardware Security Modules (HSM)

NOTE: Starting in release 6.14.00, Entrust/nCipher HSM integration is deprecated. Gen2 DSSL HSMs (nCipher v1.0) and Gen3 HSMs using nCipher 12.6 (``nshield_12_60`) are no longer supported, and upgrades are blocked if any nCipher HSM configuration is present.

A Hardware Security Module (HSM) is a dedicated, tamper-resistant device that protects cryptographic keys and performs secure key operations. In inline deployments, HSMs are used to safeguard the private keys required for TLS/SSL decryption. By offloading key storage and sensitive cryptographic tasks to an HSM, organizations ensure that decryption happens without exposing keys inside the node.

Why HSM

Most enterprise traffic today is encrypted, making TLS/SSL decryption a critical part of inline deployments. Security tools such as intrusion prevention systems (IPS) or data loss prevention (DLP) engines need decrypted traffic to analyze threats. Without an HSM, private keys must be stored directly on a Gigamon HC Series node or server, which creates risk.

With an HSM, the private keys remain inside a hardened device. The node communicates with the HSM using secure tokens, never exposing the raw keys. This means:

- Keys never leave the HSM, even if the node is compromised.
- The node can request private key operations such as decryption without handling the key itself.
- Only approved applications, such as GigaSMART® SSL/TLS decryption, can use the tokenized access.

This makes the HSM a critical part of inline solutions where compliance, regulations, or strict security rules require hardware-grade key protection.

How HSM Solution Works

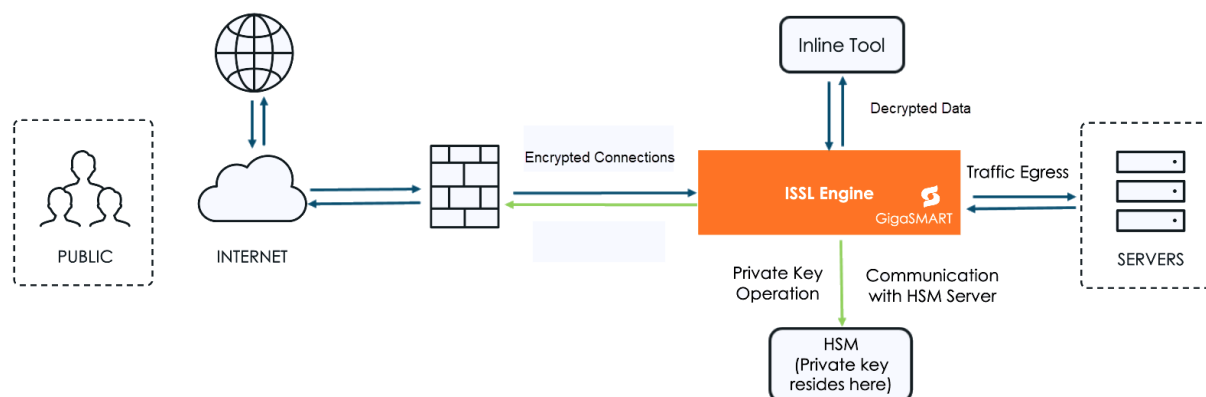
In Flexible Inline Arrangements, HSMs are supported through **HSM Groups**. An HSM Group represents one or more hardware modules connected to a node. Supported HSM devices include:

- Thales Luna Network HSMs

Each group is tied to a single vendor type; mixing vendors in the same group is not allowed. Thales Luna clustering is not supported, and IPv6 connectivity is not available. Nodes must be configured with static IPv4 addresses to communicate with HSMs.

When an HSM is in place, the node offloads TLS/SSL decryption key handling. For example, in an Inline SSL Decryption workflow, traffic passes through GigaSMART, which queries the HSM for key use. The HSM processes the request securely and returns only a tokenized response. The private key never leaves the HSM.

The following images illustrates the process flow of HSM solution



GigaSMART applications that commonly leverage HSMs include:

- SSL/TLS decryption for inline traffic inspection.
- Passive SSL/TLS Decryption

NOTE: Classic Inline Bypass does not support HSM integration. Classic deployments provide resiliency through protected inline networks, tool groups, and failover actions, but they do not include any mechanism for hardware-based key storage or integration with external HSM appliances.

HSM - Supported Platforms

HSM Group is supported in the following platforms:

- GigaVUE-HC1 Gen3
- GigaVUE-HC3 Gen3
- GigaVUE-HC1-Plus

To learn more about HSM configuration with Inline TLS/SSL Decryption, refer to:

- [Configure Entrust nShield HSM for TLS/SSL Decryption](#)

Internet Content Adaptation Protocol (ICAP)

The Internet Content Adaptation Protocol (ICAP) is used to connect inline deployments with external security services, such as Data Loss Prevention (DLP) systems. It provides a standard way to send decrypted HTTP traffic to a DLP-ICAP server for inspection and

policy enforcement.

In Gigamon deployments, the ICAP Client runs inside the GigaSMART® engine, where it acts like an inline tool. It receives decrypted HTTP traffic and forwards it to the ICAP server. The server inspects the content, applies any security policies, and returns the results. The ICAP Client then reinserts the inspected traffic back into the inline path.

NOTE: The ICAP Client is included as part of the TLS/SSL license SKUs.

How ICAP Solution works

In an Inline SSL/TLS Decryption (iSSL) workflow, decrypted HTTP requests and responses can be sent directly from GigaSMART to the ICAP Client. The ICAP Client then:

- Sends the decrypted traffic to the ICAP server for analysis.
- Accepts and applies any changes from the ICAP server before passing the traffic downstream.
- Works in both inbound and outbound inline traffic chains.

This process allows DLP systems to examine live, decrypted traffic in real time without breaking the inline flow.

Originally, DLP-ICAP servers had to be placed outside of the Gigamon decryption zone, which limited their ability to enforce policies on live traffic. With the ICAP Client, integration now happens directly in the inline path, providing real-time DLP enforcement.

The ICAP Client can also operate independent of Inline SSL , as long as it receives HTTP traffic (clear text) from another source.

The following figures illustrate typical **Inbound** and **Outbound** deployment scenarios where the ICAP Client is used to support DLP inspection.

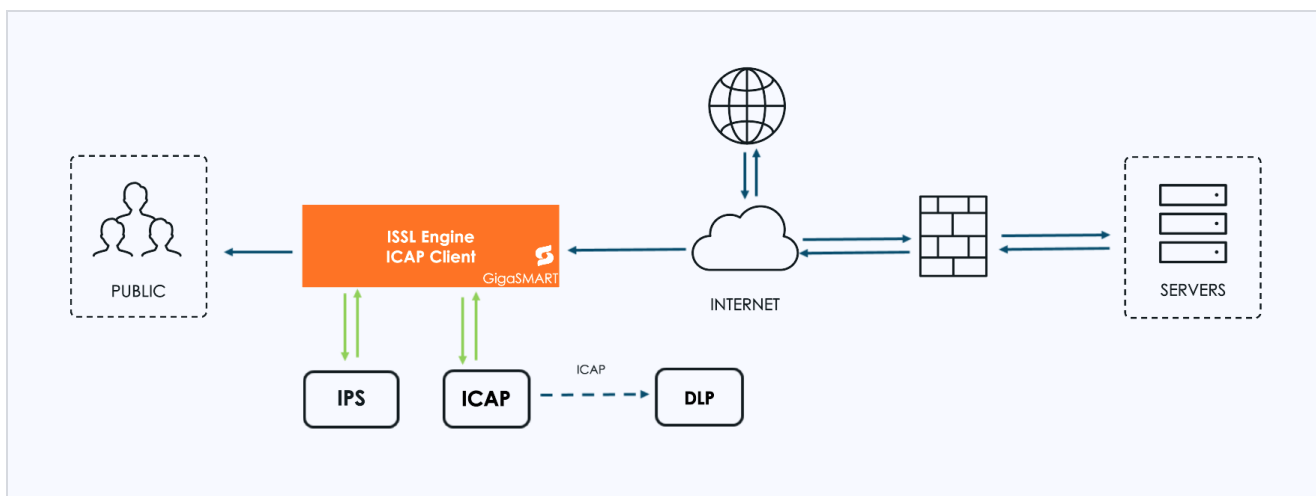
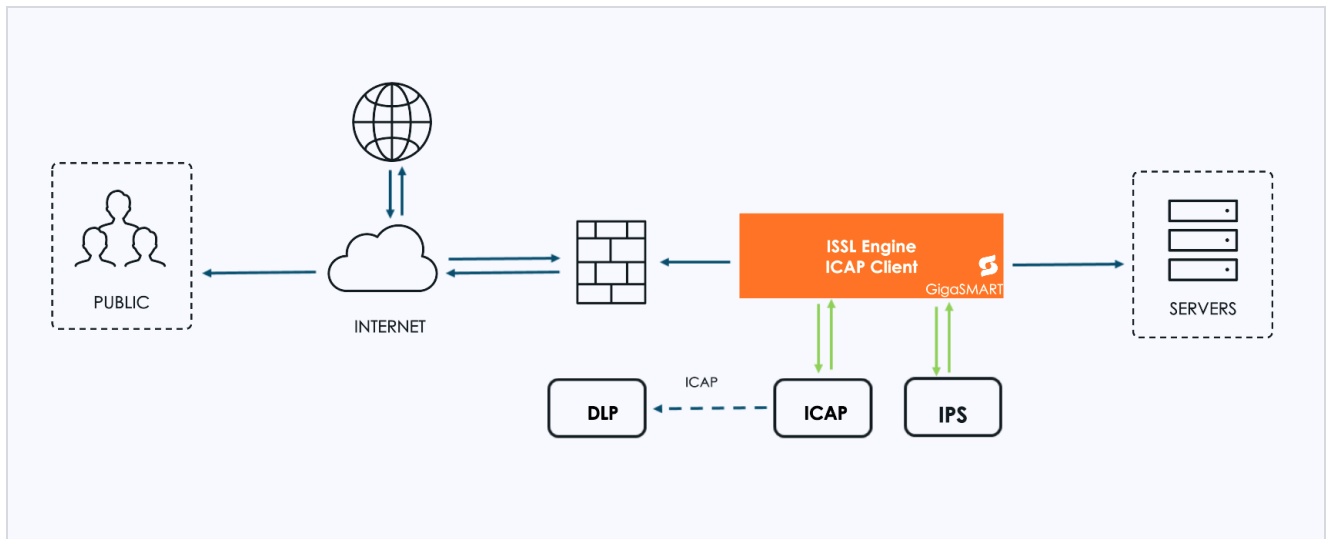


Figure 11 Inline SSL Solution with ICAP Client support – Outbound Deployment**Figure 12** Inline SSL Solution with ICAP Client support – Inbound Deployment

ICAP - Supported Platforms

ICAP Client app is supported in the following platforms and cards:

Platform	Card
GigaVUE-HC1 Gen3	SMT-HC1-S
GigaVUE-HC1P Gen3	SMT-HC1-S , SMT-HC1A-R
GigaVUE-HC3 Gen3	SMT-HC3-C08

ICAP - Rules, Notes, and Limitations

1. GSOP Integration Rules

- The ICAP GSOP must run as a standalone operation. It cannot be chained with other GSOPs.
- Each GSGroup can include only one ICAP GSOP.
- ICAP is not supported in clustered environments.

2. Protocol and Traffic Handling

- HTTP/2 traffic is not supported. HTTP/2 shall be downgraded to HTTP1.1 if required via a configuration option, so that ICAP inspection shall be done.
- HTTP/1.1 pipe lining is not supported; only one HTTP request/response can be processed at a time.
- HTTP chunk extensions are not forwarded to the ICAP server.

- HTTP trailers are forwarded as-is, but trailers within the preview length are not sent, per RFC 3507 limitations.
- Any Trailer present in HTTP messages are forwarded to the ICAP server without any modification, as the ICAP RFC does not define specific behavior for HTTP trailers.

3. Engine Port and Traffic Flow Considerations

- Using multiple engine ports in an inline pair map can disrupt traffic due to asymmetric flow. For example, a SYN packet from side A may hit engine port 1 while the SYN/ACK reply from side B reaches engine port 2, causing flow inconsistency.

ICAP - Supported GigaSMART Engine Ports

Refer to the table below for information on the number of GigaSMART engine ports required for each deployment module:

Type	Number of GS Engine	Comments
Standalone	1	1 Gen3 for ICAP
Inline SSL: Same Node	2	1 Gen3 for ICAP and 1 Gen3 or Gen2 for iSSL Inline SSL does not support HTTP2 Downgrade on Gen2. If HTTP2 Downgrade is required for iSSL, use 1 Gen3 for ICAP and 1 Gen3 for iSSL.
Inline SSL: Different Node	2	1 Gen3 for ICAP in the same node and 1 Gen3/Gen2 for iSSL in the other node

For more information on configuring an ICAP Client, refer to [Configure ICAP Client](#).

Gigamon Resiliency for Inline Protection

Gigamon Resiliency for Inline Protection (GRIP) is the umbrella term for node-level resiliency in inline deployments. It ensures that live traffic continues to flow and inline tools remain protected, even if one node fails.

GRIP is implemented differently depending on whether you are using **Classic Inline Bypass** or **Flexible Inline Arrangements**, but the goal is the same: maintain service continuity and protect inline inspection during node outages.

Both models rely on bypass protection switch relays on BPS modules to provide physical fail-safe behavior on protected inline networks

GRIP in Classic Inline Bypass

In Classic Inline Bypass, GRIP is a hardware-based failover mechanism that uses stack signaling and relay-protected inline links. Two nodes are paired using a stack signaling link:

- The primary node actively handles inline traffic.
- The standby node is ready to take over if the primary fails.
- Both nodes connect to the same inline network links through bypass combo modules (fiber) or copper TAP modules.

These modules include optical or electrical relays that automatically close when the primary fails, rerouting traffic to the standby node. Failover typically occurs within 0–10 seconds.

If both nodes fail, GRIP ensures that traffic still flows directly between the inline network ports, bypassing the tools so the network remains available, even if inspection is lost.

GRIP in Flexible Inline (Redundancy)

In Flexible Inline Arrangements, node-level resiliency is delivered through Redundancy, which functions as the Flexible Inline version of GRIP. As in Classic, protected inline networks still use BPS relays for physical protection, but Flexible Inline adds policy-driven redundancy and traffic steering on top of that hardware foundation

- Both nodes can be configured in active/standby modes.
- If one node or tool path fails, traffic flows are automatically redistributed to the healthy node or tools, guided by session-aware hashing and policy rules.
- Failover is faster and more flexible.

Across both deployment models, GRIP provides:

- **Node-Level Protection** – Ensures traffic continuity even if an entire node fails.
- **High Availability** – Prevents tool disconnections and minimizes downtime.
- **Operational Flexibility** – Hardware relay-based protection in Classic; policy-driven redundancy in Flexible.
- **Seamless Recovery** – Once the failed node recovers, it can resume its role without disrupting live traffic.

GRIP Scenarios

The following scenarios illustrate how GRIP behaves in real-world deployments, showing how traffic flows through primary and secondary nodes under different conditions.

Traffic Flows Through Node with Primary Role

When both nodes are active, the primary node handles all inline traffic. Its bypass protection switch relays remain open, directing traffic to the inline tool attached to the primary node. The secondary node monitors the state of the signaling link. As long as the link is up, the secondary node remains idle with its relays closed.

Normal

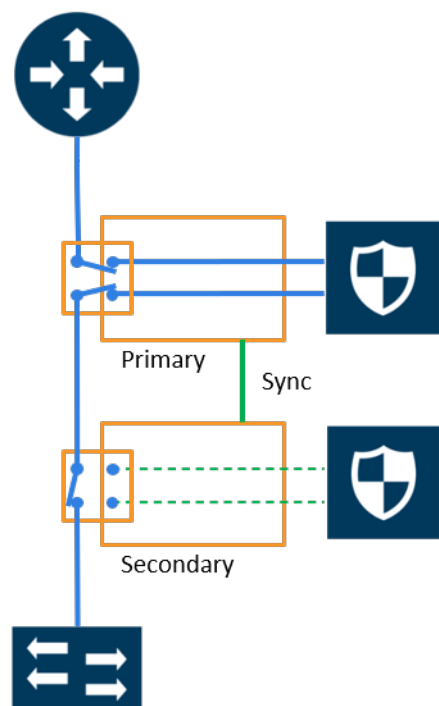


Figure 13 Traffic Flows Through Node with Primary Role

Traffic Flows Through Node with Secondary Role after Primary is Lost

If the primary node loses power or becomes unavailable, its relays close automatically. The signaling link informs the secondary node, which then opens its relays. Traffic immediately shifts to flow through the secondary node, keeping the inline tool path active.

Failover

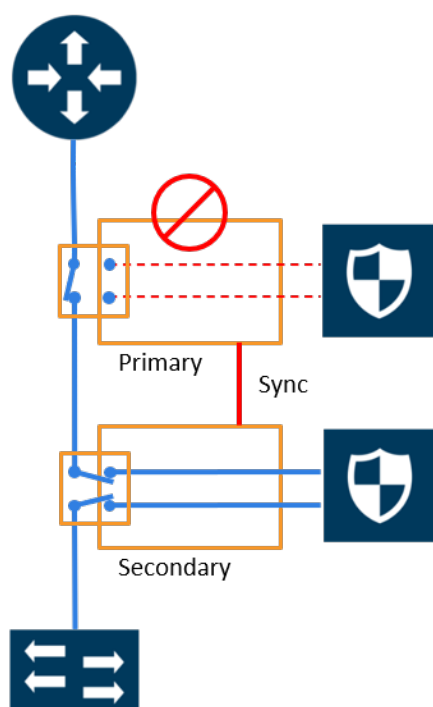


Figure 14 Traffic Flows Through Node with Secondary Role after Primary is Lost

Both Nodes Go Down and Only Secondary Comes Up

If both nodes fail at the same time, and only the secondary is later powered back up, traffic is not passed through the inline tools. Instead, it is bypassed across the relays. For this reason, it is recommended to always restore the primary node as well, or promote the secondary into the primary role if the original primary is unreliable.

Both Nodes Fail; No Traffic Monitoring

If both nodes remain down, the bypass relays on both close, allowing network traffic to continue to flow, but all inline tools are bypassed. The network remains up, but without inspection or monitoring.

2x Failover

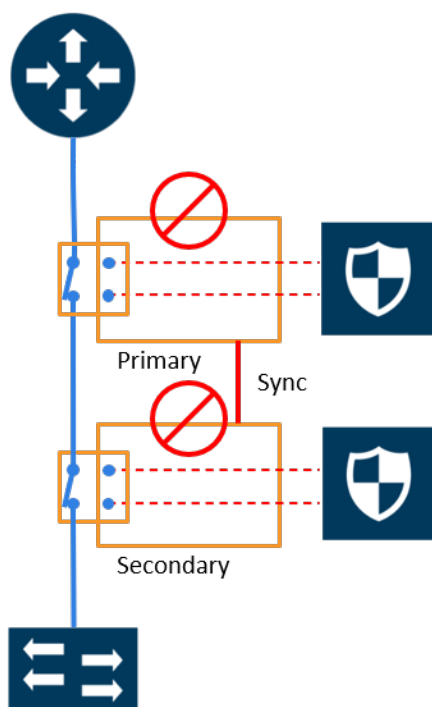


Figure 15 Both Nodes Fail; No Traffic Monitoring

Both Nodes are in Suspended State

In the GRIP solution, if both primary and secondary nodes are switched to suspended, Network traffic will be bypassed instead of being sent to inline tools in both the nodes. Switching redundancy profile protection role on secondary node alone from suspended to secondary will still cause network traffic to be bypassed instead of being sent to inline tools in both the nodes.

It is recommended to switch the redundancy profile protection role on primary node from suspended to primary first, then followed by switching the redundancy profile protection role on secondary node from suspended to secondary.

How to Handle Recovery

When the primary node recovers, it restores its inline traffic paths and opens its relays. The signaling link then instructs the secondary node to close its relays, returning traffic to the primary path. Recovery is automatic, and traffic resumes flowing through the primary node's tool path.

How to Cable GigaVUE-FM,GigaVUE HC Series Nodes

To cable two GigaVUE-FM,GigaVUE HC Series nodes, as shown in [Figure 13Traffic Flows Through Node with Primary Role](#) with the primary on the left and the secondary on the right:

- Connect the network shown at the top of [Figure 13Traffic Flows Through Node with Primary Role](#) to inline network port A on the primary node.
- Connect inline network port B on the primary node to inline network port A on the secondary node.
- Connect inline network port B on the secondary node to the network shown at the bottom of the [Figure 13Traffic Flows Through Node with Primary Role](#).
- Connect the signaling port on the primary node to the signaling port on the secondary node.

Redundancy Profile

GRIP resiliency is managed by a redundancy profile, which defines how the two nodes coordinate:

- Signaling Port – the port pair used to exchange health status between the nodes.
- Protection Role – assigns each node as Primary, Secondary, or Suspended.
 - Primary: Actively handles inline traffic.
 - Secondary: Remains on standby, takes over when the primary fails.
 - Suspended: Used for maintenance or to manually force failover.

NOTE: Cluster Limitation- GRIP is supported in clustered environments, but the Suspended role has restrictions on standby nodes. In this case, it is recommended to switch the standby into a new role or carefully apply the suspended state.

Refer to [How to Use Suspended Role for Maintenance](#) to know more [Gigamon Resiliency for Inline Protection](#)

Rules and Notes

Keep in mind the following rules and notes when you work with the Gigamon Resiliency for Inline Protection feature:

1. The signaling port type should be a stack port, and only one port should be used.
2. All the inline components should be located in the same box within the cluster.
3. Adding the Inline Networks in the Inline Network Bundle and deploying the Solutions is recommended, which will be easy to export and import across the GRIP Nodes.

4. Post-reload or Power Cycle, the signaling port link stays down when the redundancy profile is attached to the inline network and no maps have been configured. A map should be configured to bring the signaling port up. If a map exists, the signaling port will appear without any issues.
5. Link Failure Propagation is not recommended for copper ports (TAP card ports). Fabric ports support LFP only in a single path (a-to-b only) is available. In all other cases, it is best to leave LFP enabled.
6. Gigamon Resiliency for Inline Protection (GRIP™) is not supported in GigaVUE-HCT devices.
7. GRIP is not supported in other GigaVUE TA Series devices due to the absence of BPS modules.
8. Refer to [Flexible Inline TLS/SSL Decryption Solution—Rules and Notes](#), which also apply to GRIP.

Limitations

- Link failure propagation is not recommended when inline network ports involve copper ports (TAP card ports) or fabric ports with only a single available path (a-to-b only). In all other cases, enabling LFP is recommended.

Inline TLS/SSL Decryption

NOTE: In this section, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) mean the same thing. The terms are used interchangeably. Before you proceed, make sure you understand the [TLS/SSL Terminology and Acronyms](#)

Inline TLS/SSL decryption gives your security tools access to encrypted traffic. It works by decrypting packets and sending them to tools that are placed either inline (directly in the data path) or out-of-band (off the path). These tools then scan the decrypted traffic for threats, such as viruses and malware.

Unlike passive decryption, which only sends decrypted traffic to out-of-band tools that can alert but not act, inline decryption enables tools to take immediate action on threats.

Why Decrypt TLS/SSL Traffic

Most Internet traffic is now encrypted using SSL or TLS. While encryption protects data, it also makes it harder to inspect packets for threats. As a result, malware and other attacks often conceal themselves within encrypted traffic. Without decryption, these threats go unseen.

By decrypting TLS/SSL traffic:

- You can detect hidden threats across any port or application (e.g., HTTPS, email, VoIP).
- You reduce risk and gain visibility into encrypted sessions within your network.

Inline vs. Passive Decryption

Inline TLS/SSL decryption is active. It enables tools to inspect traffic in real-time and take action when a threat is detected. This is different from passive decryption, such as the existing GigaSMART SSL/TLS solution. Passive decryption only sends traffic to tools out-of-band. These tools can detect threats and alert users, but cannot stop threats directly.

Inline decryption does more. It offloads the complex decryption task so tools can focus on detecting and stopping threats faster and more effectively.

How Inline TLS/SSL Decryption Works

Inline TLS/SSL decryption performs the following key functions:

- Detects encrypted traffic across any port in your network.
- Intercepts encrypted flows between clients and servers.
- Filters traffic by policy, allowing sensitive flows (e.g., healthcare or financial data) to bypass decryption.
- Decrypts packets at a single, centralized point.
- Forwards decrypted data to one or more tools for inspection. These tools can be inline or out-of-band.
- Takes action on threats:
 - Tools can modify traffic (e.g., remove malware) or terminate sessions.
 - If modified, GigaSMART re-encrypts the packets.
 - If the session is terminated, GigaSMART ends the connection between client and server.
- Re-encrypts traffic after inspection and sends it back into the network.

Mutual TLS (mTLS) with Inline TLS/SSL Decryption

Mutual TLS (mTLS) is an extension of TLS/SSL in which both the client and the server present and validate certificates during the TLS handshake. This creates a two-way trust relationship, the client verifies that it is talking to the expected server, and the server verifies that it is talking to an authenticated client.

In a standard Inline TLS/SSL deployment, Gigamon validates the server certificate and optionally enforces certificate/revocation policies before re-signing traffic and forwarding it to inline tools for inspection. With mTLS support, Gigamon can additionally:

- Validate client certificates presented to the server.
- Enforce client-authentication policies (for example, drop connections with unknown or self-signed client certificates).
- Offload the client-auth handshake to the inline TLS/SSL solution so attached tools can focus on inspection rather than certificate processing.

In an inbound deployment with mTLS enabled, the high-level flow is as follows:

1. The client initiates a TLS connection to the protected server.
2. The GigaVUE node, acting as a Man-in-the-Middle (MitM), terminates the client-side TLS session and validates the server certificate as in a regular inbound deployment.
3. When the server requests a client certificate, the client sends its certificate to the GigaVUE node.
4. The client certificate chain is validated against a client trust store and applies client-auth policy (expired, self-signed, unknown CA, revocation status, and so on).
5. If the client is accepted, Gigamon completes the mTLS handshake on both sides, decrypts the traffic, and forwards clear-text packets to inline tools for inspection.
6. After inspection, Gigamon re-encrypts traffic and forwards it to the server, maintaining the mTLS session semantics on the wire.

NOTE: Mutual TLS (mTLS) functionality is now supported only for **Inbound and Hybrid Inline TLS/SSL Decryption** in Flexible Inline deployments. Outbound deployments continue to use one-way TLS/SSL decryption without client authentication.

Mutual TLS Inline TLS/SSL Decryption is on GigaVUE-HC Series Gen3 platforms used for Inline TLS/SSL decryption such as : GigaVUE-HC1 Gen3, GigaVUE-HC3 Gen3, GigaVUE-HC1-Plus.

The following feature combinations are not supported with Mutual TLS Inline TLS/SSL Decryption:

- Inline TLS/SSL L3 Tool NAT/PAT Support
- Entrust nShield and Thales Luna HSM for iSSL
- Post-quantum client authentication using PQC certificates (PQC cipher support is limited to server side).
- One-Arm mode and Tool Early Engage.
- Tool Early Inspect.
- Inline TLS/SSL deployments with ICAP .

Privacy and Sensitive Data Handling

Decrypted traffic may expose sensitive information, such as:

- Usernames and passwords in email
- Social security numbers in financial records

To protect user privacy and meet compliance standards, you can define policies that exclude certain traffic from decryption. This helps align with acceptable use, legal, and regulatory requirements.

What Applications Use TLS/SSL

Many applications such as email, websites, and voice calls over IP (VoIP), use TLS/SSL to secure data. Encryption ensures that sensitive data stays private while traveling over the Internet. But when data is encrypted, network tools cannot inspect it. This creates blind spots where threats can hide.

Decrypting this traffic removes those blind spots. It allows your tools to inspect data on any port or application, such as HTTPS (port 443), email, web, VoIP, FTPS, SMTP, IMAP, and POP3 (via StartTLS).

Supportability and Compatibility for Inline TLS/SSL Decryption

Refer to the following sections for details:

- [Supported Platforms](#)
- [GigaSMART Licensing](#)
-
- [Port Requirements](#)
- [GigaSMART Compatibility](#)
-

Supported Platforms

Inline TLS/SSL decryption is supported on the following platforms:

- GigaVUE-HC1
- GigaVUE-HC1-Plus
- GigaVUE-HC3

To enable decryption, both the GigaSMART module and the inline bypass module must be installed on the same node.

Mutual TLS (mTLS) Support and Limitations

Mutual TLS (mTLS) functionality is now supported only for **Inbound and Hybrid Inline TLS/SSL Decryption** in Flexible Inline deployments. Outbound deployments continue to use one-way TLS/SSL decryption without client authentication. The platforms and features that are compatible with this functionality are listed below:

Supported platforms for mTLS

Mutual TLS (mTLS) is supported only on GigaVUE-HC Series Gen 3 platforms such as

- GigaVUE-HC1 Gen3
- GigaVUE-HC3 Gen3
- GigaVUE-HC1-Plus

Limitations of mTLS functionality

- L3 Tool NAT/PAT: the Inline TLS/SSL L3 Tool NAT/PAT Support feature cannot be combined with mTLS. If NAT/PAT mode is enabled on the profile, mTLS must remain disabled.
- HSM integration: Inline TLS/SSL decryption using Entrust nShield or Thales Luna HSM cannot be used together with mTLS in the same Inline SSL application.
- PQC client authentication: Post-Quantum Cryptography (PQC) cipher support does not extend to client certificate authentication. If a server requests a PQC client certificate, the session is bypassed for client-authentication purposes.
- One-Arm mode and Tool Early Engage: One-Arm mode requires Tool Early Engage and is not supported with mTLS. Any configuration that enables One-Arm mode or Tool Early Engage must keep mTLS disabled.
- Tool Early Inspect: Tool Early Inspect changes the order of TLS handshakes and is incompatible with mTLS; these features cannot be enabled at the same time.
- ICAP client flows: Inline TLS/SSL with ICAP Client continues to operate on decrypted HTTP traffic; mTLS cannot be enforced end-to-end across the ICAP chain in this release.
- When inbound mTLS traffic is running with a large number of Server key maps or scaled configurations/rules, editing these configurations (for example, adding or removing server key map entries or updating the client trust store) can temporarily disrupt inline TLS/SSL decryption for existing connections while the new configuration is applied.

GigaSMART Licensing

Required License: Subscription based TLS/SSL Decryption license.

Inline Bypass Requirements

For physical inline bypass, install a fiber bypass (BPS) combo module. On GigaVUE-HC1, a copper TAP can also be used for physical bypass. Refer to the table for a list of supported inline bypass modules.

Model & Module Type	Description & BPS Port Pairs
GigaVUE-HC1 PLUS	Includes:
• BPS-HC1-D25A60 (HC1-Plus)	6 × SX/SR multimode inline network port pairs
• BPS-HC1-D35C60 (HC1-Plus)	6 × LX/LR single-mode inline network port pairs
GigaVUE-HC1 (Classic HC1 Chassis)	Includes:
• BPS-HC1-D25A24	2 × SX/SR multimode (50/125 μm) inline network port pairs + 4 SFP+ cages
• BPS-HC1-D25A60 (HC1-Plus)	6 × SX/SR multimode inline network port pairs
• BPS-HC1-D35C60 (HC1-Plus)	6 × LX/LR single-mode inline network port pairs
GigaVUE-HC2	Includes:
• BPS-HC0-D25A4G	4 × SX/SR (50/125 μm) multimode bypass pairs, 16 SFP/SFP+ cages
• BPS-HC0-D25B4G	4 × SX/SR (62.5/125 μm) multimode bypass pairs, 16 SFP/SFP+ cages
• BPS-HC0-D35C4G	4 × LX/LR single-mode bypass pairs, 16 SFP/SFP+ cages
• BPS-HC0-Q25A28	2 × SR4 (50/125 μm) bypass pairs, 8 SFP/SFP+ cages (40 Gb capability)
GigaVUE-HC3	Includes:
• BPS-HC3-C25F2G	2 × SR4 (40/100 Gb) BPS pairs, 16 SFP+ cages
• BPS-HC3-Q35C2G	2 × 40 Gb LR bypass pairs, 16 SFP+ cages
• BPS-HC3-C35C2G	2 × 100 Gb LR bypass pairs, 16 SFP+ cages

The following diagram shows a GigaVUE device with both the GigaSMART and inline bypass (BPS) modules installed:

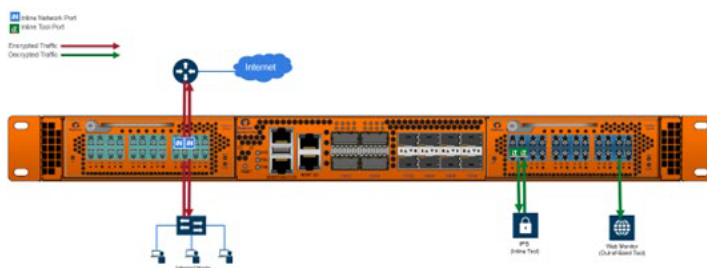


Figure 16 GigaVUE-FM, GigaVUE HC Series Modules: GigaSMART and Inline Bypass

- The GigaSMART module contains the SSL decryption software.
- The inline network ports are located on the inline bypass module.
- Inline and out-of-band tool ports are available on the same GigaVUE node.

Port Requirements

- For inline traffic, both inline network and inline tool ports require two links (a port pair) to handle bidirectional traffic.
- For out-of-band (offline) traffic, only one link is needed, as the traffic is not bidirectional.

GigaSMART Compatibility

Inline TLS/SSL decryption must be configured exclusively on a GigaSMART engine. It is not compatible with other GigaSMART operations, including Passive TLS/SSL decryption.

- Do not share the same GigaSMART engine with other operations when using inline TLS/SSL decryption.
- You can deploy both inbound and outbound inline TLS/SSL decryption on a single GigaSMART engine.

NOTE: On GigaVUE-HCI nodes, Inline TLS/SSL decryption can be configured alongside other GigaSMART applications.

Supported Ciphers

Inline TLS/SSL decryption supports modern cryptographic algorithms. It supports the commonly-supported TLS 1.2 and TLS 1.3 ciphers.

Combining the following ciphers, MACs, and Key Exchange Algorithms results in many cipher suites:

- Ciphers: AES_128_CBC, AES_128_GCM, AES_256_GCM, AES_256_CBC, Camellia, Chacha20
- MAC: SHA, SHA256, SHA384, Poly1305
- Key Exchange Algorithms: RSA, DHE_RSA, ECDHE_RSA, ECDHE_ECDSA.

Diffie Hellman Ephemeral (DHE) is a key exchange protocol.

Inline TLS/SSL Decryption supports key cipher suites and exchanges without downgrading cryptography levels of the organization.

Cipher suites are a standard combination of the following:

- **bulk encryption algorithm**—Specifies how to encrypt communications, including the algorithm, key size, and the cryptographic mode used. For example, AES_128_CBC is AES with 128-bit keys in Cipher Block Chaining mode.
- **key exchange algorithm**—Specifies how both sides authenticate each other during the TLS/SSL handshake. For example, RSA.

- **message authentication code (MAC)**—Specifies the hash algorithm used to verify that communications have not been tampered with. For example, SHA.
- **pseudorandom function**—Specifies how a 384-bit master secret, which is used as a source of randomness for session keys, is generated.

**NOTES:**

- TLS/SSL transactions with unsupported ciphers will be bypassed/TCP proxied.
- The new TLS1.3 cipher suites are defined differently and do not specify the certificate types (RSA/DSA/ECDSA) or the key exchange mechanism (DHE/ECHDE).
- The Inline TLS/SSL session is now equipped to receive a client hello with the key exchange X25519Kyber768 and now fall back to using just X25519. This ensures the system maintains secure and functional connections, even if it cannot use the newer, quantum-resistant algorithm now.

The following key sizes are supported:

- **RSA**—2048, 3072, 4096, 8192
- **DH**—1024, 2048, 4096
- **ECC**—prime256v1, ecsecp256r1, ecsecp384r1, ecsecp521r1, secp160k1, secp160r1, secp160r2, secp192k1, secp192r1, secp224k1, secp224r1, secp256k1, secp256r1, secp384r1, secp521r1, brainpoolP256r1, brainpoolP384r1, brainpool512r1, X25519, X448

The following TLS extension is supported:

- **RFC7301**—Application-Layer Protocol Negotiation (ALPN)

The below table lists the TLS 1.3 and TLS 1.2 ciphers that support Inline TLS/SSL Decryption.

Inline TLS/SSL Supported TLS 1.3 Ciphers

Cipher Name	Encryption (Enc)	MAC
TLS_AES_256_GCM_SHA384	AES_256_GCM	SHA384
TLS_CHACHA20_POLY1305_SHA256	CHACHA20_POLY1305	SHA256
TLS_AES_128_GCM_SHA256	AES_128_GCM	SHA256

Inline TLS/SSL Supported TLS 1.2 Ciphers

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE	RSA	AES128_CBC	SHA
TLS_DHE_RSA_WITH_AES_256_	DHE	RSA	AES256_CBC	SHA

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
CBC_SHA				
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE	RSA	CAMELLIA128	SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	CAMELLIA128	SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	CAMELLIA256	SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE	RSA	CAMELLIA256	SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE	RSA	AES128_CBC	SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE	RSA	AES256_CBC	SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE	RSA	AES128_GCM	SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE	RSA	AES256_GCM	SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	ECDHE	RSA	CHACHA20	POLY1305
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305	ECDHE	ECDSA	CHACHA20	POLY1305
TLS_DHE_RSA_WITH_CHACHA20_POLY1305	DHE	RSA	CHACHA20	POLY1305
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES128_CBC	SHA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES256_CBC	SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES128_CBC	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES256_CBC	SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES128_GCM	SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AES256_GCM	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE	ECDSA	AES128_CBC	SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE	ECDSA	AES256_CBC	SHA

Cipher Name	Key Exchange (Kx)	Authentication (Au)	Encryption (Enc)	MAC
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE	RSA	AES128_CBC	SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE	RSA	AES256_CBC	SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES128_CBC	SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES256_CBC	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES128_CBC	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES256_CBC	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES128_GCM	SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE	ECDSA	AES256_GCM	SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES128_GCM	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES256_GCM	SHA384

Post-Quantum Cryptography (PQC) Cipher Support

Post-Quantum Cryptography (PQC) introduces cryptographic algorithms designed to be secure against attacks from both classical and quantum computers. This update enables devices to negotiate and process SSL/TLS sessions using PQC algorithms when performing Inline SSL decryption.

Supported Algorithms

- Key Exchange (KEM):
 - ML-KEM (CRYSTALS-KYBER) in variants mlkem512, mlkem768, mlkem1024
 - Hybrid combinations (e.g., X25519_MLKEM768, SecP256r1_MLKEM768, SecP384r1MLKEM1024)
- Signature Algorithms:
 - ML-DSA (CRYSTALS-DILITHIUM) in variants mldsa44, mldsa65, mldsa87

Supported Key File Types

The supported file types for Inline SSL support for Post-Quantum Cryptography (PQC) Ciphers are as follows:

- PEM format: pq-private (for PQC private keys)
- PKCS12 format: pq-pkcs12 (for PQC key/certificate bundles)
- Certificate files: pq-certificate (for PQC certificates)

You can enable PQC ciphers via GigaVUE-OS CLI command **apps keystore** or select the Key type '**PQC**' in your Inline SSL profile.

Limitations

The main limitations of the Inline TLS/SSL support for Post-Quantum Cryptography (PQC) ciphers include:

- The FHA Inline TLS/SSL dashboard does not currently show any details related to PQC.
- This feature does not apply when NAT/PAT needs to support multiple Client Hello messages.
- The feature does not support client authentication with PQC algorithm certificates. If a server requests a client certificate, sessions will be bypassed, and PQC client certificates will not be intercepted..
- HSM Luna and NCipher do not support Post-Quantum Cryptography (PQC).
- The new PQC key type is not compatible with the GEN2 Inline SSL flex configuration.
- This feature is also incompatible with the Classic Inline Bypass configuration.

Attributes of Inline TLS/SSL Decryption Solution

This section describes the various attributes that construct an inline TLS/SSL decryption solution. You can configure these attributes in the Inline SSL App based on your deployment type. For details, refer to Configure Flexible Inline TLS/SSL Decryption Solution.

Refer to the following sections for more details:

TLS/SSL Sessions

Secure Sockets Layer (SSL) is a protocol that enables secure data transfer between a client and server. Transport Layer Security (TLS) builds on SSL and adds stronger cryptographic protection for TCP/IP communication.

A TLS/SSL session begins when the client initiates a connection. The GigaVUE node intercepts this request and negotiates a TLS/SSL session with the client. The node monitors all TCP connections and intercepts TLS/SSL sessions, while non-TCP traffic passes through unchanged.

All incoming TLS/SSL traffic terminates on the GigaVUE node. The node decrypts traffic for inbound or outbound deployments, forwards it to inline tools, and then passes it to the server.

The GigaVUE node maintains session details such as the client's IP address, allowing it to "reconnect" the client and server after decryption. The node also negotiates a new TLS/SSL session with the server. TLS/SSL traffic can be sent to tools inline or out-of-band.

TLS/SSL Handshake

TLS/SSL encryption secures traffic between client and server. Decryption uses keys to decode this traffic. TLS/SSL protocols define a series of handshake messages that set up and tear down a secure connection.

During the handshake, the client and server use Public Key Infrastructure (PKI) to exchange encryption keys for data transfer.

TLS/SSL Handshake Steps:

1. The client sends a Client Hello message with its supported TLS/SSL version, cipher suites, and a random number.
2. The server replies with a Server Hello message. It selects a cipher suite, sends its supported version, a random number, and its digital certificate.
3. The client verifies the server's certificate.
4. Using the random numbers, the client creates a `pre_master_secret`, encrypts it with the server's public key, and sends it.
5. The server verifies the client certificate if requested.
6. The client sends a Client Finished message, encrypted with the shared secret key, confirming its part of the handshake.

7. The server responds with a Server Finished message, also encrypted, confirming its part of the handshake.

8. The session is now established, and both sides use the shared secret key for encrypted communication.

TCP Transition States during TLS/SSL Session

The TCP handshake moves through different states during a TLS/SSL session:

- (Na:SYN_RCV:Nb:SYN_SENT:INIT:INIT): Client SYN received; TCP handshake starts on the server side. If the server is busy or unreachable, the session resets.
- (Nb:SYN_RCV: EST:INIT:INIT): TCP handshake is complete on the server side.
- (Na:EST:Nb:EST:Na:INIT:Nb:INIT): TCP handshake complete between client and server; session may be decrypted depending on policy.
- (Na:EST:Nb:EST:Ta:SYN_SENT:Tb:INIT): Decryption decision made; tool-side TCP handshake begins.
- (EST:EST:Ta:SYN_SENT:Tb:SYN_RCV): Tool-side TCP handshake continues.
- (EST:EST:EST:EST): TCP handshake successfully established

TLS/SSL Session Resumption

TLS/SSL sessions can be resumed to improve performance. TLS/SSL session resumption speeds up the TLS/SSL handshake.

Once a session has been established, the keys are saved so a session can be resumed efficiently later. The resumed TLS/SSL handshake has fewer steps.

Session identifier-based resumption is supported. The GigaVUE-FM,GigaVUE HC Series node maintains the session identifier data in the cache. Session ticket-based resumption is not supported. By default, resumption is enabled.

TLS/SSL Session Search

You can search for an existing TLS/SSL session by hostname. The system matches the input against the Server Name Indication (SNI) or the certificate subject name of current sessions.

StartTLS and HTTP CONNECT

When the system detects a CLIENT HELLO packet, it switches to TLS/SSL mode.

- StartTLS: Allows protocols like SMTP, IMAP, and POP3 to begin in plaintext, then upgrade to TLS/SSL on the same port. Up to 20 ports can be monitored for StartTLS traffic.

- HTTP CONNECT: Used by explicit proxies to establish an HTTP session, then upgrade to TLS. Detection is automatic.

Both methods add security by upgrading existing plain text protocols.

Behavior with StartTLS

- If StartTLS is used, Inline TLS/SSL decryption works if the decision to decrypt is made at the certificate phase.
- If the CLIENT HELLO packet does not have SNI, policy rules are applied during the certificate phase.

Explicit proxy traffic also applies policy rules during the certificate phase.

NOTE: StartTLS must be enabled for decryption of sessions that use explicit proxy.

TLS/SSL Keys and Certificates

The TLS/SSL protocol enables secure data transfer between a server and a client. Both ends use cryptographic keys to decode the transmission and certificates to establish trust.

A TLS/SSL certificate is a digital file that contains a public key, host information, and a digital signature from a Certificate Authority (CA). This certificate ensures that communication between two endpoints can be trusted.

The Inline TLS/SSL decryption solution acts as a Break-and-Inspect system.

- Outbound traffic – The Man-in-the-Middle (MitM) generates server certificates on the fly, signed by the installed Signing CA.
- Inbound traffic – Certificate generation is not required, but the server's private key and certificate chain must be provided to the MitM.

The inline TLS/SSL decryption solution uses two main components – Key Store and Trust Store.

Key Store

The key store holds private keys and certificate-key pairs. It can store up to 1000 key pairs. Keys can be used for:

- **Inbound deployment** – For decrypting traffic using the server's private key.
- **Outbound deployment** – For re-signing and re-encrypting traffic using the Signing CA.

The key store supports encrypted or password-protected PEM files to fetch or download private keys. It also supports ECDSA keys for both inbound and outbound deployments.

Trust Store

The trust store is used to validate server certificates. Gigamon only trusts certificates that are linked to a CA in the trust store. In other words, the certificate chain must connect back to one of the trusted root CAs.

Gigamon provides a default trust store, based on Mozilla's trusted CAs, which is updated periodically. You can replace it with your own trust store in PEM format, append new CA certificates, or delete specific ones. You can also search for a certificate using its SHA1 fingerprint.

NOTE: Whenever you modify the trust store, you must reconfigure the inline TLS/SSL profile for the changes to take effect.

Client Trust Store (for mTLS)

Inline TLS/SSL decryption with mTLS introduces a **Client Trust Store** dedicated to validating client certificates. When a server requests client authentication, GigVUE node validates the client certificate chain against this trust store and applies the configured policy (for example, whether to allow expired, self-signed, or unknown-CA certificates) to decide whether to complete or terminate the mTLS handshake. The client trust store is managed separately from the server trust store and is used only for inbound and hybrid mTLS deployments. Changes to a client trust store take effect only for Inline SSL profiles that already reference it, and only after those profiles are updated or redeployed.

NOTE: When a device that previously used inbound mTLS is later re-purposed for outbound Inline TLS/SSL decryption, remove all configured client trust store and client key store entries before you deploy outbound Inline SSL profiles. Otherwise, outbound sessions may be bypassed instead of decrypted.

Certificate Validation

Gigamon validates server certificates before re-signing them. This prevents untrusted certificates from being incorrectly accepted. The validation process includes:

- **Certificate expiration date and validity period** – The certificate must not be expired and must fall within the valid date range.
- **Certificate issued by trusted CA** – The GigaVUE node maintains a list of trusted root CAs. This list determines the certificates that the client will accept. The trust store acts as a trust anchor during certificate validation. The GigaVUE node validates that each incoming certificate chain is trusted by one of the certificates in the trust store.
- **Server name** – The hostname in the certificate must match the Server Name Indication (SNI). If the client does not send SNI, this check is skipped.

- **Certificate revocation check** – The system checks the certificate's status using OCSP or CRL. This requires internet access. The certificate revocation check determines the revocation status of the server certificate.

Certificates that pass validation are signed by the primary MitM CA. If a certificate fails validation but a security exception is configured, the secondary MitM CA signs the certificate instead.

If the certificate is self-signed, the re-signed certificate will also be self-signed. Typically, client applications only trust the primary MitM CA, which helps surface certificate errors to end users so they can decide whether to reject the connection.

If no exception is configured, connections with invalid certificates are dropped.

Types of Certificate Validation Errors

The types of Certificate Validation errors are as follows:

- **Expired** – The certificate validity period has ended.
- **Self-signed** – The certificate issuer and subject are the same.
- **Unknown CA** – The CA is not in the trust store or cannot be validated. (You may download and import the root certificate if you trust the site.)
- **Invalid** – The certificate does not match the SNI or contains incorrect signature/field information.

For expired, unknown CA, and invalid certificates, Gigamon re-signs the certificate with the secondary MitM CA. This allows users to either accept or reject the connection.

Client Authentication

A server can request a client certificate after sending the Server Hello message. The client responds with its certificate, and the server validates it. Gigamon supports client authentication for both inbound and outbound traffic. If client authentication is detected during the handshake, the connection is bypassed.

Client Authentication with mTLS enabled

When mTLS is enabled for an Inline SSL profile and a server requests a client certificate:

1. The client sends its certificate to Gigamon as part of the mTLS handshake.
2. GigavUE node validates the client certificate chain against the client trust store and applies the configured client-auth policy (expired, self-signed, unknown CA, revocation status).
3. If the client certificate is accepted:
 - GigaVUE node completes the handshake on both client and server sides.

- The session is decrypted and forwarded to inline tools as in a normal inbound deployment.
- 4. If the client certificate is rejected according to policy:
 - The TLS session is terminated with an appropriate error toward the client.
 - No traffic is forwarded to the server or inline tools for that session

Re-Signed Certificates

As a Man-in-the-Middle (MitM), Gigamon re-signs certificates.

- Fields copied from original certificate:
 - subject name
 - certificate validity
 - subject alternative name
- Fields removed from the certificate:
 - authority information access
 - certificate policies
 - CRL distribution points
 - SCT list
- Fields set in the re-signed certificate:
 - certificate type - v3
 - issuer
 - version
 - public key
 - random serial number
 - signature algorithm/hash
 - thumbprint
 - v3 extensions:
 - basicConstraints CA=True

NOTE: As this is a CA certificate, basicConstraints is set to True. For leaf certificates, basicConstraints is set to False.

- keyUsage—digitalSignature and keyEncipherment
- extendedkeyUsage—serverAuth
- subjectKeyIdentifier—hash
- authorityKeyIdentifier—keyid,issuer:always

Certificate Revocation Status

When Gigamon re-issues certificates for outbound traffic, clients automatically trust them because the MitM CA is already installed in the browser's trust store. This prevents clients from directly checking the revocation status of the original certificate.

Instead, the GigaVUE node performs revocation checks before generating replacement certificates.

- **Soft fail mode** – Traffic continues even if the revocation status is unknown.
- **Hard fail mode** – Traffic is blocked until the certificate's revocation status is confirmed.

If a certificate is confirmed as revoked, all future TLS/SSL connections to that server are dropped. By default, revocation checks are disabled.

Methods to Check Certificate Revocation Status

To check the certificate revocation status utilize one of the following method:

- **Certificate Revocation List (CRL)** – An online database of revoked certificates published by each CA. The list contains the serial number of the revoked certificates and the reasons for the revocation. Any revoked certificate should not be trusted even if the signatures are valid. The CRL location is included in the “CRL distribution points” X.509 extension of the certificate.
- **Online Certificate Status Protocol (OCSP)** – An Internet protocol used for obtaining the revocation status of an X.509 certificate. A real-time check can be performed using the OCSP link in the “Authority Information Access” X.509 extension.

If both CRL and OCSP are enabled, OCSP is attempted first, followed by CRL. Both methods require internet connectivity.

Policy Profile

A Policy Profile defines how traffic is processed during Inline SSL/TLS decryption. It determines which traffic is decrypted and which remains encrypted, based on a set of match rules and handling options. Each rule includes a match condition and an action—either decrypt or no-decrypt. For example, administrators can decrypt all general traffic while excluding sensitive categories such as financial transactions.

A Policy Profile is made up of several components:

- **Policy Rules:** Match traffic conditions and apply either decrypt or no-decrypt actions.
- **Default Action:** Specifies the action taken when no rule matches.
- **URL Cache Miss Action:** Defines what to do when a rule based on URL category cannot be evaluated because category data is missing.
- **Certificate Handling:** Controls how certificates are validated for decrypted traffic. Administrators can allow or block expired, invalid, self-signed, or unknown-CA certificates and enable or disable certificate-revocation checks.
- **Tool Handling:** Determines whether decrypted or non-decrypted traffic is forwarded to inline tools for further analysis.

Types of Policy Rules

Policy rules can be created based on one or more attributes such as:

- URL category (for example, finance, healthcare, or social media)
- Hostname or domain name
- Server certificate issuer
- Source or destination IP address
- Source or destination port number
- VLAN identifier

Scale and Flexibility

A single policy profile can include up to 2,048 rules, allowing fine-grained control over decryption policies and precise traffic handling across complex network environments.

Policy Evaluation

Policy evaluation defines how SSL/TLS decryption policies are applied at different stages of a connection. Each phase uses specific inputs—such as IP addresses, ports, host names, and certificates—to decide whether traffic is decrypted or left encrypted.

The below image describes the policy validation flow.

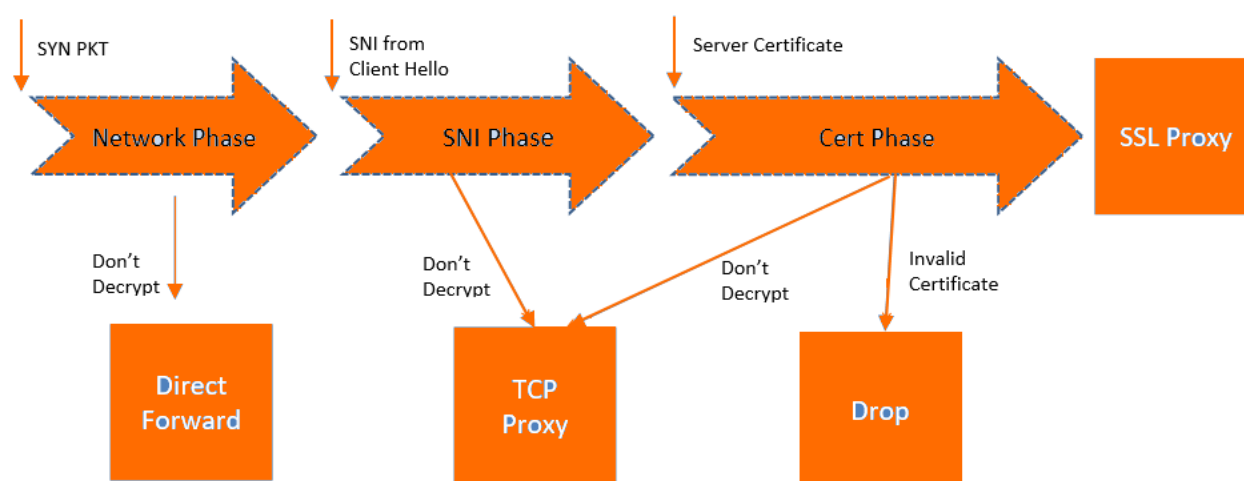


Figure 17 Policy Validation Flow

Network Phase

The Network Phase is evaluated on the TCP SYN packet.

- Inputs: source and destination IP addresses, source and destination ports, and VLAN identifiers.
- Evaluation Order: no-decrypt rules are evaluated before decrypt rules. Decrypt rules are checked in the following sequence: source IP, destination IP, source port, destination port, and VLAN.
- If a no-decrypt rule matches, packets are processed as non-proxy traffic using the bypass VLAN path (Direct Forward). This decision remains final for the lifetime of that TCP connection.
- If traffic is to be decrypted, processing continues to later phases. A decrypt verdict from the Network Phase can be overridden by a more specific rule in a subsequent phase.

For connections marked for decryption:

- If the Client Hello contains SNI, policy is further evaluated in the SNI and Certificate phases.
- If no SNI is present, only the Certificate Phase is evaluated.
- For HTTPS proxy connections, hostname information from the CONNECT request is also used during evaluation.

SNI Phase

The SNI Phase evaluates the Server Name Indication (SNI) field from the Client Hello.

- Input: the hostname obtained from SNI.
- Evaluation Order: no-decrypt (domain) → decrypt (domain) → no-decrypt (category) → decrypt (category).
- Wildcard domains (for example, *.example.com) can be used to match all sub-domains, while plain domains (for example, example.com) match only the exact host.
- If traffic is not decrypted, it is handled through the TCP Proxy path. For traffic that is decrypted, the plaintext version is sent through the configured tool path according to the decrypt tool-bypass settings.

When URL category-based rules are configured and a URL cache miss occurs, behavior depends on the URL Cache Miss Action:

- decrypt or no-decrypt — applied immediately.
- defer — causes a temporary delay.

For compliance reasons, no-decrypt is the recommended cache-miss action.

Certificate Validation

When traffic is marked for decryption (from the SNI phase or when SNI is absent), the system validates the server certificate using the configured trust store. Checks include:

- certificate expiry, hostname mismatch, and self-signed status;

- optional revocation status if enabled.

If the certificate is valid, a new server certificate is issued using the primary MitM CA. If validation fails, the connection is dropped unless a security exception is configured. When a secondary MitM CA is defined, it may be used to issue replacement certificates in such cases. The primary MitM CA is optional for inbound deployments.

Certificate Phase

The Certificate Phase is evaluated for all connections after certificate validation.

- Inputs: certificate issuer and subject name. The Common Name (CN) attribute is extracted from the certificate subject and used for policy matching.
- Evaluation Order: rules based on certificate subject (CN) first, then issuer-based rules using the CN and DN of the issuer.
- If traffic is not decrypted, it is processed as TCP Proxy traffic—the server SSL session is reset and the Client Hello is resent.

For HTTPS proxy connections, the Certificate Phase also evaluates policies using the hostname from the CONNECT request. If required, no-decrypt can be applied during this phase for such connections.

Together, these evaluation phases ensure that decryption behavior is accurate, rule-driven, and compliant, allowing administrators to define precise control over SSL/TLS traffic handling.

Policy Profile Options

This section describes a few of the options for the Inline TLS/SSL policy profile. Refer to the following sections:

- [Inline TLS/SSL Decryption Port Map](#)
- [Enable or Disable Tool Bypass](#)
- [High Availability Active Standby](#)
- [Inline Network Group Multiple Entry](#)
- [Tool Early Engage](#)
- [One-Arm Mode](#)
- [Tool Early Inspect](#)
- [Inline TLS/SSL L3 Tool NAT/PAT Support](#)

Inline TLS/SSL Decryption Port Map

The TCP destination port for decrypted traffic sent to inline tools can be configured in the decryption profile.

If not configured, the system automatically uses the same TCP destination port as the incoming traffic.

The appliance determines the TCP port for decrypted traffic based on two priority levels:

- **Priority 1 — Port Map (User-Configured):** You can define a mapping between the In Port and Out Port.
 - In Port refers to the TCP destination port received from the client.
 - Out Port is the TCP port used to send decrypted traffic to inline tools.
- **Priority 2 — Default Out Port:** This port is used when the incoming port does not match any entry in the configured port map.

NOTE: Decryption Port Mapping and Tool Early Inspect cannot be configured at the same time.

Enable or Disable Tool Bypass

Tool bypass determines whether specific traffic types are sent to inline tools. You can enable or disable tool bypass for the following types of traffic:

- TLS/SSL decrypted traffic
- Non-decrypted SSL traffic (non-TLS/SSL TCP)
- Non-TLS/SSL traffic (non-TCP)

By default, tool bypass is disabled for all traffic types. This means that all decrypted TLS/SSL, non-decrypted TLS/SSL, and non-TLS/SSL traffic is sent to the tools for inspection.

When you enable tool bypass for a traffic type, that specific traffic is excluded from tool processing and not sent to the inline tools.

High Availability Active Standby

Inline network High Availability (HA) in Active/Standby mode supports detection of link switch overs triggered by upstream devices.

When an upstream device, such as a firewall, performs an HA failover, the system identifies the change and continues forwarding traffic through the correct inline network.

For example, in an inline TLS/SSL network group with two network port pairs (Na1/Nb1 and Na2/Nb2), incoming traffic may shift from Na1 to Na2 during an upstream failover.

The system automatically detects this transition and maintains traffic continuity by routing packets through the appropriate inline link.

By default, this feature is disabled.

NOTE: Do not enable this option if the inline TLS/SSL network group operates in an Active/Active configuration.

Inline Network Group Multiple Entry

An inline network group topology can include multiple network port pairs (for example, Na1/Nb1 and Na2/Nb2).

With multiple port pairs, traffic from a network interface may traverse the system more than once.

Intercepted traffic from one interface can reenter the system through another interface within the same network group, as shown below.

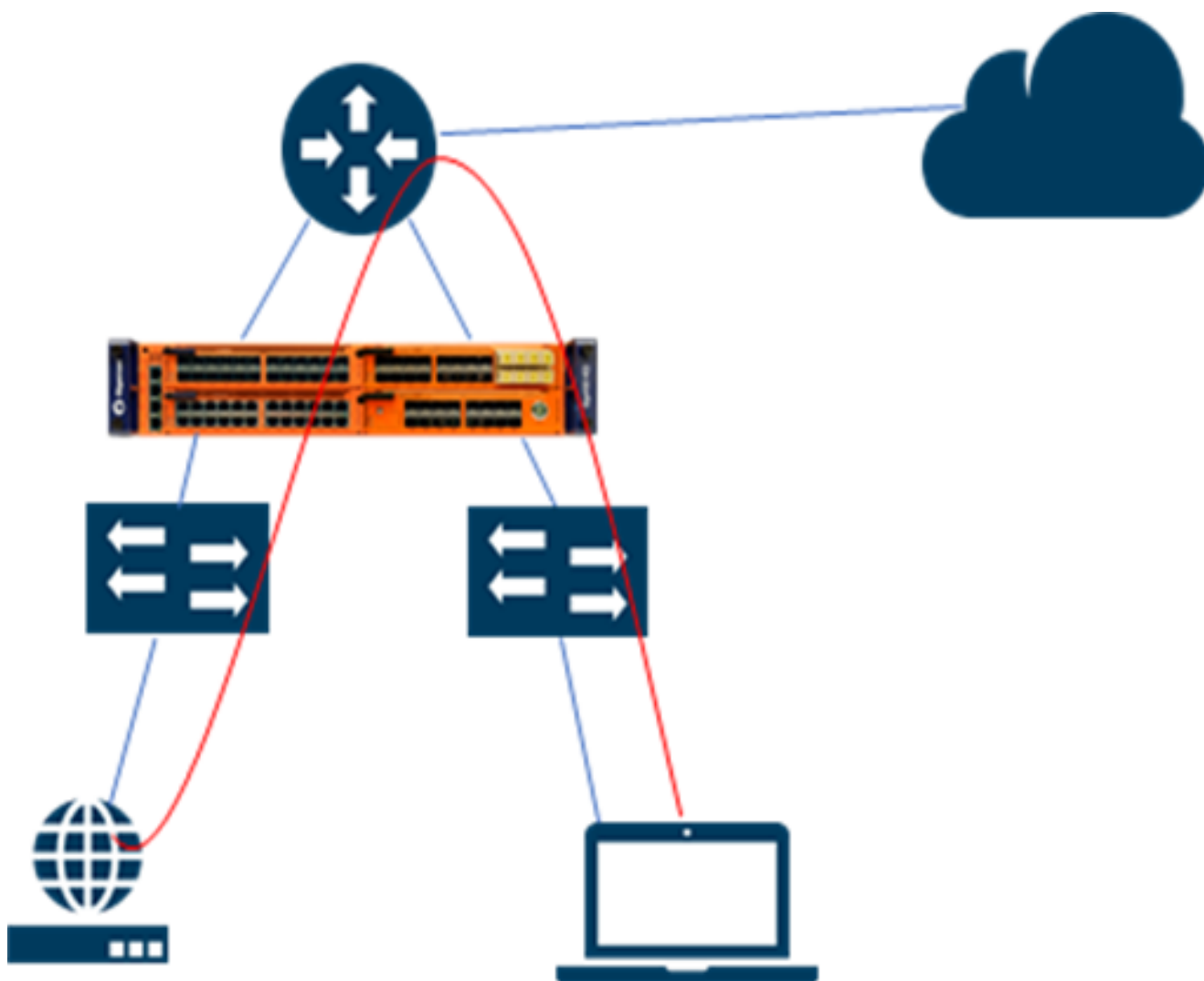


Figure 18 *Inline TLS/SSL Inline Network Group Configuration*

Inline TLS/SSL – Multiple Entry Behavior

When the inline TLS/SSL appliance is positioned between internal devices and the upstream router, traffic from internal devices to the Internet is intercepted by the appliance.

If internal devices associated with different network port pairs in the same group communicate with each other, their traffic first travels from the source device to the appliance, then to the upstream router, and finally reenters the appliance through another port pair to reach the destination device.

The appliance maintains the inline incoming interface (for example, Na1) for each connection.

If subsequent traffic from the same connection reenters through a different interface within the same group (for example, Na2), the appliance forwards the packets directly to the corresponding opposite interface (Nb2) without additional processing.

This enables seamless reentry handling for ongoing connections. Traffic that reenters through the same network port pair (for example, Nb2 → Na2) is not supported.

Similarly, any connection that uses more than the original network pair (for example, first packet on Na1/Nb1 and later through another pair) is unsupported.

All traffic for a connection must continue through the same port pair used by the first packet.

You can enable or disable Inline Network Group Multiple Entry in the profile settings. By default, this feature is disabled.

Tool Early Engage

In a Layer 3 topology, inline tools may need to modify the MAC address or VLAN IDs when forwarding client traffic back to the server.

The Tool Early Engage option allows inline tools to perform these modifications effectively.

When a client initiates a connection, the appliance first establishes the connection with the inline tool before connecting to the server.

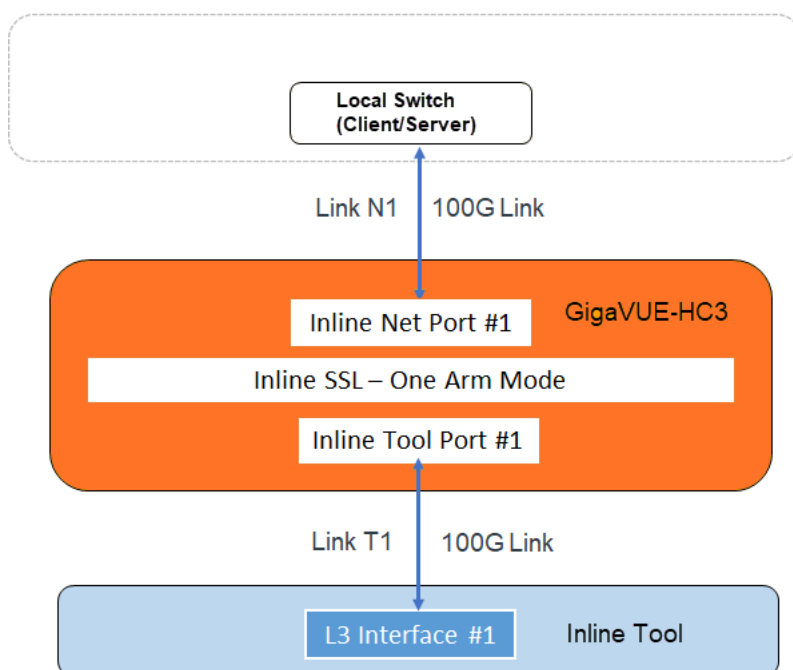
This early engagement enables the inline tool to adjust MAC addresses or VLAN IDs as needed when sending traffic back to the server.

**Notes:**

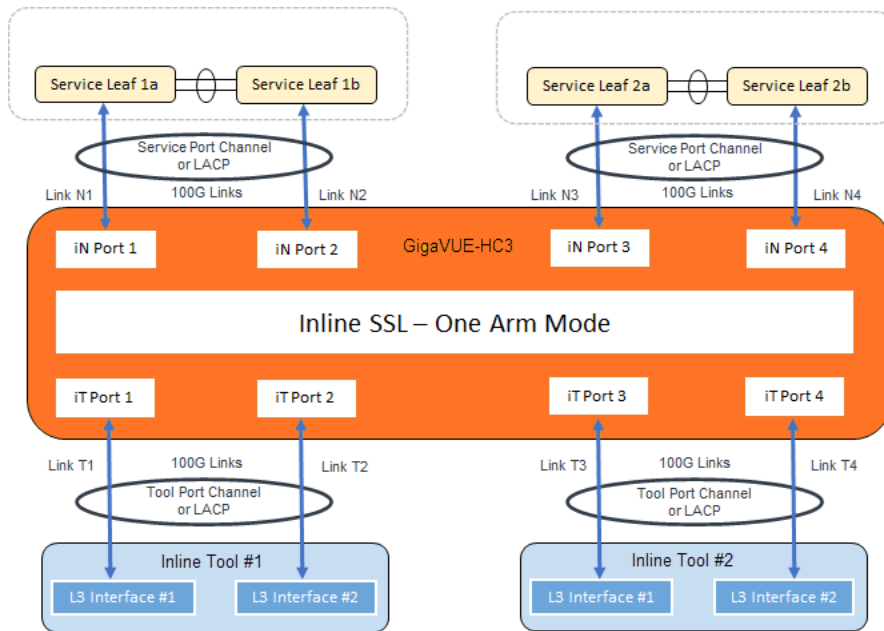
- Tool Early Engage can be enabled for a policy profile as a standalone feature, even when One-Arm mode is not used.
- Tool Early Engage and Tool Early Inspect cannot be configured together.

One-Arm Mode

In a Layer 3 topology, One-Arm mode allows both client and server traffic to traverse the same physical or logical link (for example, an aggregate port channel). You can configure this only after enabling Tool Early Engage.



For each connection between the client and server, there are two TCP sessions established between GigaSMART and the inline network and two TCP sessions established between GigaSMART and the inline tool. In the above diagram, you can see that with the One-Arm mode enabled, both TCP sessions from the inline network side arrive at GigaSMART on the same link N1. The TCP sessions from the inline tool side arrive at GigaSMART on the same link T1.



In the above figure, the inline network link and inline tool link works as a pair – (N1, T1), (N2, T2), (N3, T3), and (N4, T4). The GigaSMART sends traffic to the corresponding tool link of the received network link. Similarly, GigaSMART sends the traffic back to the server on the corresponding network link of the received inline tool link. For example, when a connection comes to GigaSMART from the inline network N1, after decryption, GigaSMART sends clear text traffic to inline tool on T1. The return traffic of the same connection arrives at GigaSMART on the inline tool link T2. GigaSMART then re-encrypts the traffic and sends it to the server on the inline network link N2.

Failover Support

If either member of a link pair fails, the paired link is also taken down to preserve flow consistency.

This behavior can be achieved by configuring **Link Aggregation Control Protocol (LACP)** or enabling **Link Failure Propagation (LFP)** between each network-tool link pair.

One-Arm Mode — Rules and Notes

Before enabling One-Arm mode for a policy profile, observe the following:

- Connect inline network interfaces to the Na side and inline tool interfaces to the Nb side.
- Tool Early Engage must be enabled.
- One-Arm mode is not supported on the Flexible Inline Decryption solution.
- To route packets through a firewall, configure the client and server gateways to use the router's IP address.
- Second-level OOB is not supported; use map-passall from the tool port instead.

- When both Tool Early Engage and One-Arm mode are enabled, MAC addresses and VLAN IDs can be changed, but IP addresses, ports, and protocols cannot.
- Inline Network Group Multiple Entry and High Availability Active/Standby features are not supported.
- Enable LACP on both network and tool sides, and LFP on the inline-network configuration.
- Bypass-tool options in the Inline TLS/SSL profile (Decrypt, No-Decrypt, Non-TLS/SSL) require another router on the network side to route packets.
- The name “one-arm” is a reserved keyword. Do not use it as an alias for any inline network, tool, or map. Rename existing aliases before upgrading to GigaVUE-OS 5.12.xx.
- Resilient Inline Arrangement (RIA) is not supported with One-Arm mode.
- If “one-arm” is configured as a tool in an inline second-level map, the VPort status displays as *Up (not Up (Normal))*.
- One-Arm mode cannot coexist with the **Tool Early Inspect** feature.

Tool Early Inspect

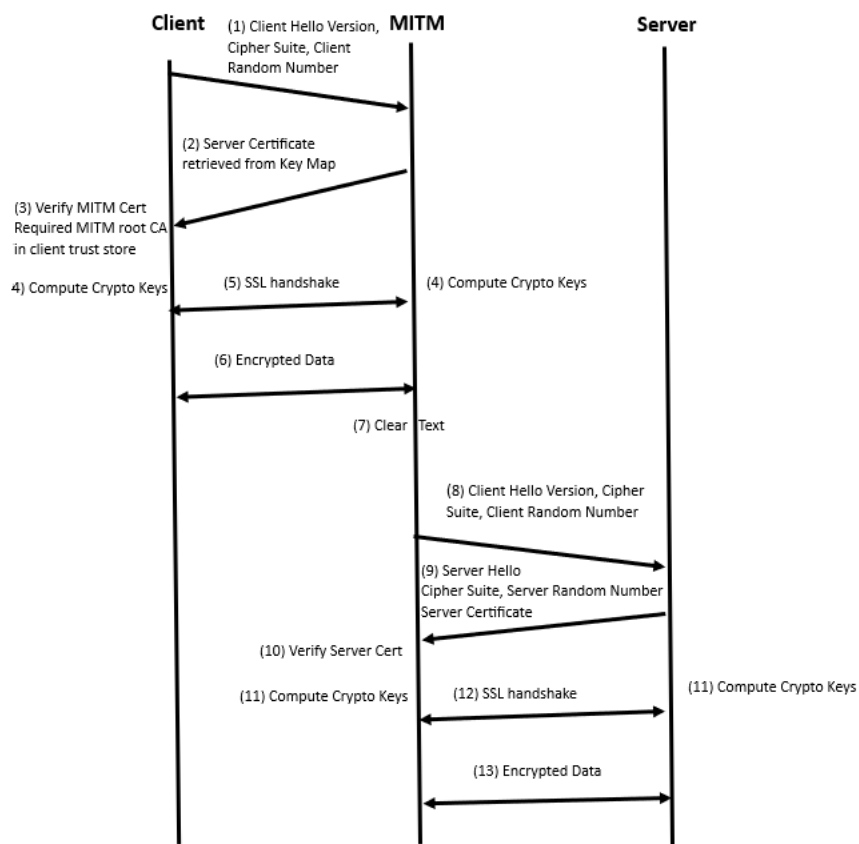
In a standard Inline TLS/SSL deployment, the node intercepts the TLS/SSL session between the client and server and forwards decrypted data to the inline tool after completing the handshake with both ends.

This means that connections rejected by the tool are still fully established to the server. With Tool Early Inspect, the client's handshake completes first using the configured server certificate and key.

Decrypted data is then sent to the inline tool for inspection before connecting to the real server, ensuring only valid sessions proceed.

NOTE: Tool Early Inspect is supported only in inbound deployment modules. Outbound and hybrid modules are not supported.

The below diagram shows how a client handshake sequence would be once the Tool Early Inspect is enabled.



Inline TLS/SSL L3 Tool NAT/PAT Support

This feature offloads TLS decryption from Layer-3 inline tools that perform NAT/PAT (Network/Port Address Translation).

The GigaSMART engine maintains two independent sessions—one toward the client and one toward the server—to achieve this separation.

Supported Platforms

- Gen3 cards in GigaVUE-HC1 and GigaVUE-HC3
- GigaVUE-HC1-Plus

HTTP 2.0 Downgrade

When NAT/PAT mode is enabled, the HTTP 2.0 Downgrade option is enabled by default. HTTP 2.0 traffic is downgraded to HTTP 1.1 for decryption. If the downgrade option is disabled, HTTP 2.0 traffic is forwarded without decryption.

Decryption Port Mapping

In the Inline SSL application profile, you can now send decrypted traffic to user-defined L4 ports. This feature supports the following scenarios:

- One-to-One Tool Port Address Translation: A specific clear text port for Inline SSL traffic is assigned, and after decryption, the flow is directed to this assigned port
- Many-to-One Tool Port Address Translation: Multiple incoming SSL Layer 4 ports are mapped to a specific single clear text Layer 4 port. If no specific mapping exists, decrypted traffic will be directed to the designated clear text port
- No Port Mapping- If one-to-one or default port mappings are not configured, decrypted traffic will continue to use the same original L4 port from the incoming encrypted data.

To configure this feature, enable the NAT/PAT Mode and then configure the port details in TCP Port MAP Decryption.

The port details can be configured through the *apps inline-ssl* command. Refer to GigaVUE-OS CLI Reference Guide.

Limitations

- L3 Tool port address translation does not apply to web proxy scenarios. Therefore, support for tool port address translation will not be included for web proxy traffic.
- The Start TLS port should not be configured in any port mapping settings, whether one-to-one or as a default port map.
- Any L4 port expected to receive the first data from the server must not be included in the port mapping configuration.

Cache Server Certificate Timeout

The server information is cached for performance optimization. The default time out is 30 minutes. The cache is flushed when the cache timeout value is set to zero. The cache is disabled when the timeout value is set to zero.

Refer to the following Gigamon Validated Design for more information:

- [Offloading TLS Decryption for an One-Armed Inline Tool in L3 with NAT/PAT Mode](#)
- [Enabling GigaSECURE TLS Decryption to Offload SSL Inspection from Next-Generation Firewall](#)

Limitations

- Decrypted data visible to inline tools is limited to HTTP/1.1 over TLS.
- StartTLS traffic is not decrypted.
- Tool bypass is not supported because all packets must pass through the inline tool.
- Cannot coexist with Network Group Multiple Entry, Inline Network HA, RIA, Tool Early Engage, Tool Early Inspect, or One-Arm mode.
- IPv6 is unsupported in release 6.1.00 but supported from 6.2.00 onward.

Cache Persistence

There are four in-memory caches as follows. They are not configurable.

- Re-signed certificate cache
- URL category cache
- Revocation certificate cache
- Session resumption cache

Caches are maintained for Internet lookups such as URL categorization and certificate revocation checks using OCSP or CRL for faster subsequent lookups. The cache persistence feature allows the information to be saved on the GigaVUE-FM, GigaVUE HC Series node in the control card's persistent storage so that it can be retrieved in case of reboots. This allows the GigaSMART card to start with the information learned earlier. This feature is enabled by default and can be disabled if needed.

On the **Cache Persistence** page, you can:

- Search for specific entries in the caches using the **Find Entries** option
- Clear the caches using the **Clear Store** option from the **Actions** drop-down menu
- Display a summary of the records.

GigaSMART Overload Bypass

Packet buffers, CPU, memory utilization and concurrent connections are monitored for overloaded conditions. GigaSMART goes to bypass when resource usage exceeds thresholds. Existing connections will continue to be processed by GigaSMART, but any new connections will be bypassed.

Table 3: Overload Bypass Connections and Thresholds

Criteria	GigaVUE-HC1	GigaVUE-HC3 (per GigaSMART Engine)
Maximum connections per second	1500	5000
Maximum connections	100000	200000

Criteria	GigaVUE-HC1	GigaVUE-HC3 (per GigaSMART Engine)
Resource Packet Buffer	Overload threshold for packet buffer resources for GigaSMART operations. Default is 80% (configurable)	
Resource CPU	Rising threshold for GigaSMART CPU statistics. Default is 90% (configurable)	
Heap exhaust	80%	

To configure the Packet Buffer and CPU threshold values, navigate to **GigaSMART > GigaSMART Operations (GSOP) > Resource Buffer** and configure the following:

- Resource Packet Buffer Overload Threshold (%)
- Resource CPU Overload Threshold (%)

▼ Resource Buffer

Enable Resource Packet Buffer	☒
Resource Packet Buffer Overload Threshold (%)	80
Enable Resource CPU	☒
Resource CPU Overload Threshold (%)	90
Application Session Filtering	☐
Metadata Export	☐
Cross Packet Match Flows (x100K)	0 0 is disabled

CPU Overload Threshold

Due to sudden bursts of traffic, the GigaSMART CPU can become too busy and drop packets. However, when a system or application reaches a threshold, SSL sessions can be bypassed. When a maximum CPU is reached, incoming connections will be bypassed.

When the CPU overload threshold is set to a configured value, (for example, 90%), the lower threshold is set to two-third of the CPU overload threshold configured (in this example 60%). A mean threshold is calculated, which will be the average of the CPU overload threshold and the lower threshold (in this example 75%).

The following actions will be taken:

- If the CPU hits the overload threshold, all new SSL connections will be bypassed.
- If the CPU reduces to the mean threshold, half of the new SSL connections will be bypassed.
- If the CPU reduces further to the lower threshold, all new SSL connections will be decrypted.

If you choose connectivity-over-security, the CPU overload threshold must be set to the lower threshold value.

Inline TLS/SSL Monitor Mode

Use the inline TLS/SSL monitor mode to assist in understanding your network topology. Monitor mode provides information about the traffic going to the GigaSMART card, which can help to learn about your deployment. When monitor mode is enabled, the monitor application collects information such as TCP ports used and VLAN information about the incoming traffic.

After inline TLS/SSL decryption is configured and monitor mode is enabled, the inline TLS/SSL application does not terminate the session. Instead, the monitor application collects information and forwards packets to the tool port or network port based on the configuration of the non-TLS/SSL TCP bypass action. For any Monitor mode, you can enable or disable seamlessly without any other configuration changes.

Monitor mode is disabled by default. To enable the monitor mode, refer to [Configure TLS/SSL Decryption Solutions](#).

For packets coming from the network port, the monitor application collects packet flow information.

From the information collected from monitor mode, you can analyze the following cases:

- duplicate TCP SYN—For a given session, the SYN messages with a different packet signature than 5tuple, for example, a different VLAN ID, indicates the packet is coming from multiple paths.
- asymmetric routing—For a given session, packets arriving from multiple network interfaces indicates a packet is coming from multiple paths.

Inline SSL Monitor mode only captures TCP information, not SSL information. However Inline SSL Persistent Monitor mode captures both TCP and SSL information.

NOTE: Monitor mode is supported for standalone nodes only, not for nodes in a cluster.

Inline TLS/SSL Traffic Filtering

Because TLS/SSL/ connections can carry sensitive data, some organizations may require the TLS/SSL connections to avoid inspection. The SSL connections that carries user data such as financial or health care information can be bypassed without inspection, based on a configured policy.

Based on the decryption policies, some connections are not decrypted and are passed through, optionally through tools, without decryption. The inline SSL decryption solution respects data privacy and supports compliance.

Inline SSL decryption provides different ways to filter traffic, as follows:

- No-decrypt lists specify traffic to always pass through. A no-decrypt list policy states that traffic from certain sites should always skip decryption.
- Decrypt lists specify traffic to always decrypt. A decrypt policy states that traffic from certain sites should always be decrypted.
- Both No-decrypt lists and Decrypt lists IP addresses, IP subnets and explicit wildcards as domain rules.
- URL Web Services categorizes the URLs by their type, such as MyBank.com is a financial institution, so as a policy, do not decrypt that traffic. This is also called URL filtering. Typically, banking and health care information are not decrypted.
- Policy rules based on network attributes, such as
 - Source IPv4 address
 - Destination IPv4 address
 - VLAN
 - L4 port

No-decrypt Listing Policy

No-decrypt lists are typically used in environments where the default is to decrypt, excepting for certain sites or classes of sites which cannot be decrypted for legal or compliance reasons. By default, traffic that is not to be decrypted is forwarded to the tools unless otherwise configured.

A no-decrypt list file can contain a maximum of 10,000 entries.

Decrypt Listing Policy

Decrypt listing is typically used at sites where specific classes of connections must be decrypted, although the default for other traffic is not to decrypt. Decrypt listed domains and host names will always be decrypted.

A decrypt list file can contain a maximum of 10,000 entries.

No-Decrypt/Decrypt List Policy — Rules and Notes

While configuring a No-Decrypt / Decrypt policy keep in mind the following rules and notes:

1. The maximum domain/hostnames support per list is 10000.
2. IP Subnets are supported from 5.13.01 version. Example, 10.10.10.0/24.
3. Special characters are not supported unless they are used to define domain names, such as `* . - @` are supported for domain names and `/` is supported if IP subnet is defined. `#` is supported to comment out a line. Example of a text file format would be as follows:
 - *.google.com
 - www.gigamon.com
 - gigamon.com
 - domain-registration.com.us
 - 10.10.1.1
 - 10.10.1.0/24
4. Range of IP addresses are not supported example, 10.10.10.10-20.
5. Use a newline for each entry. Adding characters such as `,` `;` are not supported.
6. The domain gigamon.com as an entry matches only gigamon.com. To match all subdomains of gigamon.com on v5.9+, use *.gigamon.com.
7. If the system has large set of decrypt/no-decrypt list entries, GigaVUE-FM stats page and CLI stats command does not display any output. Wait for 5 to 10 minutes after reloading to check the inline SSL show stats command in CLI and stats page in GigaVUE-FM.

IP Address Subnet with Longest Prefix Match(LPM)

The No-decrypt and Decrypt database allows the user to utilize IP subnets. This allows the user to configure overlapping IP addresses, in decrypt and no-decrypt database. The decision to decrypt or no-decrypt will be based on the longest prefix match of the IP entries available in the decrypt /no-decrypt database.

The format is as follows *subnet (no space) /prefix*. Eg: 191.1.1.0/32

URL Categorization

URL categories make it convenient to apply policies on all the possible URLs matching the category and reduce the number of policy rules. Categorization is based on the hostname in the TLS Server Name Indication (SNI) or the subject name from the server certificate if there is no SNI. There are 83 categories including one for Uncategorized, which is a default category for URLs that do not match any of the other 108 categories. The categories are fixed meaning that categories cannot be added, deleted or modified.

GigaSMART ships with a local database of 1M entries and will also perform a cloud lookup for those hosts not found in the local database. The URL Web Service provides the URL categorization. The URL database is updated daily from the URL Web Service. Each update likely adds new entries and purges other entries, but always keeping the database at 1M entries.

NOTE: When a URL is not in the cache, for cloud look-ups the stack port interface on GigaSMART must be configured to provide Internet access.

URL Category Look-ups and Caching

As part of the Inline SSL processing, URL category look-ups are performed against the database. If the URL is not found in the database, then a lookup is performed against the local cache. If the URL is not found in the local cache, then an external lookup to the URL Web Services may be performed, if configured. If the URL is found in the external look-up, then it is dynamically saved in the local cache. Future look-ups may then find the URL in the local cache instead of requiring the external look-up.

NOTE:

- For TLS connections containing SNI in the Client Hello, do not perform URL category look-up in the certificate phase.
- CN based evaluation can be performed using the configuration option.

The local cache can hold up to 250k entries (in addition to the 1M entry database). The local cache works like a circular buffer – older entries are discarded to make room for newer ones if the cache is full. Each cache entry is valid for 24 hours and updated with current time stamp whenever an entry is made. If an expired entry is encountered, a new query is issued to the URL Web Services to refresh the entry in the cache. Expired entries don't get actively deleted from the cache.

While the URL Web Service is hosted on AWS, external look-ups need to occur very quickly. Gigamon provides a timeout option, up to 10 seconds for external URL category look-ups via the URL cache miss defer option.



Notes:

- URLs may get re-categorized as part of updates from the URL Web Services. This is transparent to Gigamon and customers.
- The URL category classification is fixed, and a new category cannot be added. Gigamon provides the no-decrypt list/decrypt list functionality, which can achieve the same result as creating a custom category.
- If a URL belongs to multiple categories, any no-decrypt policy would take precedence over all decrypt policies.

Inline SSL URL categories

The following are the list of Inline SSL URL categories with examples.

NOTE: Gigamon does not endorse any of the following categories, descriptions, and examples, but replicated the information from the URL Web Services. Some categories are presented without examples since they are not appropriate.

Category Name	Description and Examples
Abortion	Abortion topics, either pro-abortion and anti-abortion.
Abused Drugs	Discussion or remedies for illegal, illicit, or abused drugs such as heroin, cocaine, or other street drugs. This category includes information on the misuse of non-proscribed substances (eg. "glue sniffing"), or the misuse of prescription medications.
Adult and Pornography	Sexually explicit material for the purpose of arousing a sexual or prurient interest. Online groups, including newsgroups and forums, that are sexually explicit in nature.
Alcohol and Tobacco	Sites that provide information on, promote, or support the sale of alcoholic beverages or tobacco products and associated paraphernalia.
Auctions	Sites that support the offering and purchasing of goods between individuals as their main purpose. Does not include classified advertisements. http://ebay.co http://quibids.com
Botnets	These are URLs, typically IP addresses, which are determined to be part of a Bot network, from which network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.
Business and Economy	Business firms, corporate websites, business information, economics, marketing, management, and entrepreneurship. http://samsung.com http://ups.com
Content Delivery Networks	Delivery of content and data for third parties, including ads, media, files, images, and video. http://metacdn.co http://edgestream.com
Cheating	Sites that support cheating on examinations and contain such materials, including free essays, exam copies, plagiarism, etc.
Computer and Internet Info	General computer and Internet sites, technical information. SaaS sites and other URLs that deliver internet services. http://ranking.co http://system.netsuite.com
Computer and Internet Security	Computer/Internet security, security discussion groups. http://siteadvisor.co http://webroot.com

Category Name	Description and Examples
Confirmed Spam Sources	Confirmed SPAM sources.
Cult and Occult	Internet resources which include discussion of astrology, spells, curses, magical powers, satanic rituals or supernatural beings. This includes horoscope sites.
Dating	Dating websites focused on establishing personal relationships. http://eharmony.com
Dead Sites	These are dead sites that do not respond to http queries. Policy engines should usually treat these as “Uncategorized” sites. http://google.com http://whitehouse.info
Dynamic Content	Domains that generate content dynamically based on arguments to their URL or other information (like geo-location) on the incoming web request. booking.com
Education Institution	Pre-school, elementary, secondary, high school, college, university, and vocational school and other educational content and information including enrollment, tuition, and syllabus. http://mit.edu http://ox.ac.uk
Entertainment and Arts	Motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. http://eonline.com http://warnerbros.com
Fashion and Beauty	Fashion or glamour magazines, beauty, clothes, cosmetics, style. http://visionmodels.co.uk http://genejuarez.com
Financial Services	Banking services and other types of financial information, such as loans, accountancy, actuaries, banks, mortgages, and general insurance companies. Does not include sites that offer market information, brokerage or trading services. http://firstpremierbankcards.com http://paypal.com
Gambling	Gambling or lottery web sites that invite the use of real or virtual money. Information or advice for placing wagers, participating in lotteries, gambling, or running numbers. Virtual casinos and offshore gambling ventures. Sports picks and betting pools.
Games	Playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. Also includes sites dedicated to selling board games as well as journals and magazines dedicated to game playing. http://duowan.com http://ubi.com
Government	Information on government, government agencies and government services such as taxation, public, and emergency services. Also includes sites that discuss or explain laws of various governmental entities. Includes local, county, state, and national government sites.

Category Name	Description and Examples
	http://www.nasa.gov http://premier-ministre.gouv.fr
Gross	Sites that contain material which describe or display material which would be considered foul or disgusting. Examples would include bodily fluids, injuries, gore.
Hacking	Illegal or questionable access to or the use of communications equipment/software. Development and distribution of programs that may allow compromise of networks and systems.
Hate and Racism	Sites that contain content and language in support of hate crimes and racism.
Health and Medicine	General health, fitness, well-being, including traditional and non-traditional methods and topics. Medical information on ailments, various conditions, dentistry, psychiatry, optometry, and other specialties. http://webmd.com http://missionvalleymedical.com
Home and Garden	Home issues and products, including maintenance, home safety, decor, cooking, gardening, home electronics, design, etc. http://homedepot.com http://waysidegardens.com
Hunting and Fishing	Sport hunting, gun clubs, and fishing. http://fishingworks.com http://wildlifelicense.com
Illegal	Criminal activity, copyright and intellectual property violations, etc.
Image and Video Search	Photo and image searches, online photo albums/digital photo exchange, image hosting. http://images.google.fr http://gettyimages.com
Individual Stock Advice and Tools	Promotion and facilitation of securities trading and management of investment assets. Also includes information on financial investment strategies, quotes, and news. http://stockstar.com http://morningstar.com
Internet Communications	Internet telephony, messaging, VoIP services and related businesses. http://skype.com http://www.chatib.com/
Internet Portals	Web sites that aggregate a broader set of Internet content and topics, and which typically serve as the starting point for an end user. http://yahoo.com http://qq.com
Job Search	Assistance in finding employment, and tools for locating prospective employers, or employers looking for employees. http://monster.com http://51job.com

Category Name	Description and Examples
Keyloggers and Monitoring	Downloads and discussion of software agents that track a user's keystrokes or monitor their web surfing habits.
Kids	Sites designed specifically for children and teenagers. http://www.mundogaturro.com http://www.poptropica.com
Legal	Legal websites, law firms, discussions and analysis of legal issues. http://www.pepperlaw.com http://earlcaterlaw.com
Local Information	City guides and tourist information, including restaurants, area/regional information, and local points of interest. http://downtownlittlerock.com http://sandiegorestaurants.com
Malware Sites	Malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code.
Marijuana	Marijuana use, cultivation, history, culture, legal issues.
Military	Information on military branches, armed services, and military history. http://defense.gov http://www.mod.uk
Motor Vehicles	Car reviews, vehicle purchasing or sales tips, parts catalogs. Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks and RVs. Journals and magazines on vehicle modifications. http://www.carmax.com http://carsales.com.au
Music	Music sales, distribution, streaming, information on musical groups and performances, lyrics, and the music business. http://itunes.com http://bandcamp.com
News and Media	Current events or contemporary issues. Also includes radio stations, magazines, online newspapers, headline news sites, newswire services, personalized news services, and weather sites. http://abcnews.go.com http://newsoftheworld.co.uk
Nudity	Nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect but may include sites containing nude paintings or photo galleries of artistic nature.
Online Greeting Cards	Online Greeting card sites. http://123greetings.com http://greeting-cards.com
Online Personal Storage	Online storage and posting of files, music, pictures, and other data. http://box.net http://freefilehosting.net
Open HTTP Proxies	The proxy servers that are accessible by any Internet user.

Category Name	Description and Examples
P2P (Peer to Peer)	Peer to peer clients and access that includes torrents, music download and programs.
Parked Sites	Parked domains are URLs which host limited content or click-through ads which may generate revenue for the hosting entities but generally do not contain content useful to the end user. Also includes Under Construction, folders, and web server default home pages. http://000.com http://buythisdomain.com
Pay to Surf	Sites that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
Personal Sites and Blogs	Personal websites posted by individuals or groups, as well as blogs. http://blogger.com http://wordpress.org
Philosophy and Political Advocacy	Politics, philosophy, discussions, promotion of a particular viewpoint or stance in order to further a cause. http://philosophynow.org http://political.com
Phishing and Other Frauds	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personal information from a user. These sites are typically quite short-lived, so examples may not last long.
Private IP Addresses	RFC 1918, Address Allocation for Private Intranets. 10.0.0.0 - 10.255.255.255 (10/8 prefix) 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
Proxy Avoid and Anonymizers	Proxy servers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering.
Questionable	Tasteless humor, "get rich quick" sites, and sites that manipulate the user experience or client in some unusual, unexpected, or suspicious manner.
Real Estate	Information on renting, buying, or selling real estate or properties. Tips on buying or selling a home. Real estate agents, rental or relocation services, and property improvement. http://prudentialproperties.com http://realtor.com
Recreation and Hobbies	Information, associations, forums and publications on recreational pastimes such as collecting, kit airplanes, outdoor activities such as hiking, camping, rock climbing, specific arts, craft, or techniques; animal and pet related information, including breed-specifics, training, shows and humane societies. http://petloverspublications.com http://craftster.org
Reference and Research	Personal, professional, or educational reference material, including online dictionaries, maps, census, almanacs, library catalogues, genealogy, and scientific information. http://reference.com http://wikipedia.org

Category Name	Description and Examples
Religion	Conventional or unconventional religious or quasi-religious subjects as well as churches, mosques, synagogues, or other places of worship. http://therocksandiego.org http://biblesociety.ca
Search Engines	Search interfaces using key words or phrases. Returned results may include text, websites, images, videos, and files. http://google.com http://sogou.com
Sex Education	Information on reproduction, sexual development, safe sex practices, sexually transmitted diseases, sexuality, birth control, sexual development, and contraceptives. http://sexetc.org
Shareware and Freeware	Sites that contains softwares, screensavers, icons, wallpapers, utilities, ringtones including downloads that request a donation on open source projects. http://download.com http://sourceforge.net
Shopping	Department stores, retail stores, company catalogs and other sites that allow online consumer or business shopping to purchase goods and services. http://amazon.com http://groupon.com
Social Network	Social networking sites that have user communities where users interact, post messages, pictures, and otherwise communicate. http://facebook.com http://twitter.com
Society	A variety of topics, groups, and associations relevant to the general populace, broad issues that impact a variety of people, including safety, children, societies, and philanthropic groups. http://dar.org http://unicefusa.org
Spam URLs	URLs contained in SPAM.
Sports	Team or conference web sites, international, national, college, professional scores and schedules; sports-related online magazines or newsletters, fantasy sports and virtual sports leagues. http://nba.com http://schoenen-dunk.de
Spyware and Adware	Spyware or Adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization, also unsolicited advertising popups and programs that may be installed on a user's computer.
Stream Media	Sales, delivery, or streaming of audio or video content, including sites that provide downloads for such viewers. http://youtube.com http://ustream.tv

Category Name	Description and Examples
Swimsuits and Intimate Apparel	Swimsuits, intimate apparel or other types of suggestive clothing.
Training and Tool	Distance education, trade schools, online courses, vocational training, software training, and skills training. http://trainingtools.com http://prezi.com
Translation	Language translation sites that allow users to see URL pages in other languages. http://translate.google.com http://microsofttranslator.com
Travel	Airlines and flight booking agencies. Travel planning, reservations, vehicle rentals, car rentals, descriptions of travel destinations, promotions for hotels or casinos. http://cheapflights.com http://expedia.com
Uncategorized	Sites that have not been categorized by URL Web Service.
Unconfirmed Spam Sources	Unconfirmed SPAM sources.
Violence	Sites that advocate violence, depictions and methods, including game/comic violence, and suicide.
Weapons	Sales, reviews, descriptions of weapons such as guns, knives, martial arts accessories.
Web Advertisements	Advertisements, media, content, and banners. http://casalemedia.com http://justwebads.com
Web Based Email	Sites offering web-based email and email clients. http://google.com/mail http://foxmail.com
Web Hosting	Free or paid hosting services for web pages and information concerning their development, publication, and promotion. http://siteground.com http://bluehost.com

Proxy Server Profile for URL Categorization and Certificate Revocation status

To ensure a stable security network you can now redirect URL look-ups and Certificate Revocation status checks to a Proxy Server Profile. This Proxy Server profile will be attached to your Inline SSL deployment . To learn more refer to *Proxy Server Configuration* section in GigaVUE Administration Guide

Inline TLS/SSL Decryption Deployments

Inline TLS/SSL decryption can be deployed in two main ways – Inbound and Outbound.

Inbound Deployment

In an inbound deployment, the client is on the Internet, and the server is inside the enterprise network. The GigaVUE node is also deployed inside the network, on the server side. To decrypt traffic, the GigaVUE node must have access to the server's private keys. This setup enables Man-in-the-Middle (MitM) decryption. The traffic uses Diffie-Hellman or Perfect Forward Secrecy (PFS) encryption.

Refer to Diagram 1 for an example of inbound inline TLS/SSL decryption deployment.

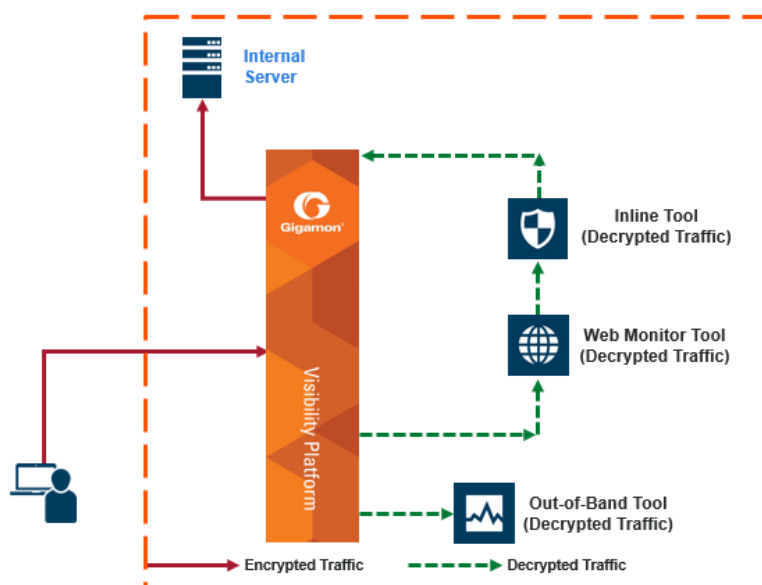


Figure 19 Inbound Deployment of Inline TLS/SSL Decryption

Inbound Deployment with Client Certificate Authentication (mTLS)

In a standard inbound deployment, the GigaVUE node is deployed on the server side and decrypts traffic destined for internal servers using their private keys. With mTLS enabled, the same topology can enforce client certificate authentication at the inline TLS/SSL layer.

In this deployment model:

- The client resides on the Internet or external network.
- The server and GigaVUE node reside inside the protected enterprise network.
- The server is configured to require client certificates for selected applications (for example, user-facing portals or API endpoints).
- The Inline TLS/SSL application:
 - Validates the server certificate against the server trust store.
 - Validates the client certificate against the client trust store.
 - Applies policy to accept or reject the session based on the outcome of both validations.

The resulting end-to-end connection is still an mTLS session from the client's perspective, but certificate validation and decryption are offloaded to the Inline TLS/SSL solution, which then forwards clear-text traffic to inline tools for inspection.

Outbound Deployment

In an outbound deployment, the client is inside the enterprise network, along with the GigaVUE node, which is deployed on the client side. The server is external, located on the Internet. In this case, the GigaVUE node acts as a trusted Man-in-the-Middle (MitM) but does not require access to the server's private key. It can still inspect TLS/SSL traffic.

Refer to Diagram 2 for an example of outbound inline TLS/SSL decryption deployment.

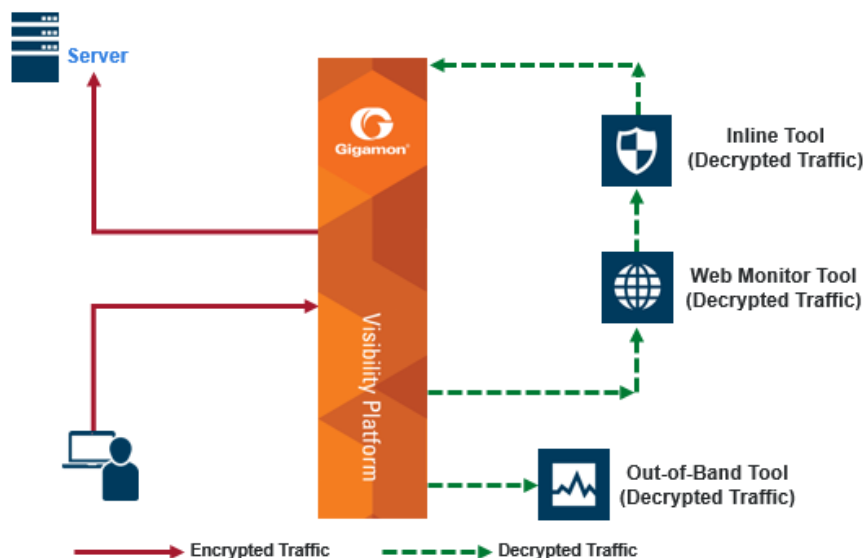


Figure 20 Outbound Deployment of Inline TLS/SSL Decryption

Basic Deployments for Inline TLS/SSL Decryption Solution

Choose from the following basic deployment methods to implement Inline TLS/SSL Decryption:

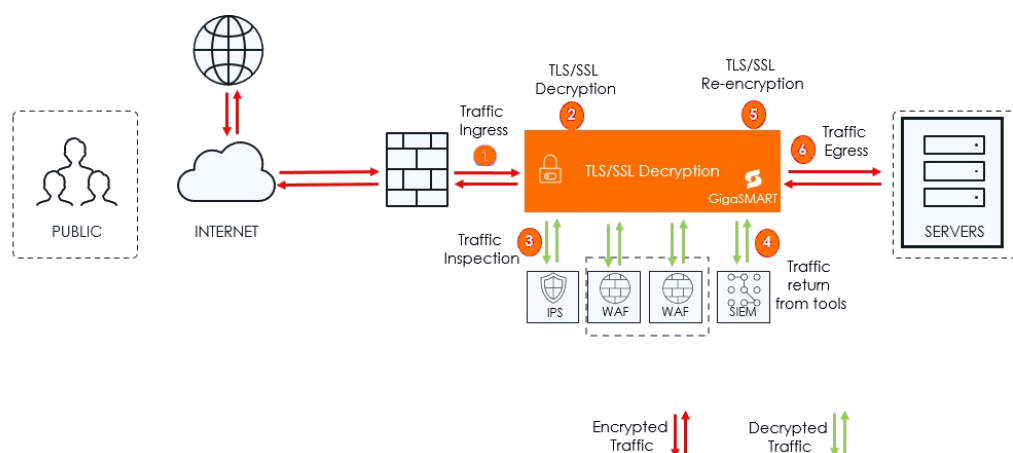
- [Inline TLS/SSL Decryption Solution with Layer 2 Transparent Tools](#)
- [Inline TLS/SSL Decryption Solution with Layer 3 Tools \(NAT-PAT\)](#)

Inline TLS/SSL Decryption Solution with Layer 2 Transparent Tools

In an Inline SSL deployment, encrypted traffic passes through a sequence of components for secure decryption, inspection, and re-encryption. This deployment is designed to support Layer 2 inspection tools that analyze traffic without altering its contents.

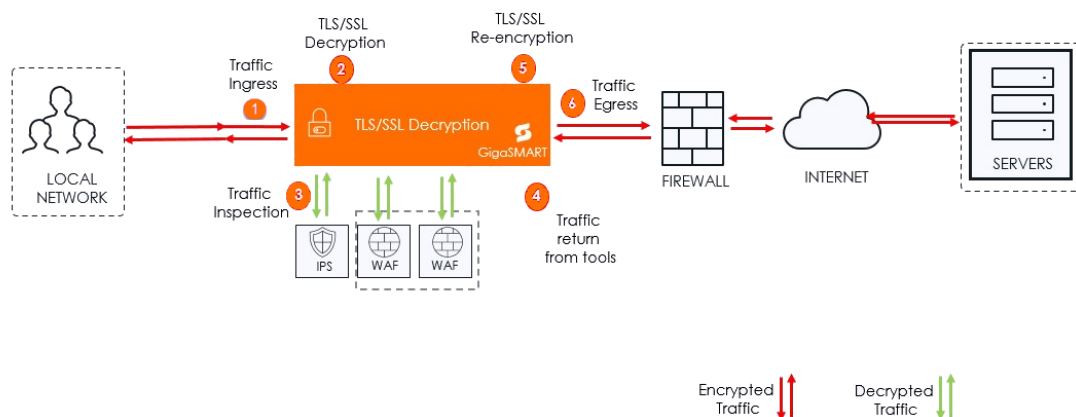
The below shown is an inbound deployment of Inline TLS/SSL Decryption.

Inline TLS/SSL Solution for Layer 2 / Transparent Tools- Inbound



The shown is an outbound deployment of Inline TLS/SSL Decryption.

Inline TLS/SSL Solution for Layer 2 / Transparent Tools-Outbound



2

The following steps describe the end-to-end flow:

1. **Traffic Ingress**-Traffic enters the system through the Inline Network Port (Ingress). This port acts as the first point of entry for all inbound encrypted traffic.
2. **TLS/SSL Decryption**-The traffic is directed to the GigaSMART engine, where the inline TLS/SSL application is. The engine decrypts the TLS/SSL traffic, making it readable for inspection tools.
3. **Traffic Inspection**-The decrypted traffic is forwarded to inline security tools (for example, IPS, WAF, SIEM, etc). These tools operate in Layer 2 (transparent) mode, meaning they inspect but do not modify packet contents. Tools may allow, alert on, or block traffic based on inspection results, but they do not change the actual data.
4. **Traffic Return from Tools**- after inspection, the traffic is returned to the GigaSMART engine. This ensures that only inspected traffic proceeds further.
5. **SSL Re-encryption**-The GigaSMART engine re-encrypts the traffic using the original TLS/SSL parameters.
6. **Traffic Egress**-The re-encrypted traffic is sent out through the Inline Network Port (Egress) to continue to the servers.

Rules and Notes

The following table lists rules and notes that you need to be aware of while configuring your deployment.

Rule / Feature	Details / Limitations
Exclusive Use	Inline tools in a flexible inline map cannot be used in classic inline or inline decryption maps. All inline networks and tools must belong to only one type of map.
Collector Maps	Only one unidirectional collector map is allowed for the same inline network. To use different VLANs in each direction, create separate unidirectional maps with unique VLAN tags. Tags can be set manually or assigned automatically by GigaVUE-FM.
Unsupported Features (GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA25E, GigaVUE-TA25, GigaVUE-TA400, GigaVUE-TA400E)	- Physical Bypass (no BPS card) - Flexible and Resilient Inline SSL (no GigaSMART card) - GRIP (no BPS card) - ICAP (no GigaSMART card) - Classic Inline Bypass
VLAN Tagging and OOB Copy Limits (GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus)	Flexible Inline Single VLAN Tag with monitoring mode may send incorrect VLAN tags. OOB copy packets may also have wrong tags. You cannot use BYPASS WITH MONITORING with MONITORING mode on the tool. OOB copy from inline network is not allowed in this mode.
Inline Map Limits — Bidirectional	GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus → 126 maps GigaVUE-HC1, GigaVUE-HC3 (CCv1 & CCv2), GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E → 256 or 512 maps depending on setup.
Inline Map Limits — Unidirectional	GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus → 252 maps GigaVUE-HC1, GigaVUE-HC3 (CCv1 & CCv2), GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E → 512 or 1024 maps depending on setup.
Flexible Inline SSL Limits	Not supported with Inline Network LAG. Setting inline tools to “Drop” in the chain does not block Inline SSL traffic.
Filtering Limits (GigaVUE-TA400, GigaVUE-TA400E)	VLAN-based filtering in the Egress Port Filter for OOB copies is not supported. If one tool in the map is in monitoring mode, all tools must use the same mode. Asymmetric hashing (a-srcip-b-dstip and b-srcip-a-dstip) is not supported.
Protocol Pass-Through (GigaVUE-TA400, GigaVUE-TA400E)	CDP pass-through is not supported when the source is an Inline Network LAG. Bypass for LACP, CDP, and LLDP is supported.
Scaling Limits — GigaVUE-TA400, GigaVUE-TA400E	Max Inline Networks and Tools: 48 Max Inline Network LAG list: 24 Max Inline tools or tool groups per direction: 16 Max OOB copy entries per direction: 17 Max OOB copy ports per entry: 128

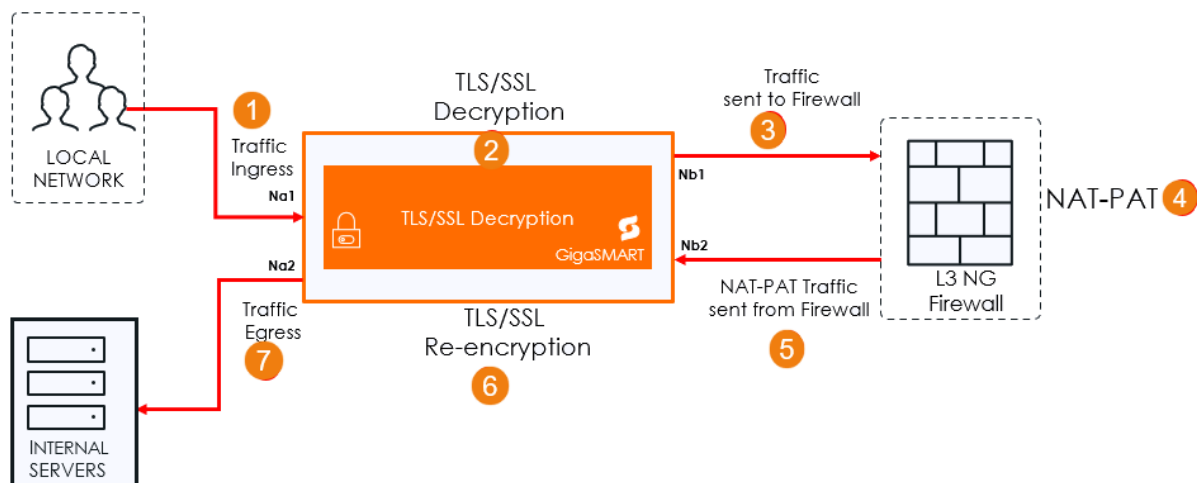
Inline TLS/SSL Decryption Solution with Layer 3 Tools (NAT-PAT)

A Layer 3 inline SSL decryption refers to Gigamon's deployment of its inline TLS/SSL decryption solution at the network layer (Layer 3 of the OSI model). In this mode, the GigaVUE node intercepts encrypted traffic flows between clients and servers, decrypts the SSL/TLS traffic, and subsequently delivers the decrypted packets to security tools for inspection. After the inspection, the traffic is re-encrypted and forwarded to its destination. Here are some key aspects of the solution:

- **Traffic Routing:** The solution allows for the configuration of subnet-based IP ranges at the ISSL profile level. This configuration determines whether traffic is routed through L3 tools. For example, traffic within a specific subnet range can be designated for L3 tools, which support NAT-PAT (Network Address Translation - Port Address Translation) for correlating client, server, and tool sessions.
- **Deployment Modes:** The solution can be deployed in a one-arm mode, which is suitable for enterprises looking to optimize their return on investment (ROI) by aligning with the capabilities of their inline tools.
- **Configuration and Management:** The deployment involves configuring flow maps to guide decrypted traffic to the appropriate tools, such as Next-Generation Firewalls (NGFWs). This includes setting up inline network bundles, flex maps, and inline SSL profiles.
- **Monitoring and Statistics:** The solution provides tools for monitoring traffic states, session statistics, and certificate hit counts. This helps in managing and optimizing the decryption process.

Architecture of an L3 Tool based Inline TLS/SSL Decryption Solution

Inline TLS/SSL Solution for Layer 3 / Transparent Tools (NAT-PAT)



The following steps describe the end-to-end flow:

1. **Traffic Ingress**-Traffic enters the system through the Inline Network Port (Ingress). This port acts as the first point of entry for all inbound encrypted traffic.
2. **TLS/SSL Decryption**-The traffic is directed to the GigaSMART engine, where the inline TLS/SSL application is. The engine decrypts the TLS/SSL traffic.
3. **Traffic Sent to Firewall**-The decrypted traffic is forwarded to the firewall.
4. **NAT-PAT**- The traffic is now either Network Address translated or Port Address translated.
5. **Traffic Sent from Firewall** :Traffic is being forwarded to the GigaSMART engine for re-encryption.
6. **SSL Re-encryption**-The GigaSMART engine re-encrypts the traffic using the TLS/SSL parameters.
7. **Traffic Egress**-The re-encrypted traffic is sent out through the Inline Network Port (Egress) to continue to the servers.

Rules and Notes

The following table lists rules and notes that you need to be aware of while configuring your deployment.

Rule / Feature	Details / Limitations
Exclusive Use	Inline tools in a flexible inline map cannot be used in classic inline or inline decryption maps. All inline networks and tools must belong to only one type of map.
Collector Maps	Only one unidirectional collector map is allowed for the same inline network. To use different VLANs in each direction, create separate unidirectional maps with unique VLAN tags. Tags can be set manually or assigned automatically by GigaVUE-FM.
Unsupported Features (GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA25E, GigaVUE-TA25, GigaVUE-TA400, GigaVUE-TA400E)	- Physical Bypass (no BPS card) - Flexible and Resilient Inline SSL (no GigaSMART card) - GRIP (no BPS card) - ICAP (no GigaSMART card) - Classic Inline Bypass
VLAN Tagging and OOB Copy Limits (GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus)	Flexible Inline Single VLAN Tag with monitoring mode may send incorrect VLAN tags. OOB copy packets may also have wrong tags. You cannot use BYPASS WITH MONITORING with MONITORING mode on the tool. OOB copy from inline network is not allowed in this mode.
Inline Map Limits — Bidirectional	GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus → 126 maps GigaVUE-HC1, GigaVUE-HC3 (CCv1 & CCv2), GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E → 256 or 512 maps depending on setup.
Inline Map Limits — Unidirectional	GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus → 252 maps GigaVUE-HC1, GigaVUE-HC3 (CCv1 & CCv2), GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E → 512 or 1024 maps depending on setup.
Flexible Inline SSL Limits	Not supported with Inline Network LAG. Setting inline tools to “Drop” in the chain does not block Inline SSL traffic.
Filtering Limits (GigaVUE-TA400, GigaVUE-TA400E)	VLAN-based filtering in the Egress Port Filter for OOB copies is not supported. If one tool in the map is in monitoring mode, all tools must use the same mode. Asymmetric hashing (a-srcip-b-dstip and b-srcip-a-dstip) is not supported.
Protocol Pass-Through (GigaVUE-TA400, GigaVUE-TA400E)	CDP pass-through is not supported when the source is an Inline Network LAG. Bypass for LACP, CDP, and LLDP is supported.
Scaling Limits — GigaVUE-TA400, GigaVUE-TA400E	Max Inline Networks and Tools: 48 Max Inline Network LAG list: 24 Max Inline tools or tool groups per direction: 16 Max OOB copy entries per direction: 17 Max OOB copy ports per entry: 128

Differences Between Layer 2 and Layer 3 Tools Deployments

Feature	L2 ISSL Decryption	L3 ISSL Decryption
Traffic Handling	This method processes traffic without the need for NAT-PAT, enabling a direct correlation between client and server sessions.	Supports NAT-PAT, with both IP and port or either of them. NAT-PAT enhances security by making it more difficult for unauthorized users to track and intercept network traffic, ultimately protecting sensitive information.
Protocol Support	Typically, it supports a wider variety of L7 protocols in OSI model without compromising performance.	The system primarily supports HTTP/1.1. Other protocols such as SMTPS and DNS-over-TLS are not supported.
Session Management	The GigaSMART maintains a single session dedicated to traffic processing.	The GigaSMART engine operates by maintaining two distinct sessions: one prior to its activation and another following its use.

Advanced Features for Inline TLS/SSL Decryption Solution

Choose from the following advanced features methods to implement Inline TLS/SSL Decryption:

- [Inline TLS/SSL Decryption Solution with RIA](#)
- [Entrust nShield and Thales-Luna HSM for TLS/SSL Decryption for iSSL](#)
- [Inline TLS/SSL Decryption Solution with ICAP Client](#)

Inline TLS/SSL Decryption Solution with RIA

GigaSMART Flex Inline Solution can now be configured in a Resilient Inline Arrangement (RIA), which is supported on all GigaVUE HC Series devices. To learn more about Resilient Inline Arrangements refer to [Resilient Inline Arrangement](#).

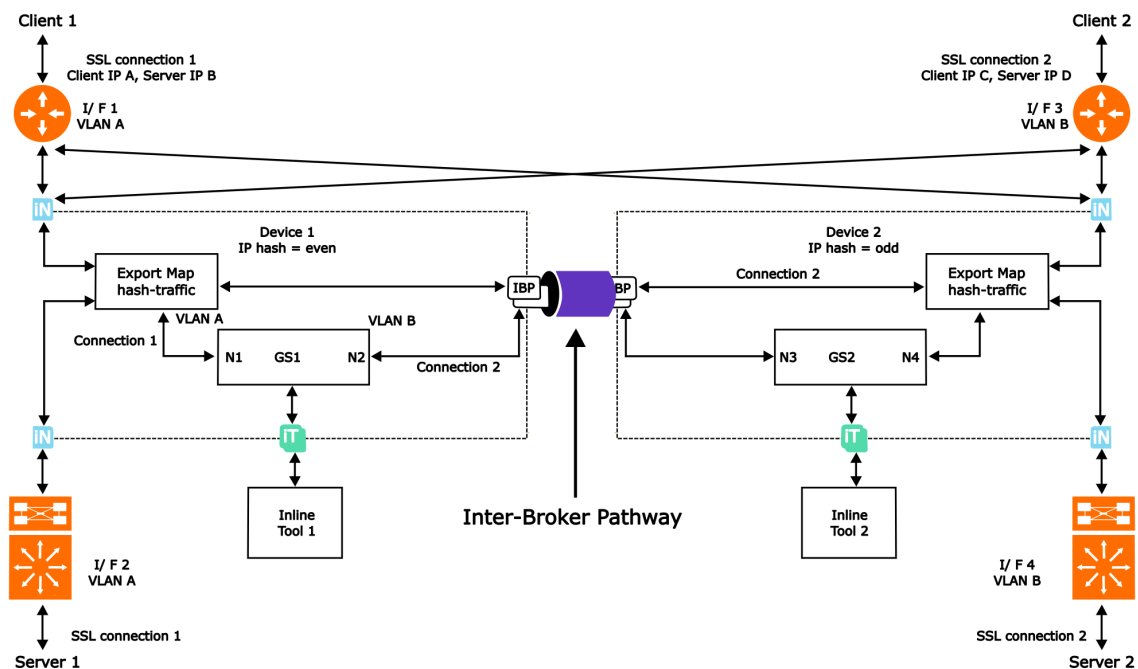
A Resilient Inline Arrangement utilizes two nodes to manage traffic in dual-path high availability environments. Both nodes process traffic simultaneously, using the source and destination IP addresses for decision-making. Traffic received from the top network interfaces is directed based on the source IP, while traffic from the bottom network

interfaces relies on the destination IP of the incoming traffic. Specifically, if the IP address ends with an even number, the traffic will be forwarded to one node; conversely, if it ends with an odd number, it will be sent to the other node.

For example:

In the Resilient Inline Arrangement described below, interface (I/F) 1 and I/F 2 are linked to node 1, while I/F 3 and I/F 4 connect to node 2. For connection 1, client 1's traffic from I/F 1, which has a VLAN A source and an IP address A, will be directed to GS1 in node 1 because the last decimal digit of IP A is even. Similarly, the traffic from server 1 of the same connection, originating from I/F 2 with VLAN A and destination IP A, will also be routed to GS1 in node 1.

For connection 2, since the last digit of IP C is even, the traffic from I/F 3 and I/F 4 will likewise be sent to GS1 in node 1. The traffic between GS1 and client 2 will occur on I/F 3 with VLAN B, requiring these packets to traverse the IBP that connects node 1 and node 2. In the same manner, the traffic between GS1 and server 2 will utilize I/F 4 after passing through the IBP.

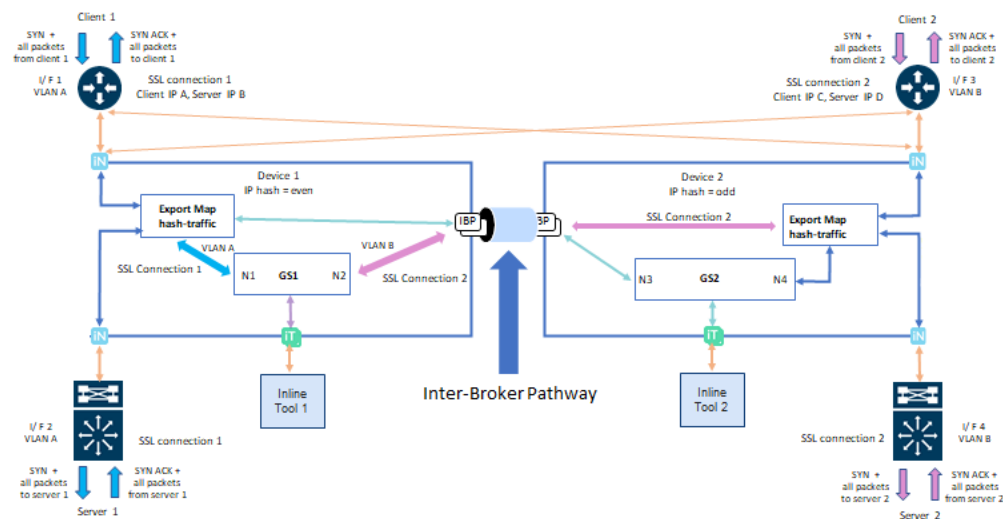


Symmetric Traffic in RIA

In a symmetric connection, the SYN packet from Client 1 arrives on Interface 1 (I/F 1) with VLAN A and is forwarded to GS1 in Node 1, as the source IP (IP A) is even. GS1 initiates a TCP connection to Server 1 by sending a SYN packet out from Interface 2 (I/F 2) with VLAN A.

Server 1 responds with a SYN-ACK from I/F 2 with VLAN A, routed back to GS1 since the destination IP (IP A) is even. Thus, all traffic between GS1 and Client 1 occurs on I/F 1, while traffic between GS1 and Server 1 uses I/F 2, connected to Node 1.

Traffic from Connection 2 on I/F 3 and I/F 4 with VLAN B is processed by GS1 in Node 1, as Client 2's IP (IP C) is also even. All traffic between GS1 and Client 2 flows through I/F 3 with VLAN B via the IBP, while traffic between GS1 and Server 2 is managed on I/F 4 with VLAN B, connected to Node 2.



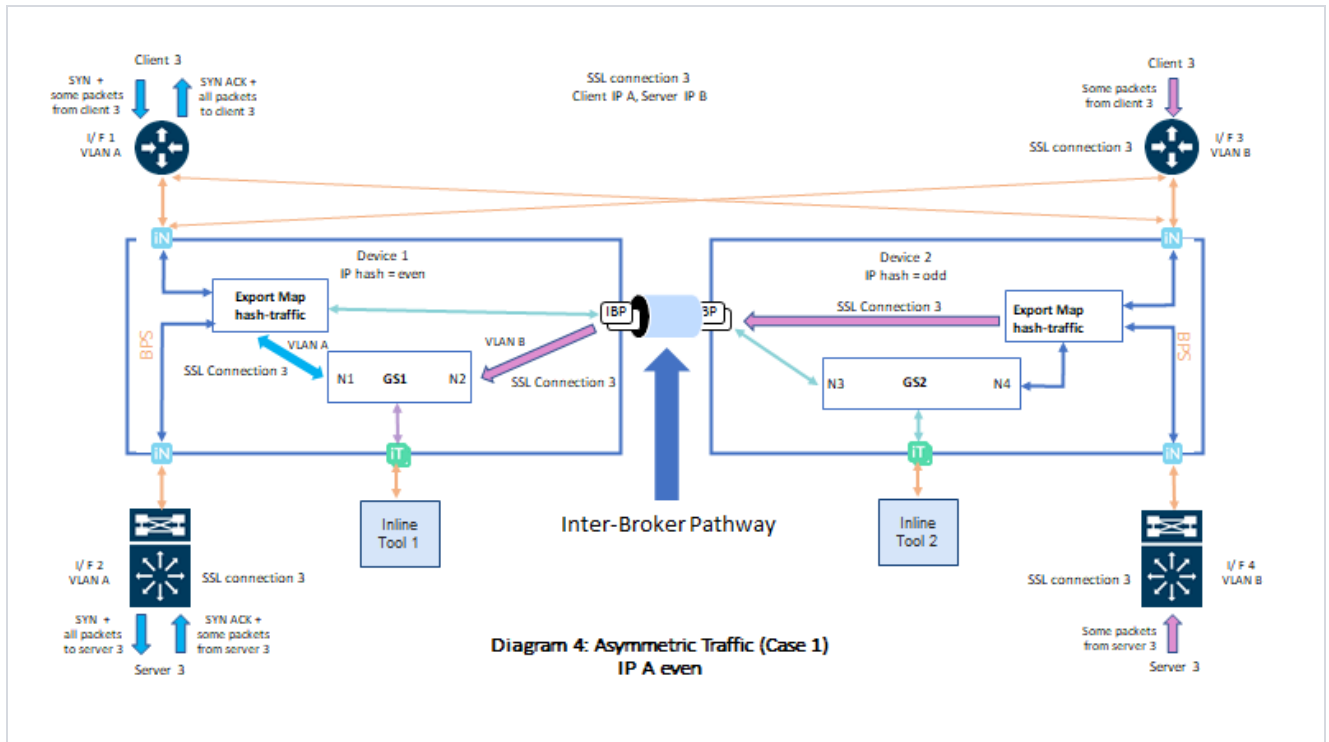
Asymmetric Traffic in RIA

An asymmetric connection can occur in various scenarios:

Scenario 1

In the resilient inline arrangement below, the SYN packet for TLS/SSL connection 3 from client 3 is received on I/F 1 with VLAN A and forwarded to GS1 in device 1, as the source IP (IP A) is even. Server 3 responds with a SYN ACK from I/F 2 with VLAN A on device 1, also forwarded to GS1 since the destination IP (IP A) is even. GS1 then sends the SYN ACK back to client 3 on I/F 1 with VLAN A.

However, due to asymmetric routing or load balancing, some subsequent traffic from client 3 or server 3 related to connection 3 may arrive at I/F 3 or I/F 4 with VLAN B. This traffic is forwarded to node 1 through IBP, allowing symmetric traffic inspection. All outgoing traffic from GS1 to client 3 will be sent via I/F 1 with VLAN A, while traffic to server 3 will go through I/F 2 with VLAN A.

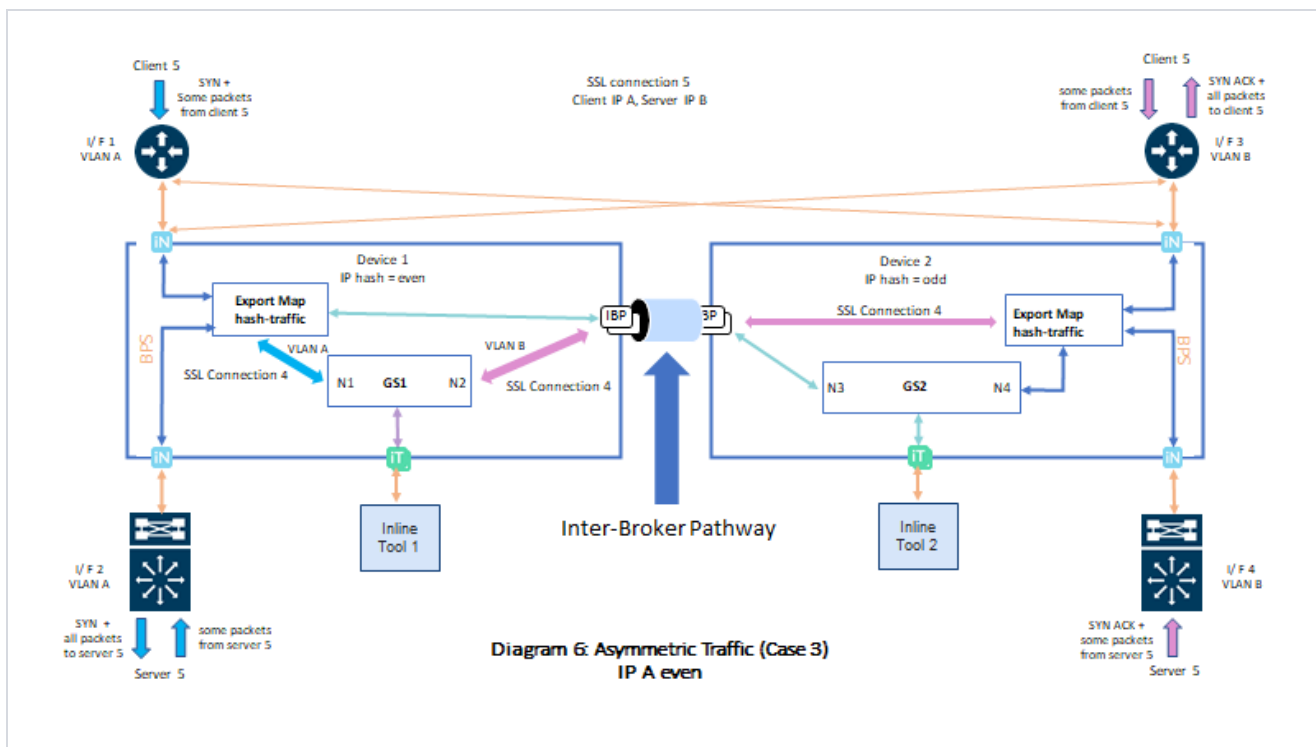


Scenario 2

Consider the following: the SYN packet for the TLS/SSL connection from client 5 arrives on interface 1 (I/F 1) with VLAN A. It is forwarded to GS1 in node 1, as the source IP (IP A) is even. GS1 initiates a TCP connection to Server 5 by sending a SYN packet from interface 2 (I/F 2) with VLAN A. Server 5 replies with a SYN ACK from interface 4 (I/F 4) with VLAN B on node 2, forwarded to GS1 through the IBP since the destination IP (IP A) is even.

Upon receiving the SYN ACK from Server 5 on I/F 4 with VLAN B in node 2, GS1 sends a SYN ACK to client 5 on interface 3 (I/F 3) with VLAN B, also on node 2. Due to asymmetric routing or load balancing, some incoming traffic from client 5 may reach I/F 3 with VLAN B on device 2, forwarded to GS1 via the IBP, as the source IP (IP A) remains even.

Additionally, some traffic from Server 5 may arrive at I/F 2 with VLAN A on node 1, also forwarded to GS1 on node 1 since the destination IP (IP A) is even. Outgoing traffic from GS1 to client 5 will go through I/F 3 with VLAN B on node 2, while traffic to Server 5 will route through I/F 2 with VLAN A on node 1, regardless of the incoming interface.



VLAN Tagging Behavior for Decrypted Traffic

The Inline Tool positioned outside the SSL App is capable of receiving the original Map's VLAN tag for local node traffic, as well as the import map's VLAN tag for remote node traffic. In cases of asymmetric traffic, the Inline Tool will receive both the original Map's VLAN and the import map's VLAN.

Conversely, the Inline Tool located within the SSL App will consistently receive the tool tag configured in the SSL App for both local and remote node traffic.

VLAN Tagging Behavior for Non-Decrypted Traffic

The Inline Tool positioned outside the SSL App can capture the VLAN tag from the original Map or the non-proxy Map for local node traffic, as well as the VLAN tag from the import Map or import non-proxy Map for remote node traffic. In scenarios involving asymmetric traffic, the Inline Tool will receive both the VLAN tags from the original Map and the import map.

Conversely, the Inline Tool located within the SSL App will obtain the non-proxy Map's Tool tag for local node traffic and the import non-proxy Map's Tool tag for remote node traffic.

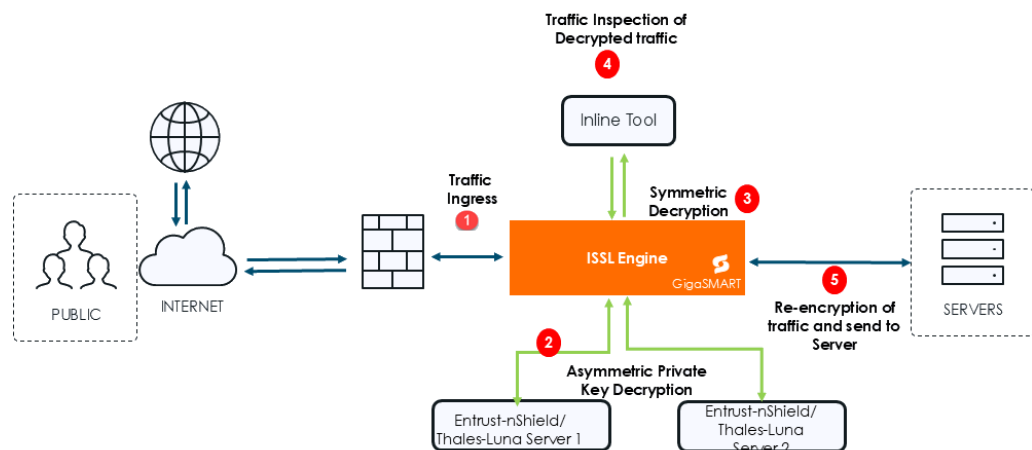
Entrust nShield and Thales-Luna HSM for TLS/SSL Decryption for iSSL

This feature enables inline TLS/SSL decryption to work with Hardware Security Modules (HSMs), enhancing the security and flexibility of cryptographic operations. HSM's are designed to:

- Securely perform cryptographic processing.
- Generate and store cryptographic keys.
- Prevent unauthorized access to sensitive data.

ISSL with Entrust nShield/Thales- Luna HSM

Inline TLS/SSL Solution with Entrust-nShield / Thales-Luna



7

The following steps describe the end-to-end flow:

1. **Traffic Ingress**-Traffic enters the system through the Inline Network Port (Ingress). This port acts as the first point of entry for all inbound encrypted traffic.
2. **Asymmetric Decryption**- TLS handshake traffic which needs private key operation directs to HSM server.

3. **Symmetric Decryption**- Post private key operation done on HSM, data traffic decrypts in GigaSMART.
4. **Traffic Inspection**- The decrypted traffic is forwarded to inline security tools . These tools inspect but do not modify packet contents. Tools may allow, alert on, or block traffic based on inspection results, but they do not change the actual data.
5. **SSL Re-encryption and sent to Server** -The GigaSMART engine re-encrypts the traffic using the TLS/SSL parameters. The re-encrypted traffic is sent out to the servers.

HSM - Supported Solutions

Inline TLS/SSL decryption supports the following HSM solutions:

- Entrust nShield HSM
- Thales Luna Network HSM

HSM Configuration Rules, Notes, and Limitations

- Network & Deployment Requirements
 - Use a static IP address for the GigaSMART engine, and ensure it is registered on the HSM server.
 - DHCP is not recommended. If the IP address changes, the entire HSM setup must be deleted and reconfigured.
 - IPv6 is not supported for Thales Luna HSM server configuration when IPv6 stack port support is enabled. IPv6 traffic can be decrypted but HSM server IP and GigaSMART engine IP configuration will not support IPv6 address.
- HSM Type Usage
 - A deployment can use only one HSM type—either Entrust nShield or Thales Luna.
 - Entrust nShield and Thales Luna HSM cannot operate together within the same HSM Group or the same GigaVUE HC Series device.
- Switching Between HSM and Non-HSM Configurations: When moving from non-HSM to HSM, or between different HSM types, the GigaSMART engines and the device must be restarted before redeployment.
- Keys, Keychain, and Certificates
 - The Keychain password must be set before importing any keys. If not set, key and certificate uploads will fail.
 - Key–certificate mismatch checks cannot be performed for RSA or ECDSA keys because private keys remain on the HSM server.
 - For inbound deployments, required CA certificates must be uploaded to trust store avoid configuration errors.
 - For outbound deployments, CA certificates are optional but recommended for improved validation.
- Unsupported Deployment Combinations

- Mixed HSM types (Entrust nShield + Thales Luna) are not supported, even if configured on different Gen3 GigaSMART cards.
- Mixed HSM and non-HSM deployments cannot exist on the same device, including across separate Gen3 cards.
- Mixed generation configurations are not supported:
- Gen2 non-HSM iSSL cannot be configured with Gen3 HSM iSSL, even on different cards within the same device.
- Thales Luna-Specific Limitations
 - Thales Luna Network HSM does not support cluster, standby, or non-HA modes.

Inline TLS/SSL Decryption Solution with ICAP Client

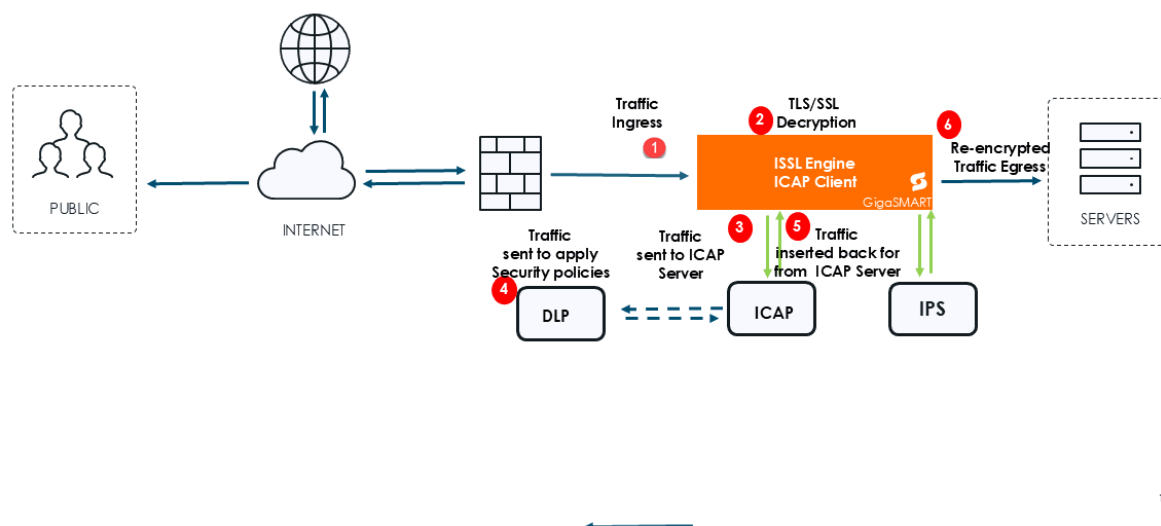
ICAP (Internet Content Adaptation Protocol) is used to inspect and modify HTTP messages by offloading them to a separate server. It allows clients to send HTTP requests and responses to an ICAP server, which can process the content and return a modified response. The message format follows HTTP/1.1, with components like the request line, headers, and body.

In a standard Inline SSL setup, the GigaVUE node decrypts SSL traffic and forwards it to an inline tool for processing. However, this setup does not support integration with DLP (Data Loss Prevention) servers running over ICAP.

By combining Inline SSL with ICAP, the decrypted traffic can now be routed through an ICAP client within the GigaSMART application. This enhancement enables direct integration with DLP ICAP servers, allowing advanced inspection and policy enforcement on decrypted content.

The following image provides an end-to-end flow of Inline TLS/SSL Configuration with an ICAP Client

Inline TLS/SSL Solution with an ICAP Client



The following steps describe the end-to-end flow:

1. **Traffic Ingress**-Traffic enters the system through the Inline Network Port (Ingress). This port acts as the first point of entry for all inbound encrypted traffic.
2. **TLS/SSL Decryption**-The traffic is directed to the GigaSMART engine, where the inline TLS/SSL application is. The engine decrypts the TLS/SSL traffic, making it readable for inspection tools.
3. **Traffic sent to ICAP Client**- the decrypted traffic can now be routed through an ICAP client within the GigaSMART application.
4. **Traffic Inspection**- The traffic is now directed to DLP ICAP servers, allowing advanced inspection and policy enforcement on decrypted content.
5. **Traffic sent back for re-encryption** - The traffic is now sent from ICAP server to the GigaSMART engine.
6. **SSL Re-encryption and sent to Server** - The re-encrypted traffic is sent out to the servers.

ICAP - Limitations

- The ICAP Client cannot be deployed inline with the following iSSL configurations:
 - One-Arm iSSL
 - L3 NAT iSSL
 - RIA iSSL

- In GigaVUE-HCI-Plus, the inline network ports must reside in the same hardware slot.
- ICAP is not supported in GigaVUE-HCT chassis.

Refer to [Configure ICAP Client](#) and [Configure ICAP Client for Inline TLS/SSL Decryption Solution](#) for configuration details.

TLS/SSL Terminology and Acronyms

The below table provides definitions of TLS/SSL terminology:

Table 4: TLS/SSL Terminology

Term	Definition
Plaintext	The original, unencrypted data.
Ciphertext	The encrypted data.
Cryptography	The practice of secure communications.
Encryption	The process of turning plaintext into ciphertext.
Decryption	The process of turning ciphertext into plaintext.
Encryption algorithm	The algorithm used to perform encryption and decryption. It is also called the cipher.
Encryption key	The key used for encryption.
Decryption key	The key used for decryption.
Symmetrical encryption algorithm	The algorithm used for encryption in which the encryption key and the decryption key are identical.
Asymmetrical encryption algorithm	The algorithm used for encryption in which the encryption key and the decryption key are different.
Public key	The key used for encryption.
Private key	The key used for decryption.

The below table lists TLS/SSL acronyms:

Table 5: TLS/SSL Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CN	Common Name

Acronym	Definition
CRL	Certificate Revocation List
DES	Data Encryption Standard
DH, D-H	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FQDN	Fully Qualified Domain Name
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MAC	Message Authentication Code
MD	Message Digest
MitM	Man-in-the-Middle
OCSP	Online Certificate Status Protocol
OoB	Out-of-Band
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PKCS12	Public Key Cryptography Standard #12
PKI	Public Key Infrastructure
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator

Inline Solutions Configuration Using Flexible Inline Arrangement Canvas

This sections elaborates on how to configure Inline Solutions using Flexible Inline Arrangement Canvas.

What is a Flexible Inline Arrangement

Flexible inline arrangements are an approach to guide multiple inline traffic flows through a user-defined sequence of inline tools and inline tool groups. It uses the same software constructs as the existing Inline Bypass solution, such as inline network, inline tool, and inline tool group. Flexible inline arrangements support physical protection based on the specialized hardware on BPS modules. It also supports both protected and unprotected inline network links.

Flexible inline arrangements offer an alternative to classic Inline Bypass. Classic Inline Bypass functionality remains intact for backwards compatibility. For information on configuring Inline Bypass solutions (classic), refer to [Inline Configurations using Inline Bypass Solutions \(Classic\)](#).

Using flexible inline maps, traffic from the same inline network can traverse different sequences of inline tools and share tools across traffic flows or with other inline networks.

You can identify specific flows of traffic using Layer 2 to Layer 4 rules, then designate the tools that will inspect the traffic, and specify the order of the tools. For example, you can send Web traffic (defined by L4 port, 80 and/or 443) through a Web Application Firewall (WAF) and an Intrusion Prevention System (IPS), have backup traffic that might bypass inspection, and send all other traffic through the same IPS.

The figure below illustrates a complex inspection scenario that is enabled by flexible inline arrangements.

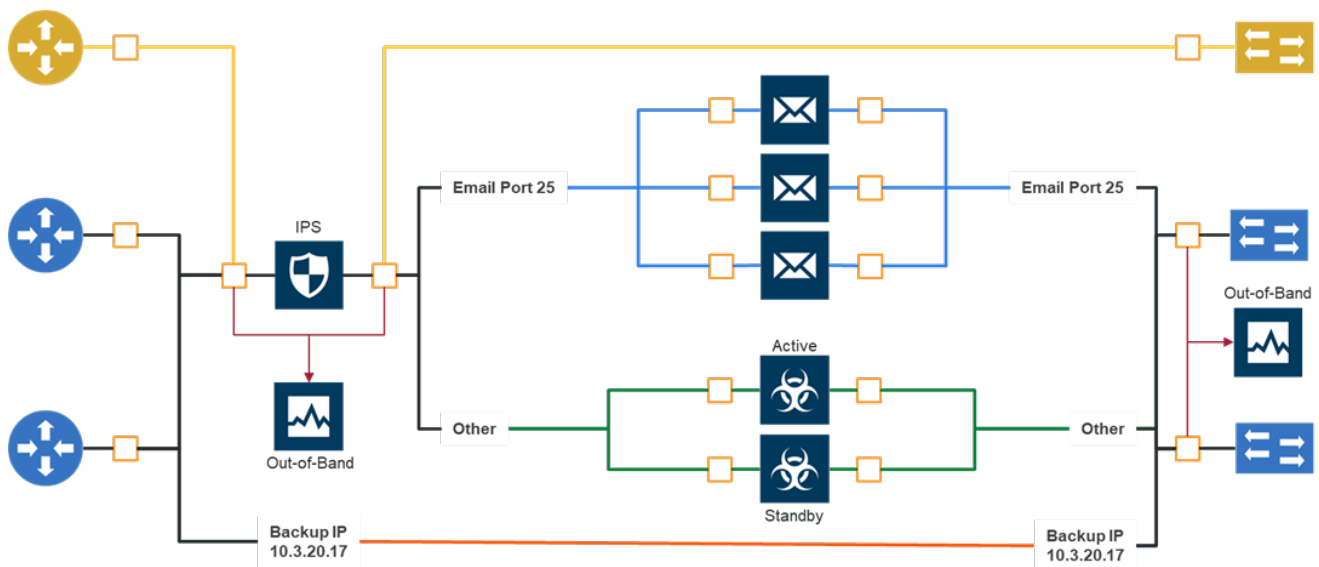


Figure 21 Flexible Inline Arrangements Scenario

In this example, on the left, there are three network links, all of which share the IPS. The details are as follows:

- At the top of the figure, the yellow line represent a flow of network traffic that only needs IPS inspection.
- In the middle of the figure, the Email and Other traffic represents network traffic flows that go through IPS inspection first, and then the Email traffic goes to dedicated inspection tools, here shown as three tools in an inline tool group, and the Other traffic goes to a threat protection active/standby pair.
- At the bottom of the figure, daily Backups of already-inspected traffic goes to bypass.

Although not shown graphically in [Figure 21Flexible Inline Arrangements Scenario](#), the traffic in the reverse direction can have a different order of tools than the west-east traffic.

Refer to the Gigamon Validated Design for more information.

- [Deploying GigaSECURE Inline SSL Solution using Flexible Inline](#)
- [Guiding Relevant Inline Traffic to Tools](#)

Flexible Inline Maps

Traffic flows are the building blocks of flexible inline arrangements. Flows can be based on any flow mapping criteria, such as TCP port, IP subnet, or VLAN. There is a one-to-one correspondence between a traffic flow and a flexible inline map.

A flexible inline map is a new map type. Flexible inline arrangements allow inline maps from inline networks to arbitrary sequences of shared (overlapping) sequences of inline tools and inline tool groups.

Using flexible inline maps, you can identify specific flows of traffic using Layer 2 (L2) to Layer 4 (L4) rules, then designate the tools that will inspect the traffic, and specify the order of traffic to the tools.

You can configure a flexible inline map with a specific inline tool that is part of an inline tool group, which is associated with another flexible inline map. For example, you have created an inline tool group, ITG1 in which inline tools, IT1, IT2, and IT3 are grouped together. You can configure a flexible inline map, Map1 with inline network, IN1 as the source and ITG1 as the destination. You can configure a second flexible inline map, Map2 with IN1 as source and IT1 as destination. Such configuration is useful to guide specific traffic to a particular inline tool and the rest of the traffic to the inline tool group in which the inline tool is associated.

To properly guide traffic through the inline tools, each flow of traffic is assigned a VLAN tag. VLAN tags can be automatically assigned or can be user-defined. You can use flexible inline single tags to map incoming VLANs on the network side to the outgoing VLANs on the tool side.

With flexible inline arrangements, VLAN tags are associated with each inline map, not with each inline network port as in the case of classic Inline Bypass. A single inline network port can have multiple inline maps, each with a separate VLAN tag.

A VLAN tag automatically assigned to an inline map can be manually added to another inline map. For example, if an inline map is given the VLAN tag 2000, the same VLAN tag can be manually added to another inline map. Here, the system would prioritize the manually added VLAN tag and modify the auto-assigned VLAN Tag. This is not applicable for VLAN's assigned to internal inline maps such as import/export maps and inner non-proxy maps configured by GigaVUE-FM for Resilient Inline Arrangement (RIA) and RIA SSL solutions.

For example, traffic flows can be defined with the following VLAN tags:

- Unspecified traffic—VLAN 101
- Web traffic—VLAN 102
- Email traffic—VLAN 103
- Database traffic—VLAN 104

NOTE: The VLAN tags are added to the traffic before it is sent to the tools and are removed before it is sent back to the network.

Types of Flexible Inline Maps

To define a traffic flow, you must configure a flexible inline map. Following are the two types of flexible inline maps:

- **byRule**—Use the byRule map type to define a flow using map rules. Any standard L2-L4 mapping rules can be specified in the map, such as, IPv4, IPv6, L4 port, or UDA.
- **collector**—Use the collector map type for all other traffic. A collector is the lowest priority of map and does not have a map rule definition. Use a collector to catch any traffic that does not go to any other map. You can define a flexible inline collector map without any other maps in place. This provides a map passall, provided there are no rule-based maps. If you want all the traffic to go to the same tools, you only need to configure a collector.

Flexible inline arrangements guide rule-based or collector-based inline traffic flows through unidirectional or bidirectional sequences of inline tools or inline tool groups. The traffic path can be set up independently for side A to side B and side B to side A directions, meaning that the traffic flow can be either symmetrical or asymmetrical.

You specify the ordered list of inline tools or inline tool groups that will inspect a particular flow of traffic. Additionally, you can specify if the A-to-B and B-to-A directions have the same order or the reverse order. Reverse order is the order of inline tools as they are wired in a physical network if a Gigamon network packet broker was not present.

For example, in the A-to-B direction, if the tools are specified in the following order: T1, T2, T3, the same order in the B-to-A direction will be: T1, T2, T3, while the reverse order in the B-to-A direction will be: T3, T2, T1. Or, you can specify the order of the tools explicitly, for example, the B-to-A direction can be: T2, T1, T3.

You can create separate flexible inline maps for each flow of traffic to be inspected by a sequence of inline tools. Create maps until you have accounted for all the flows of traffic. Any unspecified traffic will go to the collector. You can also specify map priorities for the flexible inline maps.

Supported Platforms, License, and Software Version

The below table provides you the software version, supported platforms and license that might be required to utilize flexible inline arrangements

Software Version	Supported Platforms	License	
		Monthly Subscription (Term License)	Perpetual Subscription
GigaVUE-FM and GigaVUE-OS running on software version 5.3.xx or higher support the flexible inline arrangement functionality.	GigaVUE-HC1-Plus	NA	NA
	GigaVUE-HCT	NA	NA
	GigaVUE-HC1	NA	NA
	GigaVUE-HC3 (CCv1 and CCv2)	NA	NA
	GigaVUE-TA25	IBP-TAX20-SW-TM	IBP-TAX20
	GigaVUE-TA25E	IBP-TAx20-SW-TM	IBP-TAX20
	GigaVUE-TA200	IBP-TAC20-SW-TM	IBP-TAC20
	GigaVUE-TA200E	IBP-TAC20E-SW-TM	IBP-TAC20E
	GigaVUE-TA400	IBP-TAC40-SW-TM	IBP-TAC40
	GigaVUE-TA400E	IBP-TAC40E-SW-TM	IBP-TAC40E

Flexible Inline Solution Supported in Clustered Nodes

The GigaVUE HC Series, GigaVUE-TA25, GigaVUE-TA200, GigaVUE-TA400, and GigaVUE-TA400E nodes can now be clustered with Flexible Inline solution for the configuration path. The traffic path is limited to a single node such that all inline ports should reside in the same node. This feature is applicable in Out-of-Band and Leaf-Spine cluster. The Flexible Inline features that can be configured are as follows:

Supported Feature	Reference
Flexible Inline Solution	Inline Solutions Configuration Using Flexible Inline Arrangement Canvas
Single VLAN Tag	Configure Inline Single VLAN Tag
Non Shared Tool	Configure Inline Tool Ports and Inline Tools
Resilient Weighted Hashing	Refer to 'Resilient Weighted Hashing' in Configure Inline Tool Group

Supported Feature	Reference
Out-of-Band Copy The oob-copy target ports must reside on the same node as the respective flexible inline type maps. The traffic originated from oob-copy can be exposed to out-of-band tool residing on other nodes by using hybrid ports. This feature also allows the flexibility to have different oob-copies on each direction (a-to-b and b-to-a) from GigaVUE-FM for bidirectional flex maps. Starting in software version 6.4, the tool/hybrid port which is part of a regular byRule or passall map with ingress VLAN tag enabled on the network port can also be used as an OOB-copy port of flexible inline maps.	Refer to Example 7—Protected Flexible Inline, Out-of-Band Copy in GigaVUE-OS CLI Reference Guide.
Resilient Inline Arrangement. In a Resilient Inline Arrangement, both GigaVUE® HC Series nodes should be in different clusters or either one of the node can be a standalone node.	Refer to 'Resilient Inline Arrangement' in Configure Resilient Inline Arrangement
Network Link Aggregation Group (LAG)	Refer to Configure Inline Network LAG .
Hashing	Refer to Asymmetrical Hashing options in Configure Inline Tool Group .

Limitations

- The inline-network, inline-tool and destination tool ports in oob-copy must reside on the same node and cannot be chosen from across devices in a cluster.
- FlexInline and FlexInline SSL App solutions don't support TAGS, so RBAC tagging is not supported.

Flexible Inline TLS/SSL Decryption Solution—Rules and Notes

The table below lists the main rules, limits, and unsupported features for flexible inline arrangements, organized for quick reference.

Rule / Feature	Details / Limitations
Exclusive Use	Inline tools in a flexible inline map cannot be used in classic inline or inline decryption maps. All inline networks and tools must belong to only one type of map.
Collector Maps	Only one unidirectional collector map is allowed for the same inline network. To use different VLANs in each direction, create separate unidirectional maps with unique VLAN tags. Tags can be set manually or assigned automatically by GigaVUE-FM.
Unsupported Features (GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA25E, GigaVUE-TA25, GigaVUE-TA400, GigaVUE-TA400E)	- Physical Bypass (no BPS card) - Flexible and Resilient Inline SSL (no GigaSMART card) - GRIP (no BPS card) - ICAP (no GigaSMART card) - Classic Inline Bypass
VLAN Tagging and OOB Copy Limits (GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus)	Flexible Inline Single VLAN Tag with monitoring mode may send incorrect VLAN tags. OOB copy packets may also have wrong tags. You cannot use BYPASS WITH MONITORING with MONITORING mode on the tool. OOB copy from inline network is not allowed in this mode.
Inline Map Limits — Bidirectional	GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus → 126 maps GigaVUE-HC1, GigaVUE-HC3 (CCv1 & CCv2), GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E → 256 or 512 maps depending on setup.
Inline Map Limits — Unidirectional	GigaVUE-TA25, GigaVUE-TA25E, GigaVUE-HC1-Plus → 252 maps GigaVUE-HC1, GigaVUE-HC3 (CCv1 & CCv2), GigaVUE-TA200, GigaVUE-TA200E, GigaVUE-TA400, GigaVUE-TA400E → 512 or 1024 maps depending on setup.
Flexible Inline SSL Limits	Not supported with Inline Network LAG. Setting inline tools to “Drop” in the chain does not block Inline SSL traffic.
Filtering Limits (GigaVUE-TA400, GigaVUE-TA400E)	VLAN-based filtering in the Egress Port Filter for OOB copies is not supported. If one tool in the map is in monitoring mode, all tools must use the same mode. Asymmetric hashing (a-srcip-b-dstip and b-srcip-a-dstip) is not supported.
Protocol Pass-Through (GigaVUE-TA400, GigaVUE-TA400E)	CDP pass-through is not supported when the source is an Inline Network LAG. Bypass for LACP, CDP, and LLDP is supported.
Scaling Limits — GigaVUE-TA400, GigaVUE-TA400E	Max Inline Networks and Tools: 48 Max Inline Network LAG list: 24 Max Inline tools or tool groups per direction: 16 Max OOB copy entries per direction: 17 Max OOB copy ports per entry: 128

Configure Software Constructs Using Flexible Inline Arrangement Canvas

This section describes about the different flexible inline flows and provides step-by-step instructions on how to configure them using GigaVUE-FM. It also provides information about the forwarding states of the inline network.

Refer to the following sections for details:

- [Configure Inline Network Ports and an Inline Network](#)
- [Configure IP Interface](#)
- [Configure Inline Network LAG](#)
- [Configure Inline Network Bundle](#)
- [Configure Inline Tool Ports and Inline Tools](#)
- [Configure Inline Tool Group](#)
- [Configure Inline Single VLAN Tag](#)
- [Configure Flexible Inline Maps](#)

Configure Inline Network Ports and an Inline Network

To configure inline network ports and an inline network:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the inline network.
3. Click the '+' icon next to the **Inline Network** to create a new entry.
4. Enter a name and description for the inline network in the **Alias** and **Description** fields.
5. Click **Port Editor**. In the **Quick Port Editor**, scroll to the inline network ports you want to configure. Select **Enable** to activate the network ports, and click **OK**.
6. Select the ports you want to configure as the inline network pair from the **Port A** and **Port B** drop-down lists.

7. Choose a traffic path from the **Traffic Path** drop-down list:
 - **Bypass**- Redirects all traffic from the inline network to the opposite-side inline network port, bypassing all inline tools and tool groups. Traffic is not decrypted during this process.
 - **Drop** - Drops all traffic originating from the inline network.
 - **Bypass with Monitoring** - Sends one copy of the traffic directly to the opposite-side inline network port and another copy to the sequence of inline tools and inline tool groups.

NOTE: If the Inline network is set to bypass with monitoring, GigaSMART Inline TLS/SSL decryption does not work.

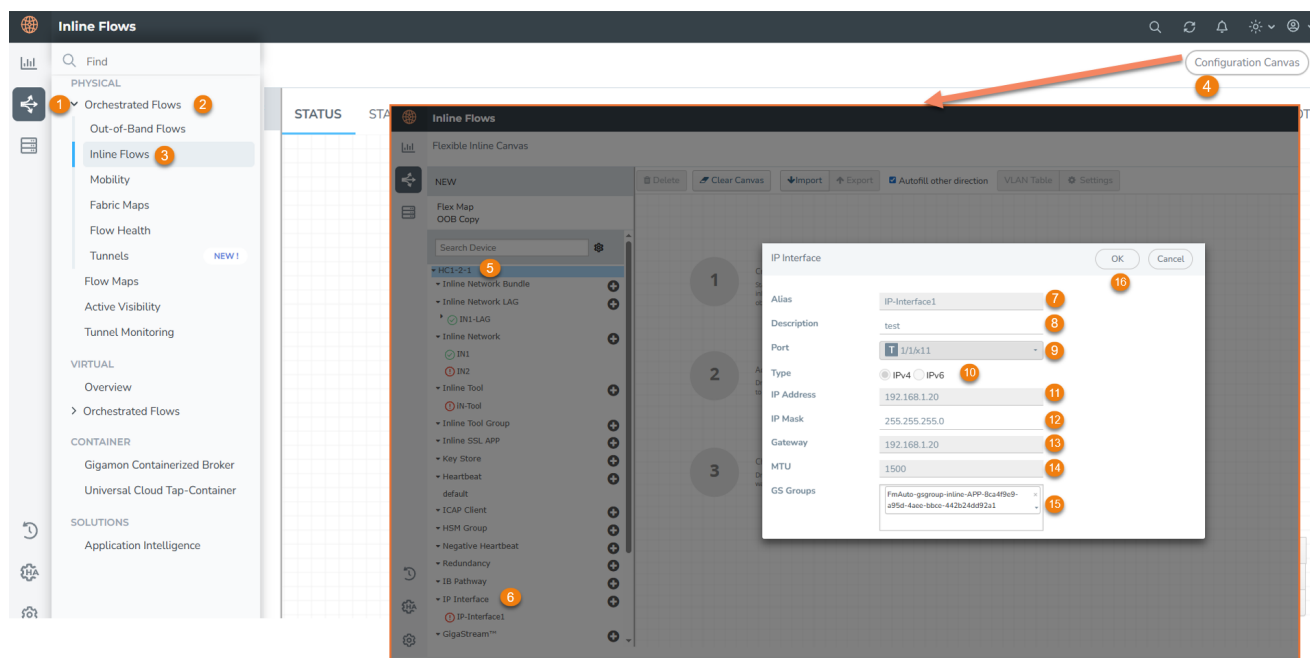
- **To Inline Tool** - Directs all traffic through the configured sequence of inline tools and tool groups, based on their current status.
8. Select the **Link Failure Propagation** check box to propagate link failure from one side of the inline network to the other.
 9. Select the **Accept Regular Heartbeat** check box to allow the inline network port pair to accept heartbeat packets from the inline tool port pair.
 10. Click **OK** to save the configuration.

Configure IP Interface

To configure IP Interface:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the IP Interface.
3. Click the '+' icon next to the **IP Interface** to create a new entry.
4. Enter a name and description for the IP Interface in the **Alias** and **Description** fields.
5. From the **Port** drop down list, choose the port you want to configure as the IP Interface.
6. Select the **Type** of the IP Interface you want to configure.
7. Enter the **IP Address** (for example, 192.168.1.20).
8. Enter the **IP Mask** (for example, 255.255.255.0).
9. Enter the **Gateway** (for example, 192.168.1.20).

10. In the **MTU** field, specify the Maximum Transmission Unit for the port (for example, 1500).
11. From the GS Groups drop-down list, select the required GigaSMART Group you created.
12. Click **OK** to save the configuration.



Configure Inline Network LAG

Before You Begin - Configure the required inline network ports and inline networks before you set up an inline network LAG. Refer to [Configure Inline Network Ports and an Inline Network](#) for details.

To configure an inline network LAG:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the device where you want to configure the inline network LAG.
3. Click the '+' icon next to the **Inline Network LAG** to create a new entry.
4. Enter a name and description for the inline network in the **Alias** and **Description** fields.

5. From the Inline Networks drop-down list, select the inline networks to include in the inline network LAG.
6. From the **Traffic Path** drop-down list, choose one of the following options:
 - **Bypass** - Forwards traffic directly between Port A and Port B of the inline network.
 - **Drop** - Drops all traffic arriving at the inline network ports.
 - **Bypass with Monitoring** - Forwards traffic as a forced bypass and sends a copy to inline tools. Ensure a traffic map is configured between the inline network and the inline tool.
 - **To Inline Tool** - Forwards traffic to the sequence of inline tools.
7. Select the **Link Failure Propagation** check box to bring down a port when its paired port goes down..
8. Select the **Physical Bypass** check box to allow traffic to flow directly between Port A and Port B of the inline network pair when a device or module powers down.
9. If the port channel uses **LACP**, select the **Bypass Link Aggregation Control Protocol** and **Link Layer Discovery Protocol** check box to maintain port channel functionality on links connected to inline network LAG ports.



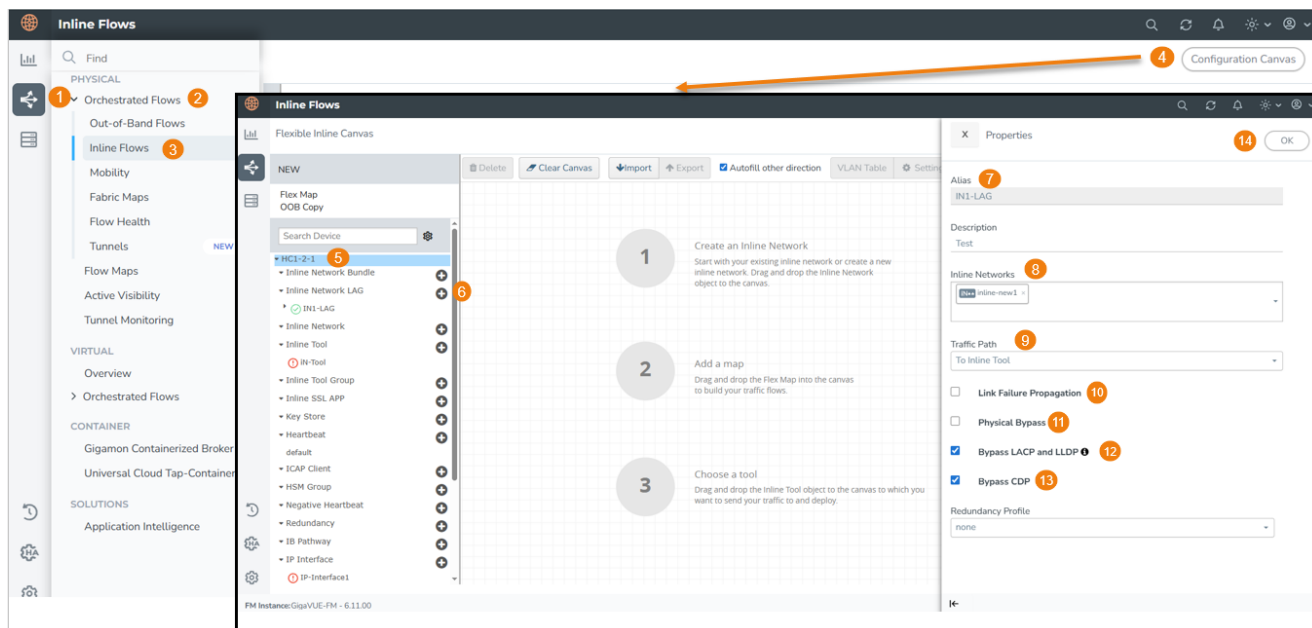
Notes:

- Inline Network LAG needs a bypass map to handle LACP bypass.
- When the Bypass LACP and LLDP checkbox is enabled, all protocol packets with MAC Destination **01-80-C2-XX-XX-XX** are bypassed.

10. If the port channel supports CDP, select the **Bypass CDP** (Cisco Discovery Protocol) check box to maintain CDP discovery functionality on the links that are connected to inline network LAG ports.

NOTE: When CDP/LLDP bypass is enabled, CDP/LLDP neighborhood discovery will not be established on the respective inline networks.

11. Click **OK** to save the configuration.



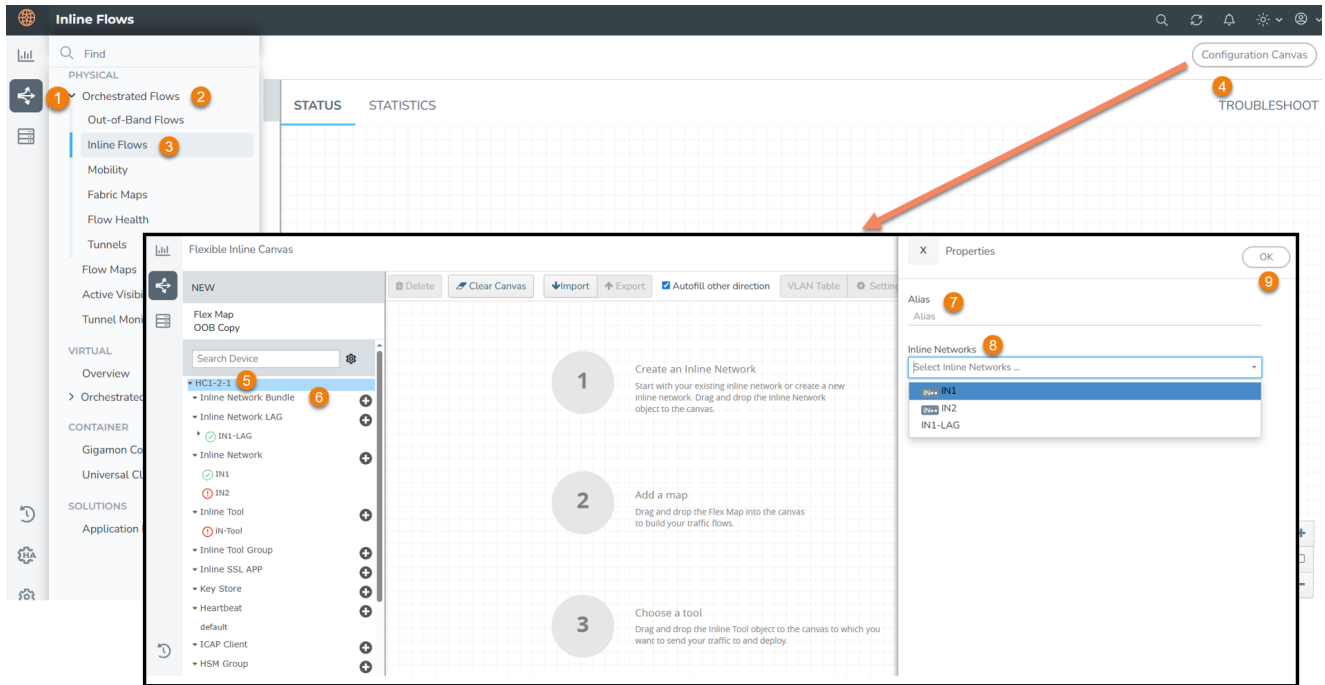
Configure Inline Network Bundle

Before You Begin - Configure the required inline network ports and inline networks before you set up an inline network bundle. Refer to [Configure Inline Network Ports and an Inline Network](#) for details.

To configure an inline network bundle:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the device where you want to configure the inline network bundle.
3. Click the '+' icon next to the **Inline Network Bundle** to create a new entry.
4. Enter a name for the inline network bundle in the **Alias** field.
5. From the **Inline Networks** drop-down list, select the inline networks you want to include in the bundle. Refer to [Configure Inline Network Ports and an Inline Network](#).
6. Click **OK** to save the bundle configuration.
7. Drag and drop the inline network bundle into the canvas, and configure the required inline map.
8. Enter the **Tool Side VLAN Tag** for each inline network added to the bundle.

9. Select the **TPID** for the Tool Side VLAN Tag.
 - o The default TPID is 0x8100.
 - o You can also select 0x9100 or 0x88a8 from the drop-down list.
10. Add the required rules for the inline map, and click **OK** to save the configuration.



Configure Inline Tool Ports and Inline Tools

To configure the inline tool ports and inline tools:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the device where you want to configure the inline tool.
3. Click the '+' icon next to the **Inline Tool** to create a new entry.
4. In the **Properties** pane, enter a name and description in the **Alias** and **Description** fields.
5. From the **Type** drop-down list, select one of the following options:
 - o **External** - To configure a third-party tool.
 - o **GigaVUE Node** - To configure a GigaVUE node as a tool.

6. Click **Port Editor**, and in the **Quick Port Editor**, scroll to the inline tool ports you want to configure. Select **Enable** to activate the ports, and click **OK**.
7. From the **Port A** and **Port B** drop-down lists, select the inline tool ports based on the direction the inline tool expects traffic from the network.
8. Verify that the **Enabled** check box is selected.
9. From the **Failover action** drop-down list, choose one of the following options:
 - **Tool Bypass** - Redirects traffic to the next inline tool or inline network port when a failover occurs.
 - **Network Bypass** - Puts inline networks in bypass mode (traffic flows from side A to side B and vice versa).
 - **Tool Drop** - Drops traffic and redirects it to a dummy VLAN with no members.

NOTE: If the failover action is set to 'drop' for an inline tool in the Flex iSSL solution, GigaSMART drops all traffic at the vport.

- **Network Drop** - Drops all traffic entering from side A and side B.
 - **Network Port Forced Down** - Brings down inline network ports.
10. Select the **Recovery Mode** to either **manual** or **automatic**.
 11. To define additional tags on the tool side, select the **Enable** check box for the **Inline tool Sharing mode**.

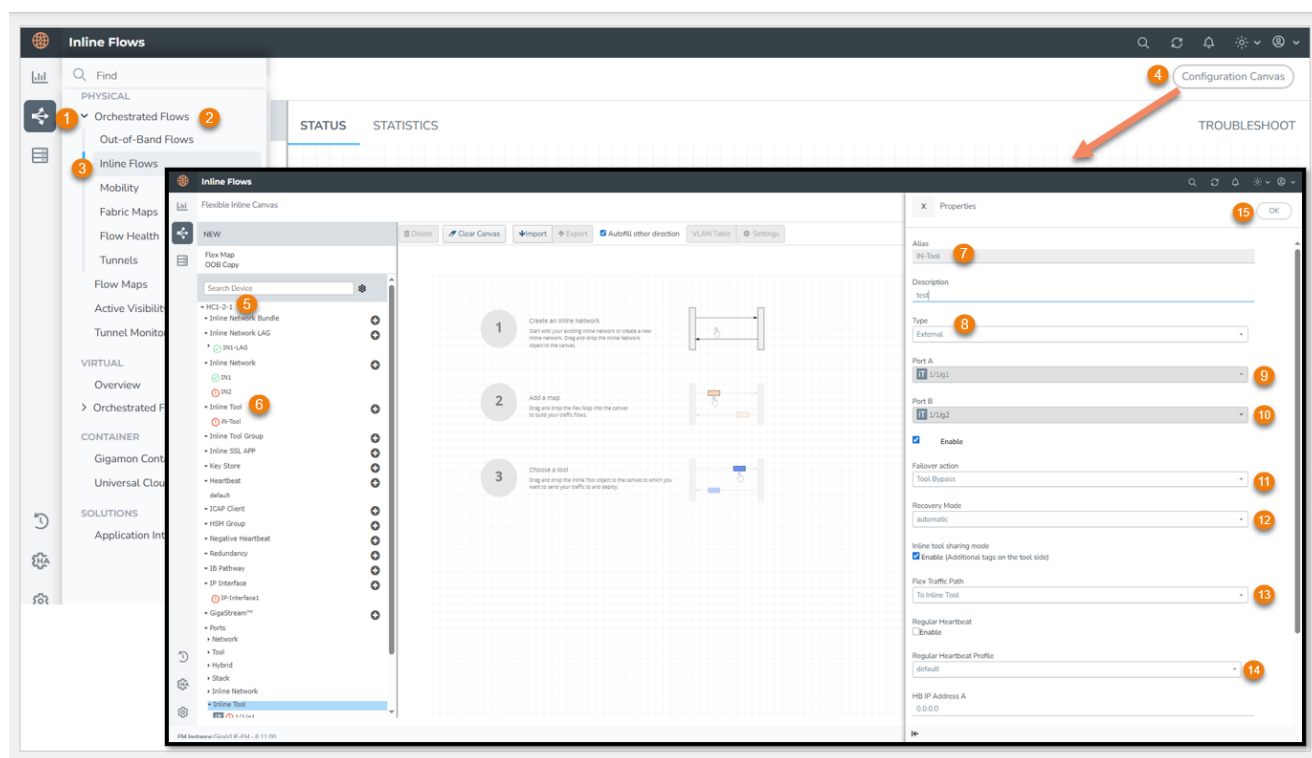
NOTE: If you disable **Inline Tool Sharing Mode**, you can use the inline tool only in one flexible inline map.

12. From the **Flex Traffic Path** drop-down list, select one of the following:
 - **Drop**- Drops traffic at the inline tool.

NOTE: If the failover action is set to 'drop' for an inline tool in the Flex iSSL solution, GigaSMART drops all traffic at the vport.

- **Bypass** - Redirects all traffic from the inline network to the opposite-side inline network port, bypassing all inline tools and tool groups. Traffic is not decrypted during this process.
 - **Bypass with Monitoring** - Sends traffic to the inline tool and absorbs it, while forwarding a copy to the next inline tool in the sequence. Also absorbs return traffic from side B.
 - **To Inline Tool** - Directs all traffic through the configured sequence of inline tools and tool groups based on their current status, and decrypts it.
13. If required, select the **Enable** check box for **Regular Heartbeat**, and choose a suitable profile from the **Regular Heartbeat Profile** drop-down list.
 14. Enter the IP addresses for side A and side B in the HB IP Address A and HB IP Address B fields, as defined in the heartbeat profile.

15. If required, select the **Enable** check box for **Negative Heartbeat**, and choose a suitable profile from the **Negative Heartbeat Profile** drop-down list.
16. Click **OK** to save the configuration.



Configure Inline Tool Group

Before You Begin - Configure the required inline tools before setting up an inline tool group. Refer to [Configure Inline Tool Ports and Inline Tools](#).

To configure an inline tool group:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the device where you want to configure the inline tool group.
3. Click the '+' icon next to the **Inline Tool Group** to create a new entry.
4. In the **Properties** pane, enter a name and description in the **Alias** and **Description** fields.
5. From the **Inline Tools** drop-down list, select the required inline tools.
6. From the **Weighting** drop-down list, choose one of the following options:

- **Equal**—Distributes traffic equally across all inline tools in the inline tool group. This is the default option.
- **Relative**—Distributes traffic to the inline tools in the inline tool group based on a relative weight or ratio assigned to the respective inline tools. The valid range is 1–256.
- **Percentage**—Distributes traffic to the inline tools in the inline tool group based on assigned percentages. The valid range is 1–100.

NOTE: If you select **Relative** or **Percentage**, enter the hash weights for the inline tools in the table below the **Weighting** drop-down list. Ensure that you assign a hash weight for each inline tool in the inline tool group. However, asymmetrical hashing is not supported for these options.

7. From the **Inline Spare Tool** drop-down list, select the inline tool that will receive traffic if the primary inline tool fails. To add a removed tool back to the spare list, delete it from the group and update it under the Inline Tool Group option in the canvas.

NOTE: You cannot select an inline spare tool if you choose a **Weighting** option.

8. Select the **Enabled** check box to make the inline tool group available for deployment.
9. Select the **Release Spare if Possible** check box to allow the spare tool to return to standby when the primary tool recovers.
10. From the **Failover Action** drop-down list, Choose one of the following options:
 - **Tool Bypass** - Redirects traffic to the next inline tool or inline tool group when a failover occurs.
 - **Network Bypass** - Puts inline networks in bypass mode (traffic flows from side A to side B and vice versa).
 - **Tool Drop** - Drops traffic for the affected inline tool or inline tool group.
 - **Network Drop** - Drops all traffic entering from side A and side B.
 - **Network Port Forced Down** - Brings down inline network ports.
11. From the **Failover Mode** drop-down list, select **Spread** to redistribute the traffic coming from the inline network (or inline network group) to the active inline tools (excluding the failed inline tool or tools).

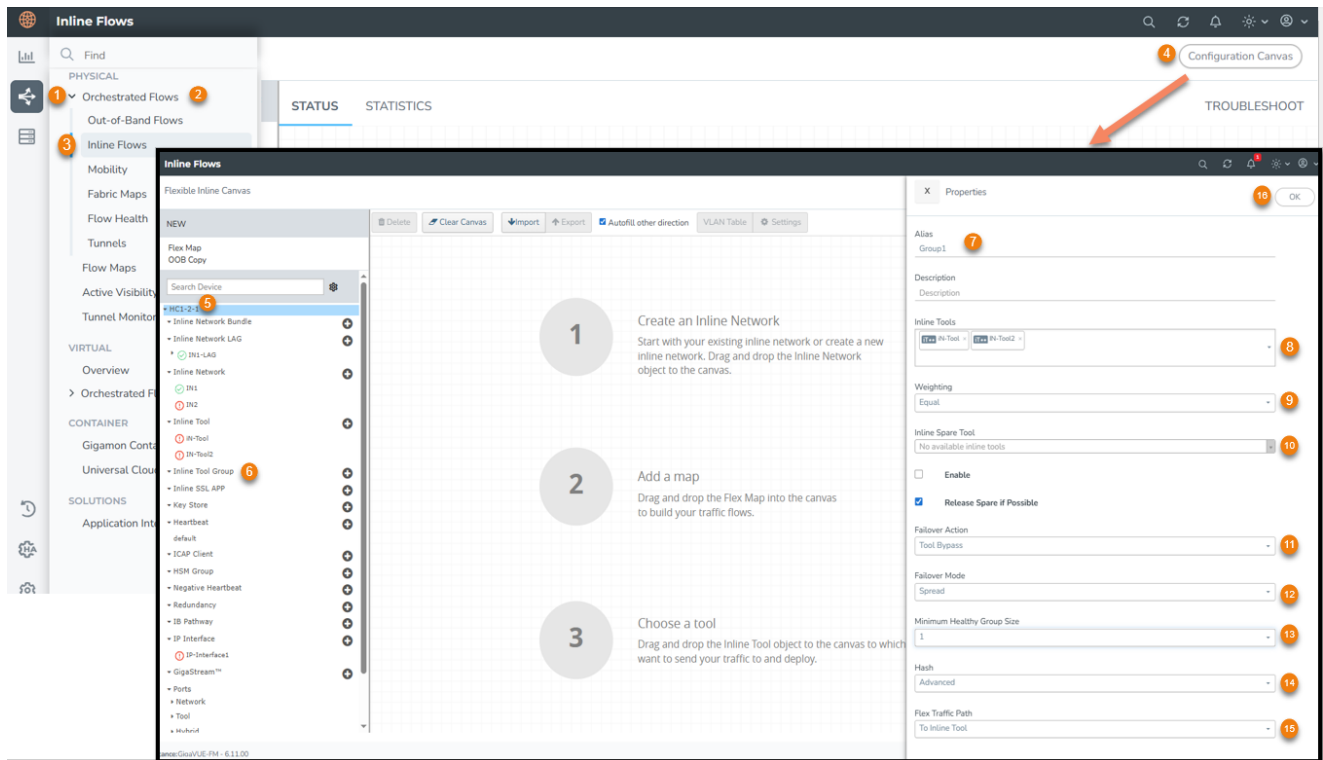
NOTE: This field is not applicable when there is only one inline tool in the tool list.

12. From the **Minimum Healthy Group Size** drop-down list, select the minimum number of inline tools (including the spare) required for the inline tool group to remain active.

13. From the **Hash** drop-down list, choose one of the following options to distribute packets across the inline tools in the group:
- **Advanced**—Uses symmetrical hashing, derived from the combination of packet fields based on the selected advanced-hash algorithm criteria
 - The most common criteria are the combination of source IP and destination IP addresses.
 - This produces a hash value that ensures all traffic from the same session is sent to the same inline tool in the group
 - **SideA as sourceIP & SideB as destinationIP**—Uses asymmetrical hashing, derived from the source IP address on side A and the destination IP address on side B of the inline network.
 - This produces a hash value that ensures all traffic from the same source address on side A is sent to the same inline tool in the inline tool group, regardless of destination or session.
 - **SideB as sourceIP & SideA as destinationIP**—Uses asymmetrical hashing, derived from the destination IP address on side A and the source IP address on side B of the inline network.
 - This produces a hash value that ensures all traffic from the same source address on side B is sent to the same inline tool in the inline tool group, regardless of destination or session.

NOTE: This field is not applicable if you select the **Relative** or **Percentage** options in the Weighting drop-down list.

14. From the **Flex Traffic Path** drop-down list, select one of the following options:
- **Drop** - Drops traffic at the inline tool group.
 - **Bypass** - Traffic bypasses the inline tool group. Use this option for performing maintenance on an inline tool group.
 - **Monitoring** - Sends traffic to the inline tool group and absorbs it, while forwarding a copy to the next inline tool group in the sequence. Also absorbs return traffic from side B.
 - **To Inline Tool** - Forwards traffic to the inline tool group.
15. Click **OK** to save the configuration.



Configure Inline Single VLAN Tag

During flexible Inline Bypass operations, network traffic sent to inline tools includes an extra VLAN tag. This tag helps identify traffic from inline tools and ensures correct routing to inline networks. However, many inline tools may not support extra VLAN tags. You can use Flexible Inline Single Tag to replace the extra VLAN tag on incoming traffic. This feature allows you to map incoming VLANs on the network side to outgoing VLANs on the tool side.

NOTE: The **OOB Copy** tag attribute **none** is invalid for single tag maps. Use the attribute **Original** or **as-inline** instead.

To configure an inline single tag:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the required inline network from the list of devices.
3. Drag and drop the inline network into the canvas.
4. Click **Settings** to open the **Settings** pane.

5. Select the **Enable** check box for **Show Single Tag Options**, and enter the VLANs expected on the inline network. Click **OK**.
6. Drag and drop a flexible inline map object into the canvas, and click the map to open the **Properties** pane.
7. Select the **Enable** check box for the **Single Tag Mode**, and enter the tool-side VLAN tags.
 - a. Use the **Enable Network Side VLAN Tag** check box to bulk enable or disable VLAN tags for flexible inline maps.
 - b. Select the **TPID** for the tool-side VLAN tag. The default value is 0x8100. You can also choose 0x9100 or 0x88a8 from the drop-down list. Click **OK**.



Notes:

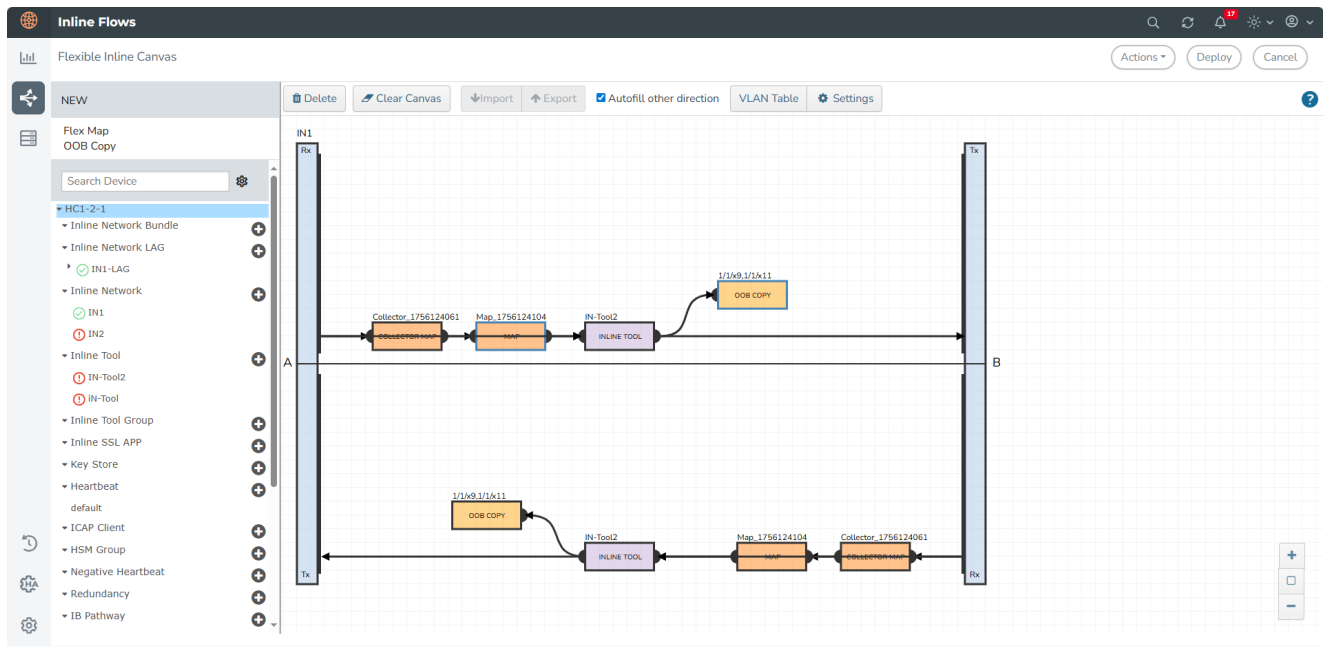
- GigaVUE-FM automatically adds a VLAN qualifier to the rules. If you don't specify any rules, it adds a default rule with the VLAN qualifier.
- You can enable or disable **Single Tag Mode** for collector maps if needed.

8. Drag and drop the required inline tools into the canvas.
9. Drag and drop the **OOB Copy** into the canvas, if required.
10. Click **Port Editor**, and in the **Quick Port Editor**, scroll to the hybrid or tool ports that you want to configure. Select **Enable** to activate the ports. Click **OK**.
11. From the **Destination Ports** drop-down list, select the required hybrid or tool ports to configure as destination ports. You can also select a hybrid or tool GigaStream. Refer to *"How to Use GigaStream"* section for details.
12. From the **VLAN Tag** drop-down list, select the required tags.
13. Click **OK** to save the configuration.



Notes:

- In GigaVUE-HCI-Plus, you cannot enable Single Tag Mode if the inline network's traffic path is in monitoring mode.
- If you enable the **Single VLAN Tag** option in a Flexible inline TLS/SSL Decryption solution, ensure that the **inline-ssl app profile** also has Single VLAN Tag configuration enabled.
- After deploying the solution, GigaVUE-FM preserves and displays any unused VLAN tags in the order they were configured.
- The VLAN Table window lists maps in the same order as shown in the configuration canvas.

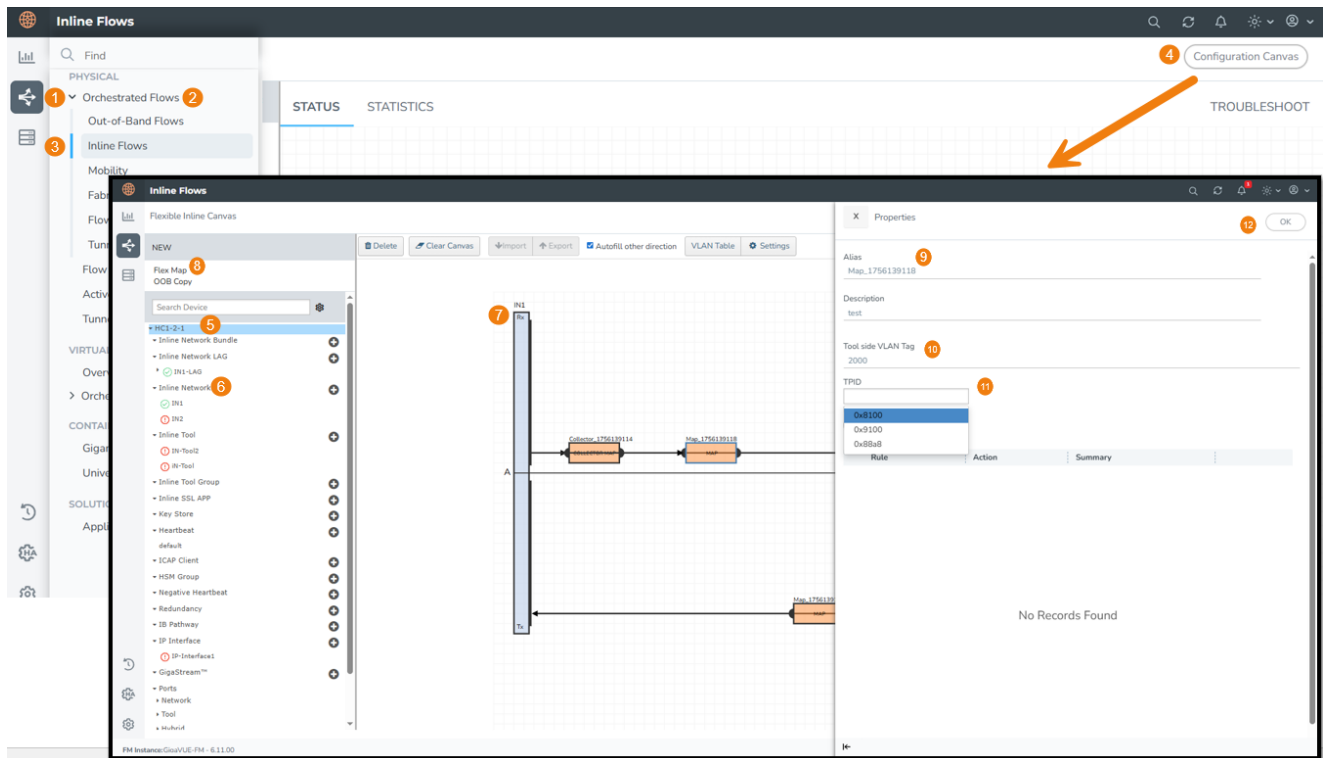


Configure Flexible Inline Maps

Before You Begin - Configure the required inline network before setting up Flexible Inline Maps. Refer to [Configure Inline Network Ports and an Inline Network](#).

To configure Flexible Inline Maps:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the device where you want to configure the Flexible Inline Maps.
3. Drag and drop the required inline network into the Flexible Inline Canvas.
4. Drag and drop the **Flex Map** into the Flexible Inline Canvas.
5. In the **Properties** pane, enter a name and description for the map in the **Alias** and **Description** fields.
6. Enter the required **Tool Side VLAN Tag**.
7. Select the **TPID** for the Tool Side VLAN Tag. The default TPID is 0x8100. The default TPID is 0x8100. You can also select 0x9100 or 0x88a8 from the drop-down list.
8. Add the required rules for the inline map. You can also import an existing map template..
9. Click **OK** to save the configuration.



Configure Resilient Inline Arrangement Solution

Before You Begin

1. A Resilient Inline Arrangement is performed on two GigaVUE devices .
2. Ensure that the names on both GigaVUE-FM,GigaVUE HC Series devices are identical, that is, the inline networks, inline tools, inline tool groups, out-of-band tools, and out-of-band tool GigaStreams must all have the same alias names on both the devices.
3. If you choose to use the inline network bundle, the alias of the inline network bundle on both the devices must be identical. However, the inline networks that are grouped into the bundle can have different aliases.

Once you are set with these basic prerequisites you can move forward to configure the following components:

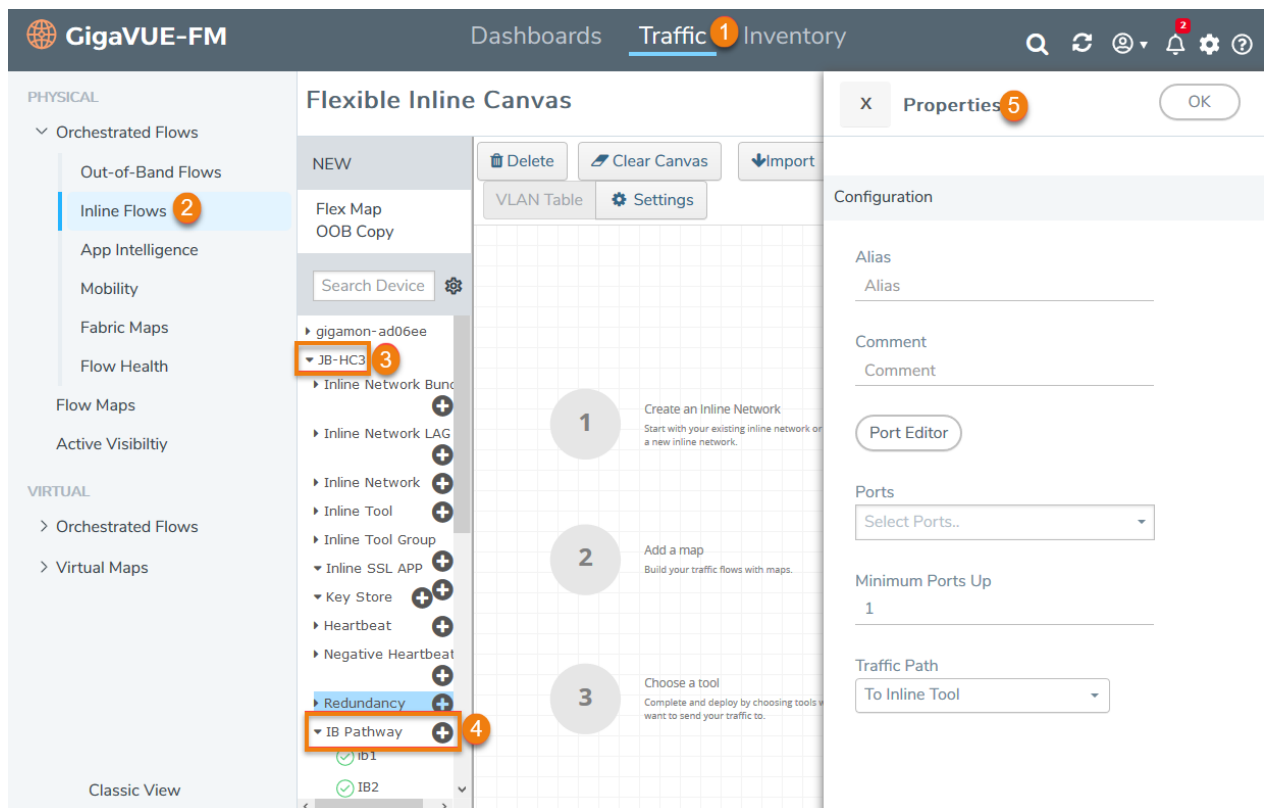
Create Inter-broker Pathway

To create a new inter-broker pathway:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the device where you want to create the inter-broker pathway.
3. Click the '+' icon next to the **IB Pathway** option to create a new inter-broker pathway.
4. In the **Properties** pane, enter a name and description in the **Alias** and **Description** fields..
5. From the **Ports** drop-down list, select the required tool ports to attach to the inter-broker pathway.

NOTE: If the required tool ports are not available, you can enable them administratively. Click **Port Editor**, scroll to the tool ports you want to configure in the **Quick Port Editor** page, select **Enable**, and click **OK**.

6. In the **Minimum Ports Up** field, enter the minimum number of tool ports that must be operational for the inter-broker pathway status to be "**Up**".
7. From the **Traffic Path** drop-down list, select one of the following options:
 - **Bypass**—Traffic bypasses the inter-broker pathway and is redirected to the next inline network port.
 - **Monitoring**—Traffic is forwarded to the sequence of inline tools in the monitoring mode.
 - **To Inline Tool**—Traffic is forwarded to the sequence of inline tools you have configured.
8. Click **OK** to save the configuration.



Configure Resilient Inline Arrangement

To configure a resilient inline arrangement:

1. Drag and drop the required inline network or inline network LAG into the flexible inline canvas, and click **Settings**.
2. In the **Settings** pane, select the **Enable** check box next to **Show Single Tag Options** to configure the resilient inline arrangement with a single VLAN tag.

NOTE: Enable **Show Single Tag Options** only if your inline tools do not support Q-in-Q VLAN tags.

3. Select the **Enable** check box next to **Show Resilient Inline Menu**.
4. Select the required **Node 1**, **Node 2**, **IB Pathway1**, and **IB Pathway2** for the resilient inline arrangement.
5. From the **Hashing Source** drop-down list, select one of the following options:
 - **Side A** - Hashing uses source IP or source port from Side A; destination IP or destination port from Side B.
 - **Side B** - Hashing uses source IP or source port from Side B; destination IP or destination port from Side A.
6. From the **Hashing Type** drop-down list, select one of the following options:
 - **L3 (IP Based)** - Hashing uses the IP address.

- **L4 (Port Based)** - Hashing uses the transport layer port number.
7. From the **Hashing LSB Node** drop-down list, select one of the following options:
 - **Node 1 as 0** - Traffic from IPs ending in 0 is hashed to Node 2.
 - **Node 2 as 0** - Traffic from IPs ending in 0 is hashed to Node 1.

NOTE: This option is available only if you selected **L3 (IP Based)** in the Hashing Type field.

8. From the **Hashing Port** drop-down list, select one of the following options:
 - **Node 1 as odd** - Traffic with odd port numbers is hashed to Node 2, while traffic with even port numbers is hashed to Node 1.
 - **Node 2 as odd** - Traffic with odd port numbers is hashed to Node 1, while traffic with even port numbers is hashed to Node 2.

NOTE: This field is available only if you select the **L4 (Port Based)** option in the **Hashing Type** field.

9. Click **OK** to save the settings.
10. Drag and drop the flexible inline map into the canvas. Click the map to open the Properties pane.
11. In the **Alias** and **Description** fields, enter the name and description of the inline map.
12. To deploy the resilient inline arrangement with a **single VLAN tag**, select the **Enable** check box next to Single Tag Mode. Refer to [Configure Resilient Inline Arrangement Solution](#).

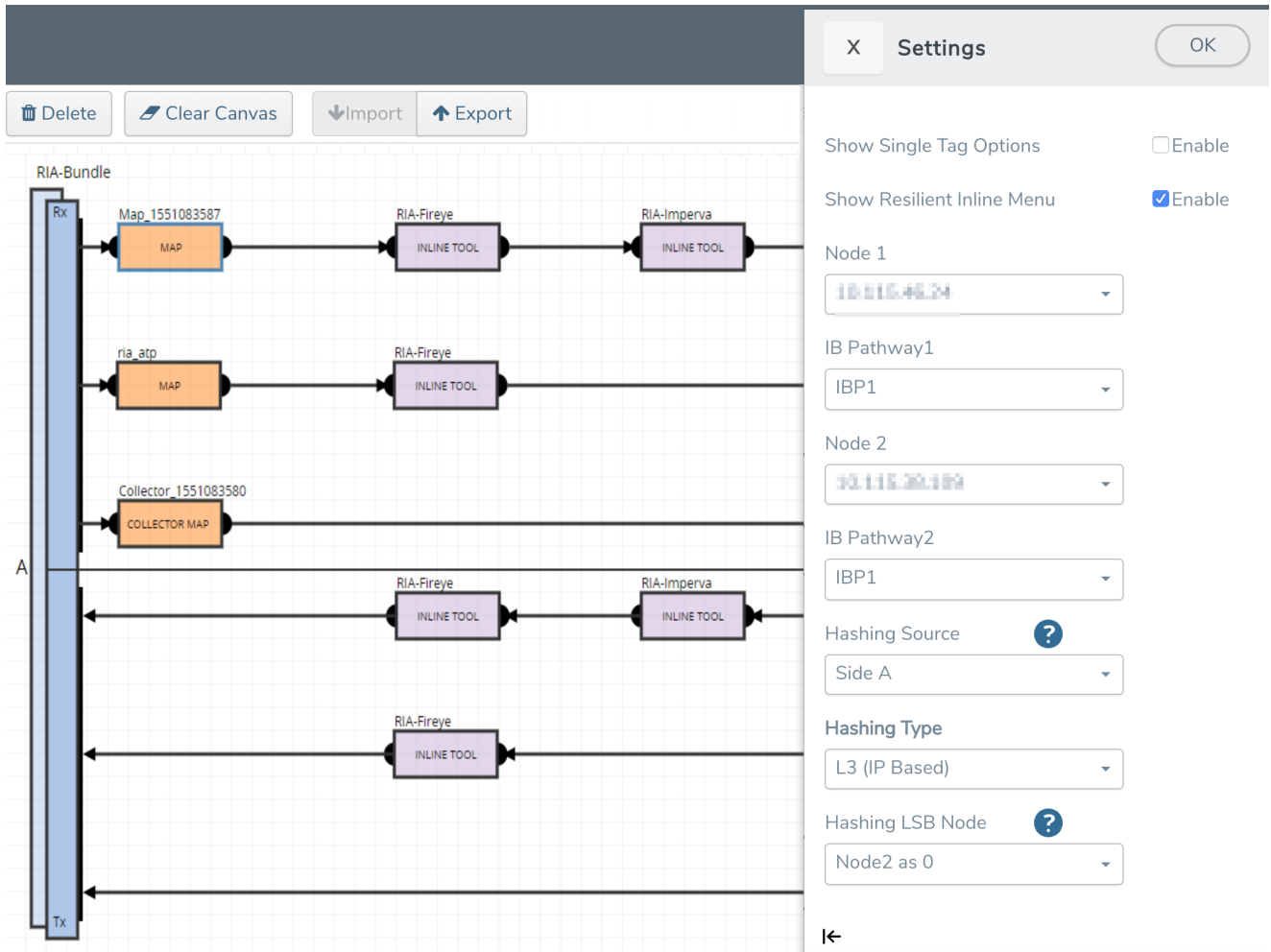
NOTE: You can choose to disable the **Single Tag Mode** for collector maps, if required.

13. Enter the **Tool Side VLAN Tag** for the inline network you are configuring.
14. Select the **TPID** for the Tool Side VLAN Tag. The default value is 0x8100. You can also choose from the supported values 0x9100 and 0x88a8 in the drop-down list.
15. From the **FlexInline Failover** drop-down list, select one of the following options:
 - **Bypass** - Traffic passes directly between the respective inline network ports.
 - **Original Map** - Traffic follows the path defined in this Flexible Inline Map.
16. Add the required rules for the inline map. Click **OK** to save the configuration.
17. Drag and drop the required **Inline Tools** or **Inline Tool Group** into the canvas.
18. If needed, drag and drop the **OOB Copy** into the canvas.
19. From the **Destination Ports** drop-down list, select the required hybrid or tool ports.
20. From the **VLAN Tag** drop-down list, select one of the following options:
 - **None** - No VLAN tag is used; traffic is routed to a different destination.

- **Original** - Uses the original VLAN tag from the packet received from the inline network.
- **As Inline** - Uses the VLAN tag configured for the Flexible Inline Map.

NOTE: The **As Inline** option is available only when you configure the Resilient Inline Arrangement with a single VLAN tag.

21. Click **Deploy**, select a traffic path and click **OK**.



Configure ICAP Client

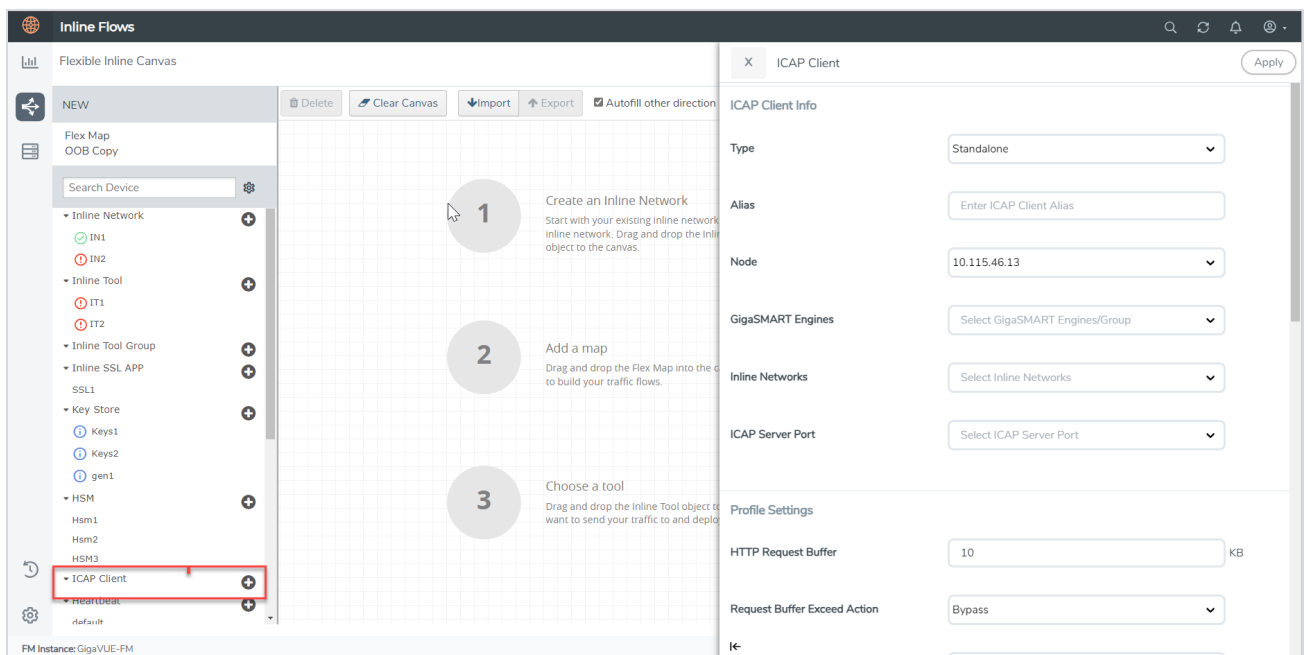
Before You Begin:

- Configure the required inline networks. Refer to [Configure Inline Network Ports and an Inline Network](#).
- Configure the required IP Interface. Refer to [Configure IP Interface](#).

NOTE: For ICAP, it is not necessary to add GS Groups when configuring IP interface. It will be added automatically when the port is added to ICAP Client.

To configure the ICAP Client:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the ICAP Client.
3. Click the '+' icon next to the **ICAP Client** to create a new entry.
4. Enter a name and description for the inline network in the **Alias** and **Description** fields.



5. In the **ICAP Client** properties pane that appears on the right, complete the required fields in the ICAP Client Info, Profile Settings, and the Server sections. Refer to [ICAP Client—Field References](#) for more details.
6. Select one from the following:
 - o If ICAP and iSSL are integrated and deployed on the same node, select the **Same Node** option.
 - o If ICAP and iSSL are integrated and deployed on different node, select the **Different Node** option.
7. Select the required tool port of Inline SSL profile, which is connected to the inline network of ICAP. (This option will not appear if you select standalone as type.)
8. Click **Apply** to save the configurations.

ICAP Client—Field References

The following table lists and describes the attributes that define the ICAP Client.

Field	Description
ICAP Client Info	
Type	Select the required type from the following: - If ICAP is deployed without iSSL and the traffic from devices other than Gigamon is sent to ICAP, select the Standalone option. - If ICAP and iSSL are integrated and deployed on the same node, select the Same Node option. - If ICAP and iSSL are integrated and deployed on different node, select the Different Node option.
Alias	Enter a unique name for the ICAP Client.
Node	Select the required node for which you want to configure the ICAP Client.
GigaSMART engines	Select the required GigaSMART engine.
Inline Networks	Select the required inline networks, which are the source for the ICAP app.
Source Ports	Select the required tool port of iSSL, which is connected to the inline network of ICAP. (This option will not appear if you select standalone as type.)
ICAP Server Port	Select the required IP interface physical port.
Profile Settings	
HTTP Request Buffer	Enter the HTTP request buffer size.
Request Buffer Exceed Action	Select the buffer action on exceeding the size: - Drop - The traffic is dropped. - Bypass - The traffic bypasses on exceeding the buffer size.
Preview Size	Enter the required preview size.
REQMOD	Enable or disable the Request Modification Mode.
RESPMOD	Enable or disable the Response Modification Mode.
Response Timeout	Enter the response timeout in seconds.
Response Timeout Action	Select the response timeout action on exceeding the timeout: - Drop - The traffic is dropped - Bypass - Traffic is bypasses on exceeding the response timeout limit.
Inactivity Timeout	Enter the session inactivity timeout value in seconds.
Port Range	Enter the ICAP client source port range for connecting to ICAP server.
Server	
Server Alias	Enter a unique name for the ICAP Server.
Description	Enter a description for the ICAP Server.
Port	Enter the L4 port number on which the ICAP server is listed.
Address	Enter the L3 IPV4/IPV6 address of the ICAP server.

Field	Description
Request Modification URL	Enter the Request Modification service URL.
Response Modification URL	Enter the Response Modification service URL.
Options URL	Enter the ICAP options URL (if necessary).

Configure GRIP Solution

To configure the GRIP solution software:

1. On the left navigation pane, go to **Inventory**  **> Nodes**. Click on the Left Node in which the configuration needs to be done.
2. Go to **System > Ports > Ports > All Ports**. Select the port that would act as the signaling port and click **Edit**.
3. Select **Enable for Admin**.
4. Select Type **Stack**.
5. Click **OK**.
6. Repeat steps 1 through 5 on the right node to complete the signaling port type configuration.
7. Go to  **> Physical > Orchestrated Flows > Inline Flows > Configuration Canvas** to create a new Flexible Inline Canvas.
8. In the displayed canvas, select the device where you want to configure and click the '+' icon next to the **Redundancy** to create a new entry.
9. Enter a name for the profile in the Alias field.
10. Click on the Signaling Port field and select the stack port configured in Step 4. Select **Primary** for Protection Role.
11. Click **OK**.
12. Repeat Steps 8 through 11 for the right node to complete the Redundancy Profile Configuration but select Protection Role as **Secondary**.

Configure Synchronization

You must synchronize the configuration of the two GigaVUE-FM, GigaVUE HC Series nodes involved in the GRIP solution. The configuration items that must be synchronized are as follows:

- the signaling ports, as dictated by the signaling link cabling

- the inline networks, as dictated by the network path cabling between the two GigaVUE-FM,GigaVUE HC Series nodes
- the redundancy profiles. The redundancy profile of each GigaVUE-FM,GigaVUE HC Series nodes needs to have the same signaling port as well as a redundancy role that is compatible with the redundancy role on the other GigaVUE-FM,GigaVUE HC Series node. For example, one is configured with the primary role and one is configured with the secondary role.
- the inline tools
- the inline maps

In the example below , the configuration is the same on both nodes, except for the protection role (primary or secondary).

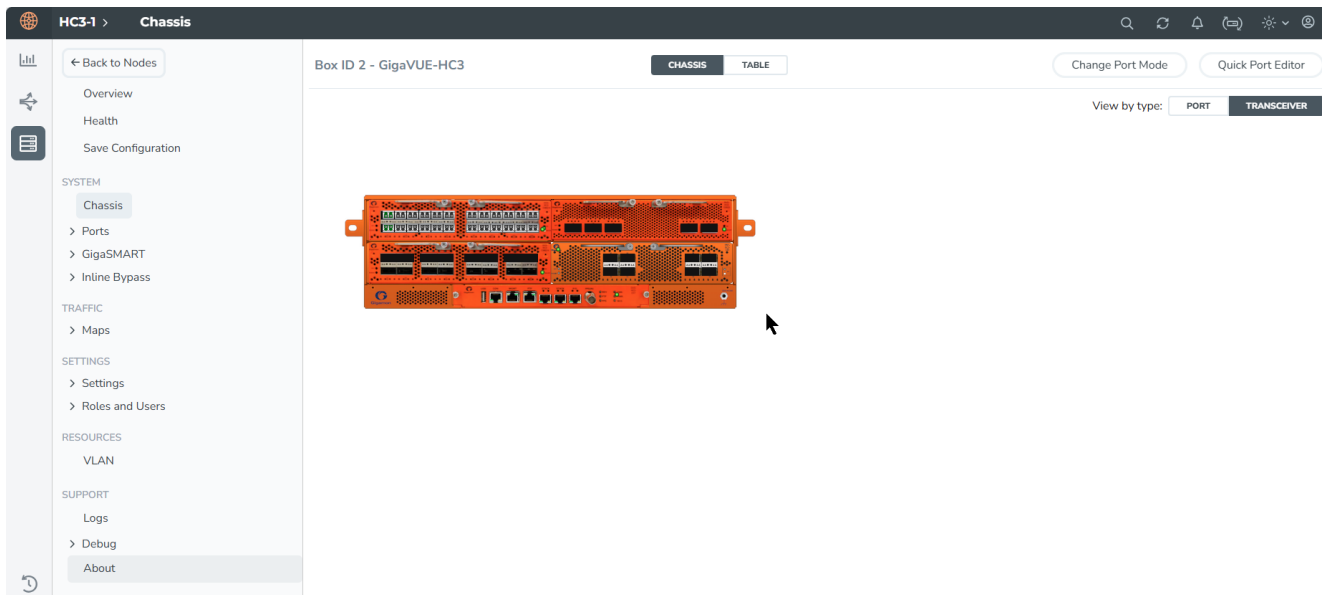
Example: Gigamon Resiliency for Inline Protection

Example is an Inline Bypass solution for GRIP using TAP-HCI-G10040 modules on the GigaVUE-HCI, with copper ports.

First, configure the GigaVUE-HCI with the primary role, then configure the GigaVUE-HCI with the secondary role. The configuration is the same (is synchronized) on both nodes, except for step 3, in which the protection role (primary or secondary) is specified.

Note that in this example, link fail propagation (LFP) is disabled to reduce inline network recovery time after failover. When a primary to secondary failover occurs and LFP is enabled for copper Inline Bypass links, network service recovery may take several seconds because of Ethernet link renegotiation. Optical links failover faster and typically recover service much faster. For inline networks where only one path is available, this is a consideration. When GRIP is deployed with high availability networks where a second path is present, it is a best practice to leave LFP enabled.

You can use the Chassis page to view the chassis and modules.



Configure Primary Role GigaVUE-HC1

Task	Description	UI Steps
1.	Configure ports on the TAP-HC0-G100C0 module as passive (in passive mode, relays are closed). Also configure ports, port type (inline-network).	- Go to System > Ports > Ports > All Ports. - Select a port of the TAP-HC1-G10040 module. - Click to open the Ports page. - Select Passive for TapTX - Click Save. - Repeat steps 2 through 6 for each port on the TAP-HC1-G10040 module - Configure Inline Network ports - Select the port. - Click Quick Port Editor. - Select Inline Network for Type. NOTE: You can use the Chassis page to locate the position of the module in the chassis and identify port IDs.
2.	Configure stack port (for signaling port/link) and enable it.	- Select the port and click Edit. - Select Enable for Admin. - Select Stack for Type. - Click OK.
3.	Create the redundancy profile by giving it a name and configuring parameters for the redundancy profile such as the signaling port and protection role (primary).	- Select Physical > Orchestrated Flows > Inline Flows > Configuration Canvas > Redundancy. - Click '+' icon. - Enter a name for the profile in the Alias field. For example, RP_001. - Click in the Signaling Port field and select the stack port configured in Task 2.

Task	Description	UI Steps
		5. Select Primary for Protection Role. 6. Click OK.
4.	Configure inline network. This step associates the redundancy profile to the inline network and also disables link fail propagation on the inline network.	Refer to the Configure Inline Network Ports and an Inline Network section for configuration details.
5.	Configure inline tool ports, port type (inline-tool), and administratively enable them.	1. Select Physical > Orchestrated Flows > Inline Flows > Configuration Canvas > Inline Tool. 2. Select the first port (for example, 1/4/x1) to configure as an inline-tool port. 3. Select Inline Network for Type and select Enable for Admin. 4. Select the second port (for example, 1/4/x2) and repeat steps 3 through 5.
6.	Configure inline tool and failover action. then enable inline tool.	Refer to the Configure Inline Network Ports and an Inline Network section for configuration details.
7.	Configure map passall, from inline network to inline tool. NOTE: When you delete a map on the primary node, irrespective of the inline-network traffic-path, the traffic is switched to the secondary node. The port utilization must be 0% on the primary node and active on the secondary node.	Refer to the Configure Inline Network Bundle section for configuration details.

Configure Secondary Role GigaVUE-HC1

Task	Description	UI Steps
1	Configure ports on the TAP-HC0-G100C0 module as passive (in passive mode, relays are closed). Also configure ports, port type (inline-network).	1. Go to System > Ports > Ports> All Ports. 2. Select a port of the TAP-HC1-G10040 module. 3. Click to open the Ports page. 4. Select Passive for TapTX 5. Click Save. 6. Repeat steps 2 through 6 for each port on the TAP-HC1-G10040 module 7. Configure Inline Network ports a. Select the port. b. Click Quick Port Editor. c. Select Inline Network for Type. NOTE: You can use the Chassis page to locate the position of the module in the chassis and identify port IDs.
2	Configure stack port (for signaling port/link) and enable it.	1. Select the port and click Edit. 2. Select Enable for Admin. 3. Select Stack for Type. 4. Click OK.
3	Create the redundancy profile by giving it a name and configuring parameters for the redundancy profile such as the signaling port and protection role (secondary).	1. Select Physical > Orchestrated Flows > Inline Flows > Configuration Canvas > Redundancy. 2. Click '+' icon. 3. Enter a name for the profile in the Alias field. For example, RP_001. 4. Click in the Signaling Port field and select the stack port configured in Task 2. 5. Select Secondary for Protection Role. 6. Click OK.
4	Configure inline network. This step associates the redundancy profile to the inline network and also disables link fail propagation on the inline network.	Refer to the Configure Inline Network Ports and an Inline Network section for configuration details.
5	Configure inline tool ports, port type (inline-tool), and administratively enable them.	1. Select Physical > Orchestrated Flows > Inline Flows > Configuration Canvas > Inline Tool. 2. Select the first port (for example, 1/4/x1) to configure as an inline-tool port. 3. Select Inline Network for Type and select Enable for Admin. 4. Select the second port (for example, 1/4/x2) and repeat steps 3 through 5.

Task	Description	UI Steps
6	Configure inline tool and failover action. then enable inline tool.	Refer to the Configure Inline Tool Ports and Inline Tools section for configuration details.
7	Configure map passall, from inline network to inline tool.	Refer to the Configure Inline Network Bundle section for configuration details.
8	Configure the path of the traffic to the inline tool, disabling physical bypass on the inline network to open the relay on the node with the primary role.	Refer to the Configure Inline Network Ports and an Inline Network section for configuration details.

Redundancy Control State

To display the Redundancy Control State, go to the Inline Networks page and click on the alias of the Inline Network for which you want to display the redundancy control state. The state is displayed on the Quick View under Configuration.

The below table describes the different Redundancy Control States.

Table 6: Redundancy Control States

State	Description
Neutral	No redundancy profile is configured.
Suspended	The protection role is configured as suspended.
Primary Forwarding	The protection role is configured as primary. The node is acting in the primary role. Traffic flows through this node.
Secondary Bypass	The protection role is configured as secondary. The node is acting in the secondary role. Traffic bypasses this node.
Secondary Forwarding	The protection role is configured as secondary. The node is acting in the primary role due to a loss of power on the primary node. Traffic flows through this node.

How to Use Suspended Role for Maintenance

Use the suspended protection role to perform maintenance activities on the primary and secondary nodes. Maintenance activities include: bringing up a module, shutting down a module, or swapping a module.

For example, to remove a module on one of the GigaVUE-HC3 nodes (Primary node), use the following steps on that module:

1. Select **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas > Redundancy**.

2. On the Redundancies page, for **Protection Role**, select **suspended**, and then click **OK**.
3. Once this is configured, the Primary node will be moved to 'Suspended' and the Secondary node will be moved to 'Secondary Forwarding' state. All the traffic will now be forwarded to the Secondary node and the Inline Tool inspection takes place.
4. Perform the maintenance activity in Primary node, like bringing up a new module, shutting down a module, swapping the modules, replacing the external inline tool.
5. Once the maintenance is done, revert the **Protection Role** in Primary Node back to **'primary'**. This will move the Redundancy Control State back to the **Primary Forwarding** and traffic will start flowing via the Primary Node.

In case of a maintenance activity (chassis, card, external inline-tool) required in Secondary node follow the below steps:

1. Set the Protection Role to **'suspended'** in the redundancy profile.
2. Once this is set, the Secondary node will be moved to **'Suspended'** and the Primary node will remain in the **'Primary Forwarding'** state and will handle the traffic.
3. Do the required maintenance activity in secondary node.
4. Once the maintenance is done, revert the Protection Role in Secondary Node back to **'secondary'**.
5. This will move the Redundancy Control State back to the **"Secondary Bypass"**.

How to Upgrade GigaVUE Nodes in GRIP Deployment

There are no specific procedures for upgrading the nodes in the GRIP deployment, but we would recommend the below steps to be on the safer side. Even when the upgrading device goes into an issue state, traffic will be inspected in any one of the nodes.

- Refer the *"Supported Upgrade Path—Standalone Nodes"* to know about the order of build version in which the GigaVUE-OS needs to be upgraded.
- Save the configuration and take the backup of both Primary and Secondary node.
- First upgrade the secondary node so that traffic will get inspected in the Primary node.
- Once the Secondary node upgrade gets completed then go for the Primary node upgrade.
- When the Primary node upgrade is in progress, traffic will be inspected in the Secondary node as the failover kicks in, with the help of the signaling port.
- As soon as the Primary node upgrade is complete, the signaling port will come up, and the Primary Node will start inspecting the traffic.

Troubleshoot

If any of the below issues occur, kindly follow the given steps to troubleshoot the issue.

Signaling Ports Down

1. Check if the power is proper from the optics; if not, try replacing the optics with new ones in a maintenance window
2. If the issue occurs after reloading, check if the maps are configured on the inline network to which the redundancy profile is attached.
3. If maps are not configured, deploying a map will bring up the signaling ports.
4. If a map is available and the signaling ports are still down, contact Gigamon Support for assistance.

Traffic outage in Inline Tool

1. Check if the Redundancy Control State is set to Primary Forwarding in the Primary node or Secondary Forwarding in case traffic is handled in the Secondary Node.
2. Check if the Inline Tool Flex Traffic Path is configured as "Bypass" by mistake. If so, revert to To-Inline-Tool to recover the traffic.
3. Check if the Inline Tool ports are in downstate and failover kicked into tool bypass (the default failover for Inline Tool). If so, correct the optics power, cable, and external Inline Tool faultiness.
4. If the issue persists, contact Gigamon Support for assistance.

Network Traffic Outage

1. Check if any of the Inline Tool's Flex Traffic Paths is set to "Drop" by mistake. If so, revert the Flex Traffic Path to To-Inline-Tool.
2. Check if any Inline Tool ports are down and failover kicked into tool-drop or network-drop. If so, check the optics power, cable, and External Inline Tool Faultiness and correct the same.
3. Check if the traffic hits the map and drops in any Inline Component ports using 'show port stats port-list <port-alias>.'
4. Try redeploying the Flex Inline Solution from GigaVUE-FM and check if the traffic resumes. If not, contact Gigamon Support for assistance.

Configure TLS/SSL Decryption Solutions

NOTE: Starting in release 6.14.00, Entrust/nCipher HSM integration is deprecated. Gen2 DSSL HSMs (nCipher v1.0) and Gen3 HSMs using nCipher 12.6 (`nshield\_12\_60`) are no longer supported, and upgrades are blocked if any nCipher HSM configuration is present.

The Inline TLS/SSL Decryption solution can be configured based on use cases. Refer to the following topics for various use cases:

- [Configure Inline TLS/SSL Decryption Solution with Layer 2 Tools](#)
- [Configure Inline TLS/SSL Decryption Solution with Layer 3 Tools](#)
- [Configure Inline TLS/SSL Decryption Solution with RIA](#)
- [Configure Thales-Luna HSM for TLS/SSL Decryption](#)
- [Configure ICAP Client for Inline TLS/SSL Decryption Solution](#)

Inline SSL App—Field References

These are the fields that you will come across while configuring the **Inline SSL APP**. The table below provides a list and description of the attributes that define the Flexible Inline Decryption solution.

Field	Description
Alias	Enter a unique name for the flexible inline SSL APP.
Resilient Inline Arrangements	Enable this to configure a Resilient Inline Arrangement.
GS engines	Select the required GigaSMART engines.
TLS/SSL Monitor Mode	Select a TLS/SSL Monitor Mode from one of the following options: • Enable—When the monitor mode is enabled, the TLS/SSL decryption or encryption is off. The monitor application collects information, such as the TCP ports in use and VLAN information about the incoming traffic, and forwards the packets to the tool port or network port based on the non-TLS/SSL TCP bypass action. • Disable—This is the default value. When the monitor mode is disabled, the TLS/SSL decryption or encryption is on. Use this mode during the deployment stage. • Inline—Both monitor mode and TLS/SSL decryption or encryption are on. Use this mode to debug issues.
HSM Group	Select an HSM Group alias that you have configured from the drop-down list. Select Disable from the drop-down list to disable the HSM Group.

Field	Description
	 Notes: Thales-Luna Network HSM configuration is supported in Inbound, Outbound, and Hybrid deployment types.
Advanced Session Statistics	Enable this option to visualize advanced Inline SSL Session dashboards, such as Session Insights and Session Table, in the Fabric Health Analytics dashboard. The basic dashboards are available by default as you configure an Inline SSL session. Refer View Inline TLS/SSL Dashboards to know more.
Keychain Password	The keychain password must be configured before installing certificates and keys. To add or reset the Keychain Password: - Click Keychain Password, and then choose either Add or Reset. - If you choose to reset the Keychain Password, enter a password that is 8 to 30 characters long and contains at least one numerical character, one uppercase character, one lowercase character, and one special character. - Select the Auto Login check box to enable GigaVUE-FM to unlock the keystore when the device reboots. - Click OK to save the Keychain Password.
Add new keys	To configure a certificate-key pair: - Click Add new keys to open the Key page. - Enter a name and description for the key. - Select the required Key Type and File Type. - You can choose to include a Passphrase for the key when you select PEM or PKCS12 as File type if needed. - When you choose Luna-HSM, enter the Key label for the key. - Add the required Private Key and Certificate. - Click OK to save the configuration.
Deployment Type	Select one of the following deployment types: - Inbound—For inbound deployments, add a new Server Key Mapping. Enter the domain name or IP address of the server, and then select the required Key Pair Alias. - Outbound—For outbound deployments, add a primary and a secondary signing Certificate Authorities (CA). - Hybrid—For hybrid deployments, add a new Server Key Mapping, and a primary and a secondary signing CA.
mTLS	Enables mutual TLS (client certificate authentication) for inbound and hybrid Inline TLS/SSL sessions that use this profile.
Configurations	
Default Action	Select one of the following options : - Decrypt—Decrypt all the traffic that is guided into the Inline SSL APP. - No Decrypt—Do not decrypt the traffic that is guided into the Inline SSL APP.
URL Cache Miss Action	Select one of the following options: Decrypt— This option Decrypts all the traffic that is guided into the Inline SSL APP.

Field	Description
	- No Decrypt— This will not decrypt the traffic that is guided into the Inline SSL APP. - Defer—Delay the decryption until the Defer Timeout seconds provided.
Tool Fail Action	The failover action taken in response to a failure of an inline tool. Select one of the following options: - Bypass Tool—The traffic bypasses the failed inline tool. - Drop Connection—The traffic is dropped.
Tool Bypass	Select the required options: - Decrypted TLS/SSL Traffic—Bypasses the decrypted SSL traffic. - No Decrypted TLS/SSL Traffic—Bypasses the non-decrypted SSL traffic. - Non-TLS/SSL TCP Traffic—Bypasses the non-TLS/SSL, that is the TCP intercepted traffic.
High Availability	Select the check box to detect the link switchover by upstream device that is in active or standby mode. NOTE: Do not select this check box if the inline network links are in active state.
Network Group Multiple Entry	Select this check box to allow the traffic from different inline network to reenter GigaSMART.
Tool Early Engage	Select this check box to allow the inline tools to change the MAC address or VLAN IDs. When a connection request is received from the client, GigaSMART establishes the connection with the inline tool first, before connecting with the server. This helps the inline tools to modify the MAC address or VLAN IDs when sending the traffic back to the server.
HTTP Downgrade	HTTP 2.0 Downgrade option is enabled by default. HTTP 2.0 traffic is downgraded to HTTP 1.1 for decryption. If the downgrade option is disabled, HTTP 2.0 traffic is forwarded without decryption.
NAT/PAT mode	Enable this to perform NAT/PAT (Network/Port Address Translation) in Layer-3 inline tools .
Tool Early Inspect	Select this check box to allow the inline tool to inspect the decrypted data first before connecting to the server. This will allow the inline tool to validate the data and ensure that only valid connections are sent to the server.  Notes: - You can access Tool Early Inspect feature from the flex Inline SSL APP only. Tool Early Inspect cannot co-exist with features such as RIA, NAT/PAT mode, Tool Early Engage, One-Arm, and Decryption Port Mapping. - If Tool Early Inspect is enabled, you can configure the connections timeout value. Connection timeout represents the time by which the tool should respond after receiving the first decrypted data. If no response is received within the configured time interval, the connections will be reset.
StartTLS Port	Enter the required SSL/TLS ports.
MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that can be transferred as a single entity in a network connection.

Field	Description
Session Logging	
Session Logging	Select the Enable check box to log the Inline TLS/SSL session related information to a remote server.
IP Version	Select IPV4 or IPV6 as the IP Version for the Session Logging server. You can select one session logging configuration per GigaSMART group.
Remote Syslog Server IP	Enter the IP address of the remote syslog server.
Associated IP Interface	In the Associated IP interface drop-down list, select the IP interface that you assigned to the GigaSMART group.
Remote Syslog Port Number	Enter the port number of the remote syslog server.
Log Level	In the Log Level drop-down list, select the severity log level of the events that you want to send to the inline TLS/SSL session logging server.
Traffic Path	
Single VLAN Tag	Enable the check box to deploy flexible inline TLS/SSL solution with a single VLAN tag. If an inline tool is involved in an inline TLS/SSL map, the inline tool can be supported across multiple maps with different single VLAN tags. NOTE: Deploying a flexible Inline SSL solution with SVT is optional, and you can choose to enable or disable the Single VLAN Tag option. If you choose to enable the Single VLAN Tag option in the iSSL solution, you should also enable the Single VLAN Tag configuration in the flex map deployed in that solution. NOTE: If you enable the Single VLAN tag option in the Flexible Inline SSL solution, you should also enable the Single VLAN Tag configuration in the inline-ssl app profile deployed in the solution
Tool Side VLAN Tag	Enter the required tool side VLAN tag for the inline network.
TPID	Select the TPID for the Tool Side VLAN Tag. The default value of TPID is 0x8100. You can select the other supported values 0x9100 and 0x88a8 from the drop-down list.
Traffic Path	Select one of the following options: - Drop—Traffic is dropped at the virtual port. - Bypass—Traffic bypasses the virtual port. - Monitoring—Traffic is fed to the virtual port and absorbed, while a copy of the traffic is sent to the next inline tool in the sequence. Traffic returned from side B of the network is also absorbed at the virtual port in the monitoring mode. NOTE: You can select the Monitoring option only if you have set the SSL Monitor Mode to either Enable or Inline. - To Inline Tool—Traffic is forwarded to the inline tool. This is the default value.
Inline Failover Action	Select one of the following options: - Virtual port bypass—All virtual ports configured as the source of any map that triggered this failover action, will be put in the bypass mode, that is all traffic will bypass the virtual port and will be guided to the inline tool or inline tool group. - Virtual port drop—All virtual ports configured as the source of any map that triggered this failover action, will be put in the drop mode, that is all traffic will be

Field	Description
	dropped at the virtual port. • Network bypass—All inline networks configured as the source of any map involving the inline tool or inline tool group that triggered this failover action, will be put in the bypass mode, that is, all traffic coming to side A will be directed to side B and vice versa. • Network drop—All inline networks configured as the source of any map involving the inline tool or inline tool group that triggered this failover action, will be put in the drop mode, that is, all traffic coming to side A or side B will be dropped. • Network port forced down—For all inline networks configured as the source of any map involving the inline tool or inline tool group that triggered this failover action, the inline network ports will be brought down.
Security Exceptions	You can choose to either decrypt or drop the traffic for the following certificates: • Self-signed certificate • Unknown CA certificate • Invalid certificate • Expired certificate • You can also choose to configure the security exceptions for certificate revocation validation based on OCSP or CRL on an inline decryption profile. Select one of the following options: ◦ Soft Fail—If you select this option, the client browser displays the secondary MitM certificate and the inline decryption session stats in GigaVUE-FM displays as Decrypt. ◦ Hard Fail—If you select this option, the client browser displays the certificate from DigiCert and the inline decryption session stats in GigaVUE-FM displays as Bypass: Unknown Revocation.
No-decrypt list/Decrypt list	Select the following check boxes: • No-decrypt list—Allows traffic from certain classes such as sites, domains, host-based IP address and IP subnets (decision based on LPM) to bypass decryption. • Decrypt list—Allows traffic from certain sites, domains, host-based IP address and IP subnets (decision based on LPM) to always be decrypted. Select from the below operations that can be performed on an uploaded list: • Append _ This would add to the uploaded list. • Replace- This would remove the previously added list and add a new list. This option is supported only on Generation 3 cards. • Clear- This would completely clear the list. • Download - This would download the list that has been uploaded. If you select Append/Replace, you can enter the list using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
Policy Rules	Add the required policy rules for the inline decryption profile. Click Add a Rule. In the Condition field, Select one of the following options from the drop-down list:

Field	Description
	• Category • Domain • IPv4 Destination • IPv4 Source • IPv6 Destination • IPv6 Source • L4 Port Destination • L4 Port Source • VLAN • X509 Certificate Issuer Name Select one of the following options: • Decrypt—Decrypt all the traffic that is guided into the Inline SSL APP. • Decrypt—Do not decrypt the traffic that is guided into the Inline SSL APP.
Network Access	Network access configuration is used to get URL categorization updates To configure the network access for the GigaSMART engine ports: - o Select either DHCP or IP Address as the network access configuration mode. - o If you select IP Address as the mode, enter the IP Address, Netmask, Gateway, DNS, MTU, and VLAN. ▪ DNS or Split DNS- Configure either a default single DNS server or a Split DNS Server. If you want to attach Split DNS server profile to your Inline SSL deployment choose a Split DNS server from the drop-down. To configure a new Split DNS Profile, click on Create new Split DNS. - o Select either Eth2 or Eth3 as the Interface. - o If you want to attach a Proxy profile to your Inline SSL deployment select a Proxy Server Profile from the drop-down. To configure a new Proxy Server Profile, click on Create new Proxy.  Notes: • The Eth3 option is available only for GigaVUE-HC3 devices. • IP Address configuration mode details should be entered when you select Luna HSM configuration from the HSM Group drop down. • If your Proxy Server profile is associated with an Inline SSL application, choose 'None' in the Proxy Server profile field on the Inline SSL configuration page to disconnect the proxy server profile prior to deleting the profile. • You cannot enable Gen 2 and Gen 3 GigaSMART engine for network access simultaneously.
Decryption Port Mapping	The TCP destination port for decrypted traffic sent to inline tools can be configured as part of the inline decryption profile. Configure the required Priority 1 map, which is user configurable and Priority 2 map, which is the default out port.
Trust Store	Server Trust Store: The trust store contains a trusted certificate authority (CA) for server validation. You can choose to either append or replace the trust store. Client Trust store The trust store contains a trusted certificate authority (CA) for client validation

Field	Description
	when mTLS is enabled for this profile. You can choose to either append or replace the trust store. NOTE: The Client trust store is used only for inbound and hybrid mTLS sessions. If you later disable mTLS and redeploy the device for outbound only Inline TLS/SSL decryption, then it will remove all client trust store and signing certificate configurations that are attached to this profile.
TCP Settings	Configure the required TCP settings as follows: • TCP Inactive Timeout— TCP Inactive session timeout in minutes. • TCP Delayed ACK—GigaSMART Inline TLS/SSL decryption ACKs every TCP packet by default. If TCP Delayed ACK is enabled, then GigaSMART decryption will wait for 100ms or ACK every third packet – whichever comes first. • TCP SYN Retries—number of retries made by the MitM to initiate a session with the destination server. If a SYN/ACK response isn't received from the destination server on initial TCP SYN, GigaSMART attempts for additional number of TCP SYN Retries as defined by the user. • TCP TIMEWAIT Timeout— Configure the 'TCP TIMEWAIT' timeout value from 0-300 seconds. The default value is 30 seconds. The TCP connection in the TIME_WAIT state gets deleted after the timeout period.
Split-Proxy Settings	
Split-Proxy	Select the check box to enable the split proxy settings for the inline decryption solution. The TLS connection between the server and client is divided into two independent connections, and the security parameters are kept separate.
Non-PFS Ciphers (Server)	Select the check box to enable the non-PFS ciphers settings for the inline decryption solution that has the split proxy settings enabled. This setting is to indirectly force the server to use protocols that are lower than TLS 1.3 with non-PFS ciphers. This means that the ciphers with DHE/ECDHE key-exchange will not be used on the server side.
Miscellaneous (Global Settings)	
SSL/TLS Version	Select the minimum and maximum SSL/TLS version.
Connection Reset Action	Select one of the following options for the minimum SSL/TLS version: • Drop—Closes all sessions that are below the minimum SSL/TLS version specified. This ensures that the network is safe from weak TLS/SSL connections. This is the default option. • No Decrypt—Bypasses all sessions that are below the minimum SSL/TLS version specified. Select one of the following options for the maximum SSL/TLS version: - o No Decrypt—Bypasses all sessions that are above the maximum SSL/TLS version specified. This is the default option. - o Drop—Closes all sessions that are above the maximum SSL/TLS version specified.
Caching persistence	Select this check box to allow the information to be saved on the node in the control card's persistent storage so that it can be retrieved in case of reboots.
DHE Cipher Suites	Enable this use DHE Cipher suites.

Configure Inline TLS/SSL Decryption Solution with Layer 2 Tools

This section describes how to configure and deploy an Inline TLS/SSL Decryption solution using Layer 2 tools.

Prerequisites

- A configured and reachable GigaSMART engine on the selected device to host the Inline SSL app.
- Configure and unlock the Keychain Password in GigaVUE-FM to access the keystore; optionally enable Auto Login for unattended restarts.
- Prepare required keys and certificates for your deployment direction:
 - Inbound: server private key(s) and corresponding certificate(s).
 - Outbound/Hybrid: appropriate CA/certificate chain for re-signing or policy-based decryption.
- Keep key types and file formats (PEM/PKCS12/Luna-HSM) and any passphrases ready.
- Decide the deployment type you will use (Inbound, Outbound, or Hybrid) so the Inline SSL app can be configured accordingly.
- Plan the software constructs you will create during configuration: at minimum, an Inline Network and an Inline Tool to connect your Layer 2 (transparent) inspection device(s). Ensure the required ports are identified and available.
- Ensure your connected tools can operate in Layer 2 transparent mode (inspect decrypted traffic without altering packet contents)

Access Flexible Inline Canvas

1. Go to  > **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the TLS/SSL decryption.

Configure Inline Network

1. On the left pane, click the '+' icon next to **Inline Network** option to create a new entry.

2. Enter a name and description for the inline network in the **Alias** and **Description** fields. Then, click **Port Editor**.
3. In the **Alias** and **Description** fields, enter a name and description for the inline network.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline network ports that you want to configure. Select **Enable** to administratively enable inline network ports, and click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the ports that you want to configure as the inline network pair.
6. From the **Traffic Path** drop-down list, select **To Inline Tool**.
 - **To Inline Tool**—All traffic originating from the inline network is directed to the sequence of inline tools and inline tool groups and is guided through the inline tools and inline tool groups according to the current inline tool and inline tool group status.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Network Ports and Inline Network](#).

NOTE: If there are multiple Inline Network Ports, you can configure Inline Network bundle. Refer to [Configure Inline Network Bundle](#).

Configure Inline Tool

1. On the left pane, click the '+' icon next to the **Inline Tool** option to create a new inline tool.
2. In the **Properties** pane, in the **Alias** and **Description** fields, enter a name and description for the inline tool.
3. From the **Type** drop-down list, select one of the following options:
 - **External**- To configure a third-party tool.
 - **GigaVUE Node**- To configure a GigaVUE node as a tool.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline tool ports that you want to configure. Select **Enable** to administratively enable the inline tool ports, and then click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the inline tool ports according to the direction the inline tool expects traffic from the network.
6. Verify that the **Enabled** check box is selected.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Tool Ports and Inline Tools](#).

Create an Inline SSL APP

1. On the left pane, click the '+' icon next to the **Inline SSL APP** option.
2. Enter a name for the Inline SSL APP and select the required GigaSMART engines.
3. In the **Alias** field, enter a name for the Inline SSL APP.
4. From the **GigaSMART Engine** drop-down list, select the required engine.
5. Under **Deployment Type**, set up **Key chain Password**:
 - a. Click **Keychain Password**, and choose either Add or Reset.
 - b. If you choose to reset the Keychain Password, enter a password that is 8 to 30 characters long and contains at least one numerical character, one uppercase character, one lowercase character, and one special character.
 - c. Select the **Auto Login** check box to enable GigaVUE-FM to unlock the keystore when the device reboots.
 - d. Click **OK** to save the Key chain Password.
6. Configure **Keys and Certificates**. A key in an inbound deployment can be selected only for decryption or for re-signing and re-encryption in an outbound deployment.
 - a. Click **Add Keys** to open the Key page.
 - b. Enter a name and description for the key.
 - c. Select the required **Key Type** and **File Type**.
 - d. If using PEM or PKCS12 as file type, optionally include a passphrase.
 - e. You can choose to include a Passphrase for the key when you select PEM or PKCS12 as file type if required.
 - f. When you choose Luna-HSM, enter the Key label for the key.
 - g. Add the required **Private Key** and **Certificate**.
 - h. Click **OK** to save the configuration.
7. Select the required deployment type.
 - o **Outbound** - Add the configured primary and a secondary signing Certificate Authorities (CA).
 - o **Inbound** - Add a new Server Key Mapping. Enter the domain name or IP address of the server, and select the required Key Pair Alias.
 - o **Hybrid** - Add a new Server Key Mapping, and a primary and a secondary signing CA.
8. Click **OK** to save the configuration.

Deploy Inline TLS/SSL Decryption Solution

In the Flexible Inline Canvas:

1. Drag and drop the required inline network or inline network bundle.
2. Drag and drop the flexible inline map into the canvas. The **Properties** pane opens automatically. If configuration is needed, provide values for the following fields:
 - In the **Alias** and **Description** fields, enter the name and description of the inline map.
 - Enter the **Tool Side VLAN Tag** for the inline network for which you are configuring the map.
 - Select the **TPID** for the Tool Side VLAN Tag. The default value of TPID is 0x8100. You can select the other supported values 0x9100 and 0x88a8 from the drop-down list.
 - Add the required rules for the inline map, and click **OK** to save the configuration.
3. Drag and drop the Inline SSL APP.
4. Drag and drop the required inline tools or inline tool group.
5. Drag and drop the **OOB Copy**, if required.
6. Click **Deploy**, and choose the Traffic Path—either **Logical Bypass** or **Keep as is**. Select the option that best suits your deployment needs, and click **OK**.

Verify the Solution

In GigaVUE-FM, open the Flexible Inline Canvas: **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas**, select the target device, and open the deployed solution on the canvas. Confirm the solution shows as deployed.

What to Do Next

After deployment, you can view the Monitor and Session statistics. Refer to [View Inline TLS/SSL Session Statistics on Statistics](#). You can also view the Inline TLS/SSL Dashboards. Refer to [View Inline TLS/SSL Dashboards](#).

Configure Inline TLS/SSL Decryption Solution with Layer 3 Tools

This section describes how to configure and deploy an Inline TLS/SSL Decryption solution using Layer 3 tools.

Prerequisites

- A configured and reachable GigaSMART engine on the selected device to host the Inline SSL app.
- Configure and unlock the Keychain Password in GigaVUE-FM to access the keystore (optionally enable Auto Login for unattended restarts).
- Prepare required keys and certificates for your selected deployment type: inbound (server private keys/certs), outbound (CA/resigning chain), or hybrid. Ensure supported file types (PEM/PKCS12/Luna-HSM) and passphrases are available.
- Decide the deployment type (Inbound, Outbound, or Hybrid) so the Inline SSL app can be configured accordingly.
- Plan the software constructs you will create: at minimum an Inline Network (and, where applicable, an Inline Network Bundle) plus an Inline Tool path for the Layer 3 security device(s); ensure the necessary ports are identified and available.
- Define routing/policy selection for Layer 3: identify the subnet-based IP ranges at the Inline SSL profile level that will be steered through the L3 tool path.
- Plan to enable NAT/PAT in the Inline SSL app when offloading TLS decryption from Layer 3 inline tools (Policy Profile > NAT/PAT).

Access Flexible Inline Canvas

1. Go to  > **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the TLS/SSL decryption.

Configure Inline Network

1. On the left pane, click the '+' icon next to **Inline Network** option to create a new entry.

2. Enter a name and description for the inline network in the **Alias** and **Description** fields. Then, click **Port Editor**.
3. In the **Alias** and **Description** fields, enter a name and description for the inline network.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline network ports that you want to configure. Select **Enable** to administratively enable inline network ports, and click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the ports that you want to configure as the inline network pair.
6. From the **Traffic Path** drop-down list, select **To Inline Tool**.
 - **To Inline Tool**—All traffic originating from the inline network is directed to the sequence of inline tools and inline tool groups and is guided through the inline tools and inline tool groups according to the current inline tool and inline tool group status.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Network Ports and Inline Network](#).

Repeat steps 1 through 7 to create the required number of Inline Networks and group them into an Inline Network Bundle.

Configure Inline Network Bundle

1. On the left pane, click the '+' icon next to **Inline Network Bundle** option to create a new entry.
2. Enter a name and description for the inline network bundle in the **Alias** and **Description** fields.
3. From the **Inline Networks** drop-down list, select the inline networks you want to include in the bundle.
4. Click **OK** to save the bundle configuration.

Configure Inline Tool

1. On the left pane, click the '+' icon next to the **Inline Tool** option to create a new inline tool.
2. In the **Properties** pane, in the **Alias** and **Description** fields, enter a name and description for the inline tool.
3. From the **Type** drop-down list, select one of the following options:
 - **External**- To configure a third-party tool.
 - **GigaVUE Node**- To configure a GigaVUE node as a tool.

4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline tool ports that you want to configure. Select **Enable** to administratively enable the inline tool ports, and then click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the inline tool ports according to the direction the inline tool expects traffic from the network.
6. Verify that the **Enabled** check box is selected.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Tool Ports and Inline Tools](#).

Create an Inline SSL APP

1. On the left pane, click the '+' icon next to the **Inline SSL APP** option.
2. Enter a name for the Inline SSL APP and select the required GigaSMART engines.
3. In the **Alias** field, enter a name for the Inline SSL APP.
4. From the **GigaSMART Engine** drop-down list, select the required engine.
5. Under **Deployment Type**, set up **Key chain Password**:
 - a. Click **Keychain Password**, and choose either Add or Reset.
 - b. If you choose to reset the Keychain Password, enter a password that is 8 to 30 characters long and contains at least one numerical character, one uppercase character, one lowercase character, and one special character.
 - c. Select the **Auto Login** check box to enable GigaVUE-FM to unlock the keystore when the device reboots.
 - d. Click **OK** to save the Key chain Password.
6. Configure **Keys and Certificates**. A key in an inbound deployment can be selected only for decryption or for re-signing and re-encryption in an outbound deployment.
 - a. Click **Add Keys** to open the Key page.
 - b. Enter a name and description for the key.
 - c. Select the required **Key Type** and **File Type**.
 - d. If using PEM or PKCS12 as file type, optionally include a passphrase.
 - e. You can choose to include a Passphrase for the key when you select PEM or PKCS12 as file type if required.
 - f. Add the required **Private Key** and **Certificate**.
 - g. Click **OK** to save the configuration.
7. Select the required deployment type.

- **Outbound** - Add the configured primary and a secondary signing Certificate Authorities (CA).
 - **Inbound** - Add a new Server Key Mapping. Enter the domain name or IP address of the server, and select the required Key Pair Alias.
 - **Hybrid** - Add a new Server Key Mapping, and a primary and a secondary signing CA.
8. Under **Advanced > Configurations**, enable NAT/PAT (Network Address Translation/Port Address Translation) on traffic passing through Layer 3 inline tools to offload TLS decryption. Select the NAT-PAT checkbox to apply this setting.
 9. Click **OK** to save the configuration. Refer to [Inline SSL App—Field References](#) for any additional details when configuring the Inline SSL APP.

Deploy Inline TLS/SSL Decryption Solution

In the Flexible Inline Canvas:

1. Drag and drop the required inline network bundle.
2. Drag and drop the flexible inline map into the canvas. The **Properties** pane opens automatically. If configuration is needed, provide values for the following fields:
 - In the **Alias** and **Description** fields, enter the name and description of the inline map.
 - Enter the **Tool Side VLAN Tag** for the inline network for which you are configuring the map.
 - Select the **TPID** for the Tool Side VLAN Tag. The default value of TPID is 0x8100. You can select the other supported values 0x9100 and 0x88a8 from the drop-down list.
 - Add the required rules for the inline map, and click **OK** to save the configuration.
3. Drag and drop the Inline SSL APP.
4. Drag and drop the required inline tools or inline tool group.
5. Drag and drop the **OOB Copy**, if required.
6. Click **Deploy**, and choose the Traffic Path—either **Logical Bypass** or **Keep as is**. Select the option that best suits your deployment needs, and click **OK**.

Verify the Solution

In GigaVUE-FM, open the Flexible Inline Canvas: **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas**, select the target device, and open the deployed solution on the canvas. Confirm the solution shows as deployed.

What to Do Next

After deployment, you can view the Monitor and Session statistics. Refer to [View Inline TLS/SSL Session Statistics](#). You can also view the Inline TLS/SSL Dashboards. Refer to [View Inline TLS/SSL Dashboards](#).

Configure Inbound mTLS for Inline TLS/SSL Decryption

This section describes how to enable client certificate authentication (mTLS) for inbound Inline TLS/SSL decryption deployments using Flexible Inline arrangements

Prerequisites

- Ensure that servers are configured to request or require client certificates for the relevant services.
- Ensure you have access to the CA certificates used to issue client certificates (to populate the client trust store).

Create a Client Trust store

1. On the left navigation pane, go to **Inventory**  > **Physical Node>Nodes>Settings>Trust Store> Client Trust Store**
2. Create a new Client Trust Store:
 - Specify a unique alias for the client trust store.
 - Upload the CA certificates that issue client certificates for your environment.
3. Click on Apply to save the Client Authentication and it appears in the Client Trust store list.

Access Flexible Inline Canvas

1. Go to  > **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the TLS/SSL decryption.

Create an Inline SSL APP

1. On the left pane, click the '+' icon next to the **Inline SSL APP** option.

2. Enter a name for the Inline SSL APP and select the required GigaSMART engines.
3. In the **Alias** field, enter a name for the Inline SSL APP.
4. From the **GigaSMART Engine** drop-down list, select the required engine.
5. Under **Deployment Type**, set up **Key chain Password**:
 - a. Click **Keychain Password**, and choose either Add or Reset.
 - b. If you choose to reset the Keychain Password, enter a password that is 8 to 30 characters long and contains at least one numerical character, one uppercase character, one lowercase character, and one special character.
 - c. Select the **Auto Login** check box to enable GigaVUE-FM to unlock the keystore when the device reboots.
 - d. Click **OK** to save the Key chain Password.
6. Configure **Keys and Certificates**. A key in an inbound deployment can be selected only for decryption or for re-signing and re-encryption in an outbound deployment.
 - a. Click **Add Keys** to open the Key page.
 - b. Enter a name and description for the key.
 - c. Select the required **Key Type** and **File Type**.
 - d. If using PEM or PKCS12 as file type, optionally include a passphrase.
 - e. You can choose to include a Passphrase for the key when you select PEM or PKCS12 as file type if required.
 - f. When you choose Luna-HSM, enter the Key label for the key.
 - g. Add the required **Private Key** and **Certificate**.
 - h. Click **OK** to save the configuration.
7. Select the required deployment type.
 - **Inbound** - Add a new Server Key Mapping. Enter the domain name or IP address of the server, and select the required Key Pair Alias.
8. Enable the **mTLS** toggle.
9. Under Client Trust store. Select the **Client Trust Store** or create a new one by clicking on the **Add Trust Store** button. You can configure to allow or drop sessions when:
 - The client certificate is expired.
 - The certificate chain is self-signed.
 - The certificate chain is signed by an unknown CA.
10. Click **OK** to save the configuration.

Deploy the solution

In the Flexible Inline Canvas:

1. Drag and drop the required inline network or inline network bundle.
2. Drag and drop the flexible inline map into the canvas. The **Properties** pane opens automatically. If configuration is needed, provide values for the following fields:
 - In the **Alias** and **Description** fields, enter the name and description of the inline map.
 - Enter the **Tool Side VLAN Tag** for the inline network for which you are configuring the map.
 - Select the **TPID** for the Tool Side VLAN Tag. The default value of TPID is 0x8100. You can select the other supported values 0x9100 and 0x88a8 from the drop-down list.
 - Add the required rules for the inline map, and click **OK** to save the configuration.
3. Drag and drop the Inline SSL APP.
4. Drag and drop the required inline tools or inline tool group.
5. Drag and drop the **OOB Copy**, if required.
6. Click **Deploy**.

Verify the Solution

In GigaVUE-FM, open the Flexible Inline Canvas: **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas**, select the target device, and open the deployed solution on the canvas. Confirm the solution shows as deployed.

What to Do Next

After deployment, at the Monitor and Session statistics you can view if :

- the mTLS sessions are counted as decrypted inbound sessions
- Client certificate-related counters show successful validation events.

Refer to [View Inline Solution Status and Statistics](#). You can also view the Inline TLS/SSL Dashboards. Refer to [View Inline TLS/SSL Dashboards](#).

NOTE: If you later remove this inbound mTLS solution and deploy an outbound Inline SSL solution on the same device, first delete all client trust-store entries created for mTLS and any client key-store entries used for mTLS client authentication, and then deploy the new outbound Inline SSL application.

Configure Inline TLS/SSL Decryption Solution with RIA

This section describes how to configure and deploy Resilient Inline TLS/SSL.

Prerequisites

- Resilient Configuration requires two nodes . Ensure you have configured both devices with the required software constructs.
- Use inline-capable ports and, where applicable, inline bypass modules for fail-open behavior on power or device failure.
- Cable two inline nodes in path (client–device–server) with identical inline tool connectivity on each.
- Build an Inter-broker Pathway (IB-P) using at least one—preferably two or more aggregated—tool ports between nodes, and set a minimum-up count for IB-P status “Up.”
- For Inbound iSSL, prepare server private keys/certificates (RSA/ECDSA) with key pair aliases, define actions for unknown/invalid/self-signed certs, and set TLS policy (for example, decrypt TLS 1.2/1.3 and drop TLS 1.0/1.1).
- Ensure inline tools on both nodes are identical in count, type, speed, and capacity for consistent distribution and service behavior.
- Use only one RIA-enabled iSSL app per two-node pair.

Access Flexible Inline Canvas

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the TLS/SSL decryption.

You should proceed to configure the following software constructs for both nodes before you deploy your solution.

Configure Inline Network

1. On the left pane, click the ‘+’ icon next to **Inline Network** option to create a new entry.
2. Enter a name and description for the inline network in the **Alias** and **Description** fields. Then, click **Port Editor**.

3. In the **Alias** and **Description** fields, enter a name and description for the inline network.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline network ports that you want to configure. Select **Enable** to administratively enable inline network ports, and click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the ports that you want to configure as the inline network pair.
6. From the **Traffic Path** drop-down list, select **To Inline Tool**.
 - o **To Inline Tool**—All traffic originating from the inline network is directed to the sequence of inline tools and inline tool groups and is guided through the inline tools and inline tool groups according to the current inline tool and inline tool group status.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Network Ports and Inline Network](#).

NOTE: If there are multiple Inline Network Ports, you can configure Inline Network bundle. Refer to [Configure Inline Network Bundle](#).

Configure Inline Tool

1. On the left pane, click the '+' icon next to the **Inline Tool** option to create a new inline tool.
2. In the **Properties** pane, in the **Alias** and **Description** fields, enter a name and description for the inline tool.
3. From the **Type** drop-down list, select one of the following options:
 - o **External**- To configure a third-party tool.
 - o **GigaVUE Node**- To configure a GigaVUE node as a tool.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline tool ports that you want to configure. Select **Enable** to administratively enable the inline tool ports, and then click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the inline tool ports according to the direction the inline tool expects traffic from the network.
6. Verify that the **Enabled** check box is selected.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Tool Ports and Inline Tools](#).

Create Inter-broker Pathway

The inter-broker pathway (IBP) links the two RIA nodes so flows that hash to one node can traverse to the peer when needed, ensuring symmetric inspection and continuous traffic forwarding across nodes even during asymmetric paths or node/tool events.

To create a new inter-broker pathway:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed canvas, select the device where you want to create the inter-broker pathway.
3. Click the '+' icon next to the **IB Pathway** option to create a new inter-broker pathway.
4. In the **Properties** pane, enter a name and description in the **Alias** and **Description** fields..
5. From the **Ports** drop-down list, select the required tool ports to attach to the inter-broker pathway.

NOTE: If the required tool ports are not available, you can enable them administratively. Click **Port Editor**, scroll to the tool ports you want to configure in the **Quick Port Editor** page, select **Enable**, and click **OK**.

6. In the **Minimum Ports Up** field, enter the minimum number of tool ports that must be operational for the inter-broker pathway status to be "Up".
7. From the **Traffic Path** drop-down list, select one of the following options:
 - **Bypass**—Traffic bypasses the inter-broker pathway and is redirected to the next inline network port.
 - **Monitoring**—Traffic is forwarded to the sequence of inline tools in the monitoring mode.
 - **To Inline Tool**—Traffic is forwarded to the sequence of inline tools you have configured.
8. Click **OK** to save the configuration.

Configure Resilient Inline Arrangement

To configure a resilient inline arrangement:

1. Drag and drop the required inline network or inline network LAG into the flexible inline canvas, and click **Settings**.

2. In the **Settings** pane, select the **Enable** check box next to **Show Single Tag Options** to configure the resilient inline arrangement with a single VLAN tag.

NOTE: Enable **Show Single Tag Options** only if your inline tools do not support Q-in-Q VLAN tags.

3. Select the **Enable** check box next to **Show Resilient Inline Menu**.
4. Select the required **Node 1**, **Node 2**, **IB Pathway1**, and **IB Pathway2** for the resilient inline arrangement.
5. From the **Hashing Source** drop-down list, select one of the following options:
 - **Side A** - Hashing uses source IP or source port from Side A; destination IP or destination port from Side B.
 - **Side B** - Hashing uses source IP or source port from Side B; destination IP or destination port from Side A.
6. From the **Hashing Type** drop-down list, select one of the following options:
 - **L3 (IP Based)** - Hashing uses the IP address.
 - **L4 (Port Based)** - Hashing uses the transport layer port number.
7. From the **Hashing LSB Node** drop-down list, select one of the following options:
 - **Node 1 as 0** - Traffic from IPs ending in 0 is hashed to Node 2.
 - **Node 2 as 0** - Traffic from IPs ending in 0 is hashed to Node 1.

NOTE: This option is available only if you selected **L3 (IP Based)** in the Hashing Type field.

8. From the **Hashing Port** drop-down list, select one of the following options:
 - **Node 1 as odd** - Traffic with odd port numbers is hashed to Node 2, while traffic with even port numbers is hashed to Node 1.
 - **Node 2 as odd** - Traffic with odd port numbers is hashed to Node 1, while traffic with even port numbers is hashed to Node 2.

NOTE: This field is available only if you select the **L4 (Port Based)** option in the **Hashing Type** field.

9. Click **OK** to save the settings.
10. Drag and drop the flexible inline map into the canvas. Click the map to open the Properties pane.
11. In the **Alias** and **Description** fields, enter the name and description of the inline map.
12. To deploy the resilient inline arrangement with a **single VLAN tag**, select the **Enable** check box next to Single Tag Mode. Refer to [Configure Inline TLS/SSL Decryption Solution with RIA](#).

NOTE: You can choose to disable the **Single Tag Mode** for collector maps, if required.

13. Enter the **Tool Side VLAN Tag** for the inline network you are configuring.
 14. Select the **TPID** for the Tool Side VLAN Tag. The default value is 0x8100. You can also choose from the supported values 0x9100 and 0x88a8 in the drop-down list.
 15. From the **FlexInline Failover** drop-down list, select one of the following options:
 - **Bypass** - Traffic passes directly between the respective inline network ports.
 - **Original Map** - Traffic follows the path defined in this Flexible Inline Map.
 16. Add the required rules for the inline map. Click **OK** to save the configuration.
 17. Drag and drop the required **Inline Tools** or **Inline Tool Group** into the canvas.
 18. If needed, drag and drop the **OOB Copy** into the canvas.
 19. From the **Destination Ports** drop-down list, select the required hybrid or tool ports.
 20. From the **VLAN Tag** drop-down list, select one of the following options:
 - **None** - No VLAN tag is used; traffic is routed to a different destination.
 - **Original** - Uses the original VLAN tag from the packet received from the inline network.
 - **As Inline** - Uses the VLAN tag configured for the Flexible Inline Map.
- NOTE:** The **As Inline** option is available only when you configure the Resilient Inline Arrangement with a single VLAN tag.
21. Click **Deploy**, select a traffic path and click **OK**.

Create an Inline SSL APP

1. On the left pane, click the '+' icon next to the **Inline SSL APP** option.
2. Enter a name for the Inline SSL APP.
3. Enable Resilient Inline Arrangements check box.
4. Select the nodes that would be configured and their respective GigaSMART modules.
5. Select the required GigaSMART engines.
6. Under Deployment Type, set up Key chain Password:
 - a. Click **Keychain Password**, and then choose either Add or Reset.
 - b. If you choose to reset the Keychain Password, enter a password that is 8 to 30 characters long and contains at least one numerical character, one uppercase character, one lowercase character, and one special character.

- c. Select the **Auto Login** check box to enable GigaVUE-FM to unlock the keystore when the device reboots.
 - d. Click **OK** to save the Key chain Password.
7. Configure **Keys and Certificates**. A key in an inbound deployment can be selected only for decryption or for re-signing and re-encryption in an outbound deployment.
 - a. Click **Add new keys** to open the Key page.
 - b. Enter a name and description for the key.
 - c. Select the required **Key Type** and **File Type**.
 - d. If using PEM or PKCS12 as file type, optionally include a passphrase.
 - e. You can choose to include a Passphrase for the key when you select PEM or PKCS12 as file type if required.
 - f. When you choose Luna-HSM, enter the Key label for the key.
 - g. Add the required **Private Key** and **Certificate**.
 - h. Click **OK** to save the configuration.
8. Select the required deployment type.
 - o **Outbound** - Add the configured primary and a secondary signing Certificate Authorities (CA).
 - o **Inbound** - Add a new Server Key Mapping. Enter the domain name or IP address of the server, and select the required Key Pair Alias.
 - o **Hybrid** - Add a new Server Key Mapping, and a primary and a secondary signing CA.
9. The platform pushes the added keys to both nodes. To delete a key, delete it from each node individually.
10. Click **OK** to save the Inline SSL App configuration. You can configure Inline SSL App for any one of the nodes. It will be available for the second node as well.

Deploy Inline TLS/SSL Decryption Solution

In the Flexible Inline Canvas:

1. Drag and drop the required inline network or inline network bundle.
2. Drag and drop the flexible inline map into the canvas. Use the Flex Map, Inline Tools, and Inline SSL App—available on both nodes with the same alias—to configure the Flex Inline TLS/SSL maps.
3. Under the Settings option, enable the '**Show Resilient Inline Menu**' check-box and setup the Node, IB Pathway, and Hashing configurations.
4. Click **Deploy**.

Verify the Solution

- In GigaVUE-FM, open the Flexible Inline Canvas: **Physical > Orchestrated Flows > Inline Flows > Configuration Canvas**, select the target device, and open the deployed solution on the canvas. Confirm the solution shows as deployed for both nodes.
- Ensure Resilient Inline settings (node selection, hashing/IP parity) are correct and the Inter-broker Pathway (IBP) state is Up.
- Check that traffic and sessions appear on both nodes, with asymmetric flows traversing the IBP as designed.
- If Single VLAN Tag (SVT) is used, confirm it's enabled and tool-side VLANs match your policy.

What to Do Next

After deployment, you can view the Monitor and Session statistics. Refer to [View Inline TLS/SSL Session Statistics Statistics](#). You can also view the Inline TLS/SSL Dashboards. Refer to [View Inline TLS/SSL Dashboards](#).

Configure Thales-Luna HSM for TLS/SSL Decryption

This section describes the configuration and use of Thales-Luna HSM for TLS/SSL decryption.

Prerequisites

- From the Thales Luna HSM administrator:
 - HSM server IP address and port, and a valid partition label and partition password for the Luna partition you will use.
 - The private keys' key labels in the Luna partition (for example, for primary and secondary signing). With Luna, the private key remains in the HSM; you reference it by its unique label/handle during configuration.
 - The corresponding server certificate(s) for those key labels, and any required CA certificate(s) for trust.
- A Keychain password must be configured on the device before installing certificates and keys in the keystore.
- A static IP address to assign to the GigaSMART engine for HSM communication; static IP is recommended. When Luna HSM is selected, IP address configuration details must be entered for the Inline SSL application.

Access Flexible Inline Canvas

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the TLS/SSL decryption.

Configure Inline Network

1. On the left pane, click the '+' icon next to **Inline Network** option to create a new entry.
2. Enter a name and description for the inline network in the **Alias** and **Description** fields. Then, click **Port Editor**.
3. In the **Alias** and **Description** fields, enter a name and description for the inline network.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline network ports that you want to configure. Select **Enable** to administratively enable inline network ports, and click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the ports that you want to configure as the inline network pair.
6. From the **Traffic Path** drop-down list, select **To Inline Tool**.
 - o **To Inline Tool**—All traffic originating from the inline network is directed to the sequence of inline tools and inline tool groups and is guided through the inline tools and inline tool groups according to the current inline tool and inline tool group status.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Network Ports and Inline Network](#).

Configure Inline Tool

1. On the left pane, click the '+' icon next to the **Inline Tool** option to create a new inline tool.
2. In the **Properties** pane, in the **Alias** and **Description** fields, enter a name and description for the inline tool.
3. From the **Type** drop-down list, select one of the following options:
 - o **External**- To configure a third-party tool.
 - o **GigaVUE Node**- To configure a GigaVUE node as a tool.

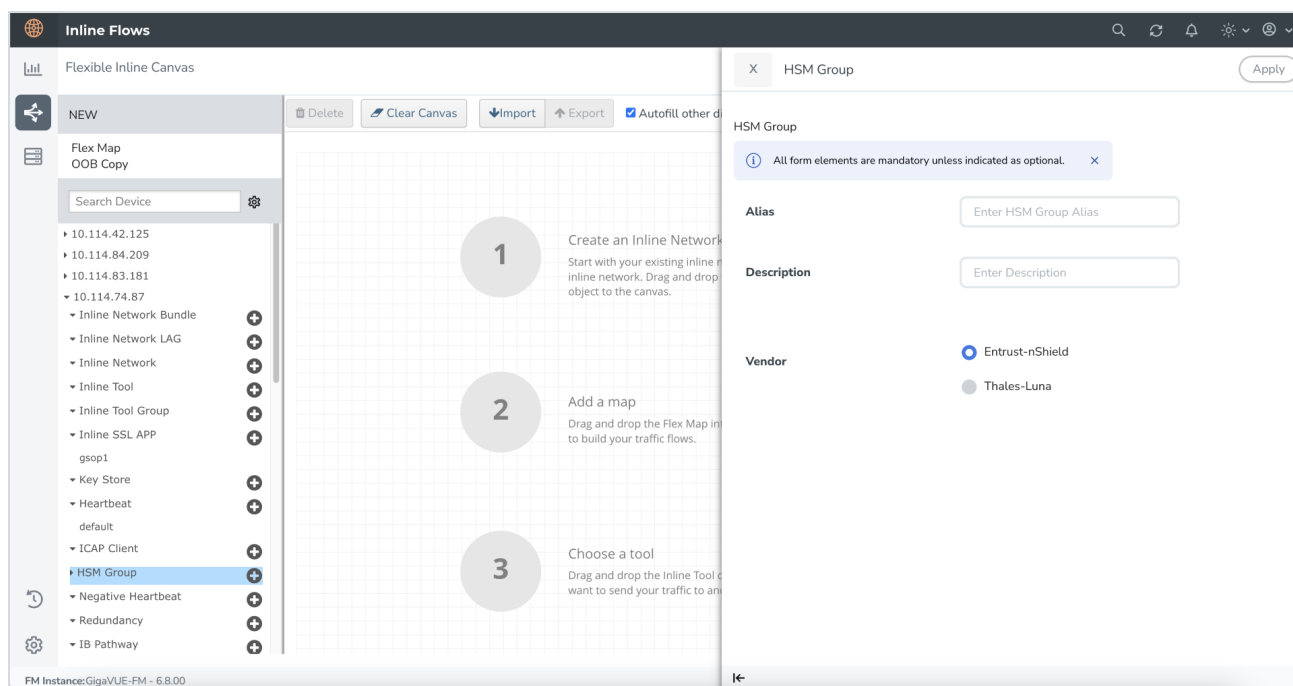
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline tool ports that you want to configure. Select **Enable** to administratively enable the inline tool ports, and then click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the inline tool ports according to the direction the inline tool expects traffic from the network.
6. Verify that the **Enabled** check box is selected.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Tool Ports and Inline Tools](#).

Create HSM Group

To configure HSM Group:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the HSM Group.
3. Click the '+' icon next to the **HSM Group** to create a new entry.
4. Enter a name and description for the **HSM Group** in the **Alias** and **Description** fields.



5. Select the required vendor type from the available options —**Entrust-nShield** or **Thales-Luna**—to create the corresponding HSM Group.

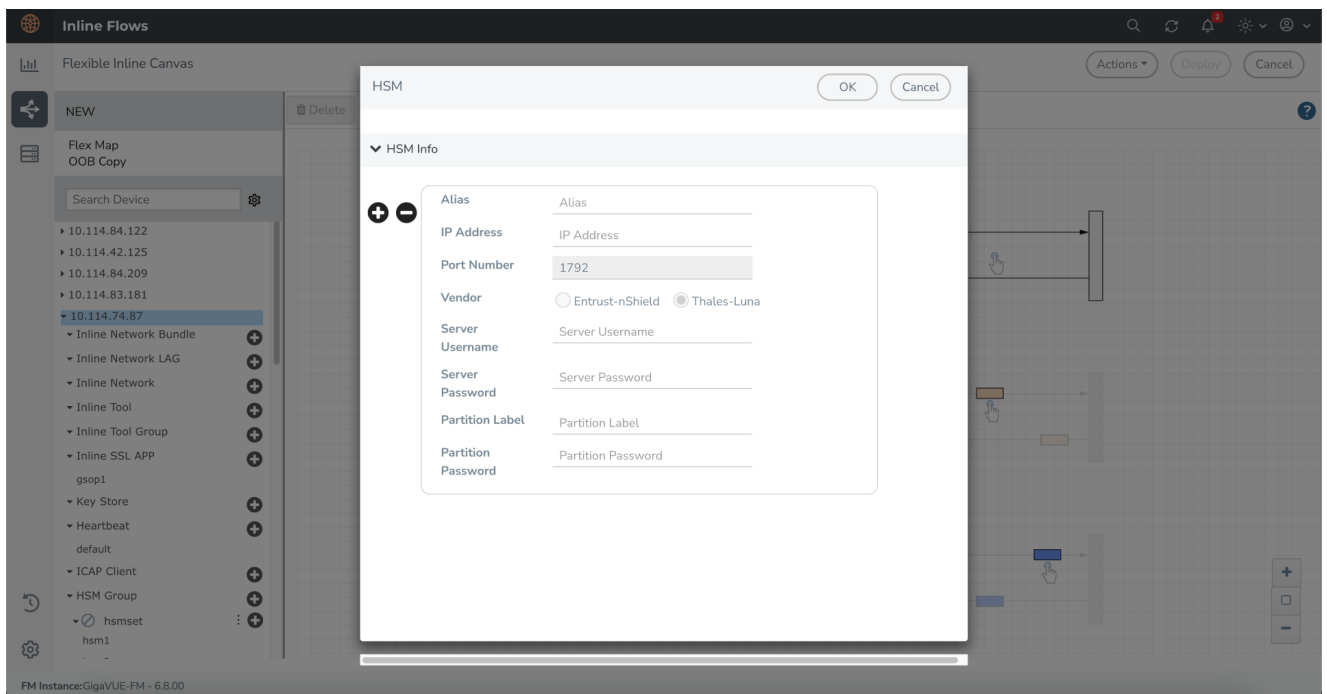
NOTE: For Thales-Luna Network HSM, you can create a maximum of 16 HSM units per device.

6. Click **Apply** to save the configurations. All individual HSM units you create will be listed under the configured HSM Group.

Add Thales -Luna HSM Appliance to the HSM Group

To add your vendor type as Thales-Luna to your configured HSM Group follow the below steps:

1. In the Flexible Inline Canvas, select the device for which the HSM Group is configured.
2. Click the expand menu on the configured **HSM Group**.
3. Click the '+' icon next to the configured **Thales-Luna** HSM to proceed.



4. In the HSM pop-up that appears, enter a name for the HSM appliance in the **Alias** field.
5. Enter the IP address of the HSM server and **Port Number**.



Notes:

- The default port number for Thales- Luna HSM is 1792.
- It is preferable to use a static IP address to prevent the Thales Luna registration from expiring.

6. By default, Thales-Luna is selected and Entrust nShield is disabled in the **Vendor** type when configuring Thales-Luna.
7. Enter the valid username and password in the **Server Username** and **Server Password** fields.
8. Enter the valid details in the **Partition Label** and **Partition Password** fields.

NOTE: When adding multiple HSM appliances, make sure to keep the Partition Password same for all the partitions.

9. Click **OK** to save the configuration.



Notes

For **Thales-Luna** configuration, if the operational status of the HSM Group shows '**Registration pending**', follow the below steps to register the HSM client (GigaSMART engine) with the HSM server:

1. Register the HSM Client (GigaSMART engine's IP address) on the HSM server.

Create an Inline SSL APP and Attach the HSM Group

1. On the left pane, click the '+' icon next to the **Inline SSL APP** option.
2. Enter a name for the Inline SSL APP and select the required GigaSMART engines.
3. From the **HSM Group** drop-down list, select the configured **hsm-luna** Group alias.
4. Under Deployment Type, set up Key chain Password:
 - a. Click **Keychain Password**, and then choose either Add or Reset.
 - b. If you choose to reset the Keychain Password, enter a password that is 8 to 30 characters long and contains at least one numerical character, one uppercase character, one lowercase character, and one special character.
 - c. Select the **Auto Login** check box to enable GigaVUE-FM to unlock the keystore when the device reboots.
 - d. Click **OK** to save the Key chain Password.

5. Configure **Keys and Certificates**. A key in an inbound deployment can be selected only for decryption or for re-signing and re-encryption in an outbound deployment.
 - a. Click **Add Keys** to open the Key page.
 - b. In the **Key Alias** and **Description** fields, enter a name and description for the SSL key.
 - c. For Key Type, select either **RSA** or **ECDSA**.
 - d. From the **File Type** drop-down list, select **Luna-HSM**.
 - e. Choose one of the following methods to import the required key token:
 - **Install from URL**—Enter a valid directory path including the file name and enter the password to access the server.
 - **Install from Local Directory**—Browse and select the key handler file from your local directory.
 - f. Choose one of the following methods to import the corresponding certificate:
 - **Install from URL**—Enter a valid directory path including the file name and enter the password to access the server.
 - **Install from Local Directory**—Browse and select the certificate file from your local directory.

NOTE: You can obtain the key token and the corresponding certificate from your HSM administrator.

- g. Click **OK**. You have successfully created the Primary key.
 - h. Repeat **steps 1-6** to configure the secondary signing certificate and private key.
6. Thales-Luna HSM configuration is supported in Inbound, Outbound, and Hybrid deployment types. Select the required deployment type. Refer to [TLS/SSL Sessions](#) for more details.
 - **Outbound** - Add the configured primary and a secondary signing Certificate Authorities (CA).
 - **Inbound** - Add a new Server Key Mapping. Enter the domain name or IP address of the server, and then select the required Key Pair Alias.
 - **Hybrid** - Add a new Server Key Mapping, and a primary and a secondary signing CA.
7. Select Outbound as your deployment type and add the configured primary and a secondary signing Certificate Authorities (CA).
8. Under **Configurations**, for Default Action select one of the following options:
 - **Decrypt**—Decrypt all the traffic that is guided into the Inline SSL APP.
 - **No Decrypt**—Do not decrypt the traffic that is guided into the Inline SSL APP.
9. For **URL Cache Miss Action**, select one of the following options

- **Decrypt**—Decrypt all the traffic that is guided into the Inline SSL APP.
 - **No Decrypt**—Do not decrypt the traffic that is guided into the Inline SSL APP.
 - **Defer**—Delay the decryption until the Defer Timeout seconds provided.
10. Under **Security Expectations**, choose to either decrypt or drop the traffic for the following certificates:
- Self-signed certificate
 - Unknown CA certificate
 - Invalid certificate
 - Expired certificate
11. Under **Network Access**, select IP Address as the network access configuration mode. Enter the IP Address, Netmask, Gateway, DNS, MTU, and VLAN.



Notes:

- DHCP mode is not supported when configuring Thales-Luna HSM, as IP changes can break connectivity if the new address isn't registered with the HSM server
- Ensure that IP address you are using is already registered in the HSM server.

12. Under **Trust Store**, set up Set up the Signing Certificate Authority (CA).
- Click **Append** and choose one of the following methods:
 - **Copy and Paste** - Directly paste the Trust Store Certificate.
 - **Install from Local Directory** - Browse and select the certificate file from your local directory.
 - Click **Replace** to update the existing certificate with a new one.
13. Click **OK**. You have successfully created the Inline SSL APP.

Refer to [Inline SSL App—Field References](#) for any additional details when configuring the Inline SSL APP.

Deploy the Inline SSL Solution

1. Drag and drop the required inline network or inline network bundle into the flexible inline canvas.
2. Drag and drop the flexible inline map into the canvas.
3. In the Properties pane, click **Add Rule**, and add **Bi-directional** as the rule condition.
4. In the rule description, add protocol as TCP. Add the required rules for the inline map, and then click OK to save the configuration.
5. Drag and drop the Inline SSL APP into the canvas.

6. Drag and drop the required inline tools or inline tool group into the canvas.
7. Click **Deploy**.

Register GigaSMART Engine on Thales Luna HSM Server

After deploying the Gigamon configuration, the Luna HSM administrator must register the GigaSMART engine (client) on the Luna HSM using the GigaSMART IP you configured in Network Access.

If client registration is not completed within the required time window (10 minutes), operational status can move to a registration timeout state. Work with your HSM admin to complete registration on the Luna HSM side. Refer to [Client Register - Luna Command Reference](#) for more details.

Verify the Solution

- Confirm the solution is Deployed on the Flexible Inline Canvas (**Physical > Orchestrated Flows > Inline Flows > Configuration Canvas**) and the Inline SSL app is present in the canvas.
- Verify HSM group, connectivity, and trust
 - In GigaVUE-FM, verify the HSM Group exists and is associated to the target node (s).
 - Confirm the Thales Luna HSM appliance/client is registered and reachable; check that the Luna partition/slot assignment is correct and shows a healthy/connected state.
 - Ensure you are not mixing HSM vendors on the same device (do not combine Entrust and Thales).
- Confirm that the Inline SSL app is using Thales Luna HSM-backed keys (not local files), the Keychain Password is unlocked, and the keys/certificates load without errors or HSM/keystore alerts so they are available for decryption
 - In the Inline SSL App's keys/certificates area:
 - Verify each required key/cert shows Thales Luna HSM as the source (HSM-backed), not local/PEM/PKCS12.
 - Ensure the GigaVUE-FM Keychain Password is unlocked so the app can access the keystore.
 - Confirm keys/certs load without errors (no red badges or "key not found/permission denied/keystore locked" messages).
 - Check Events/Alerts for any HSM-related issues (e.g., partition login failures, HSM connectivity, permission errors). There should be no HSM/keystore alerts.

What to Do Next

After deployment, you can view the the statistics details , refer to [View HSM Statistics](#).

Modify an HSM Deployment for Inline TLS/SSL Decryption

When modifying an HSM Decryption deployment, follow the steps below to ensure a smooth and secure transition:

1. **Switch to Bypass Mode**

Move the Inline Network traffic path to Bypass mode to prevent disruption during the configuration change.

2. **Apply Deployment Changes**

Make the required deployment modifications. Supported transitions include:

- From non-HSM based decryption to Thales Luna HSM based decryption
- From HSM-based decryption to non-HSM based decryption

3. **Reboot GigaSMART Card**

After applying the changes, reboot the GigaSMART card to apply the new configuration.

4. **Switch to Inline Mode**

Move the Inline Network traffic path from Bypass mode to '**To Inline Tool**' mode to resume normal operation.



Notes:

- Ensure that at least one active Luna HSM is available in the High Availability (HA) group to avoid decryption service interruption.
- If a partition fails in the Luna HSM configuration but at least one active partition remains, do not reload the device.
- The network connection between the HSM and GigaSMART must use a static IP address. Do not use DHCP, as the IP address must remain consistent for proper communication.

Configure ICAP Client for Inline TLS/SSL Decryption Solution

This section provides topics on configuring and using **ICAP Client** for Inline TLS/SSL Decryption Solution.

Prerequisites

- Allocate two separate GigaSMART engines—one dedicated to Inline SSL and one to ICAP—and if HTTP/2 downgrade is required in Inline SSL, use Gen3 devices for both engines.
- Rely on the system to add the GigaSMART Group automatically for ICAP when the port is attached to the ICAP Client, so you do not need to add it during IP Interface creation.
- Gather the ICAP server details, including IP/hostname and listening port (typically 1344), plus any required service URIs (REQMOD, RESPMOD, OPTIONS).
- Decide on the deployment type—Same Node or Different Node—and for Same Node be prepared to select the Inline SSL Inline Tool as the ICAP Client's Source port, while for Different Node you must ensure a network interconnect carries the clear-text feed from the Inline SSL node to the ICAP node's Inline Network.
- Verify compatibility constraints beforehand, because the ICAP Client cannot be deployed inline with One-Arm iSSL, L3 NAT iSSL, or RIA iSSL.

Access Flexible Inline Canvas

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the TLS/SSL decryption.

Configure Inline Network

For an Inline SSL with ICAP deployment, create the Inline SSL constructs (one Inline Network with NA/NB legs and an Inline Tool) and a separate Inline Network for ICAP, then configure an IP Interface on a tool port with the required IP/subnet/gateway/VLAN to reach the ICAP server.

1. On the left pane, click the '+' icon next to **Inline Network** option to create a new entry.

2. Enter a name and description for the inline network in the **Alias** and **Description** fields. Then, click **Port Editor**.
3. In the **Alias** and **Description** fields, enter a name and description for the inline network.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline network ports that you want to configure. Select **Enable** to administratively enable inline network ports, and click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the ports that you want to configure as the inline network pair.
6. From the **Traffic Path** drop-down list, select **To Inline Tool**.
 - **To Inline Tool**—All traffic originating from the inline network is directed to the sequence of inline tools and inline tool groups and is guided through the inline tools and inline tool groups according to the current inline tool and inline tool group status.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Network Ports and Inline Network](#).

Configure Inline Tool

1. On the left pane, click the '+' icon next to the **Inline Tool** option to create a new inline tool.
2. In the **Properties** pane, in the **Alias** and **Description** fields, enter a name and description for the inline tool.
3. From the **Type** drop-down list, select one of the following options:
 - **External**- To configure a third-party tool.
 - **GigaVUE Node**- To configure a GigaVUE node as a tool.
4. Click **Port Editor**. In the **Quick Port Editor**, scroll down to the inline tool ports that you want to configure. Select **Enable** to administratively enable the inline tool ports, and then click **OK** to apply the changes.
5. From the **Port A** and **Port B** drop-down lists, select the inline tool ports according to the direction the inline tool expects traffic from the network.
6. Verify that the **Enabled** check box is selected.
7. Click **OK**. You have successfully created an Inline Network.

To explore additional options during configuration, refer to [Inline Tool Ports and Inline Tools](#).

Configure IP Interface

1. On the left pane, click the '+' icon next to the **IP Interface** option to create a new IP Interface.
2. In the **Alias** and **Description** fields, enter a name and description for the IP Interface.
3. From the **Port** drop down list, select the port that is connected to Network and has reach ability to the ICAP server.
4. Select the **Type** of the IP Interface that you want to configure.
5. Enter an **IP Address**. For example, 192.168.1.20.
6. Enter an **IP Mask**. For example, 255.255.255.0.
7. Enter a **Gateway**. For example, 192.168.1.20.
8. Enter the Maximum Transmission Unit (MTU) for this port in the **MTU** field. For example, 1500.
9. Click **OK** to save the configuration.

NOTE: For ICAP, it is not necessary to add GS Groups when configuring IP interface. It will be added automatically when the port is added to ICAP Client.

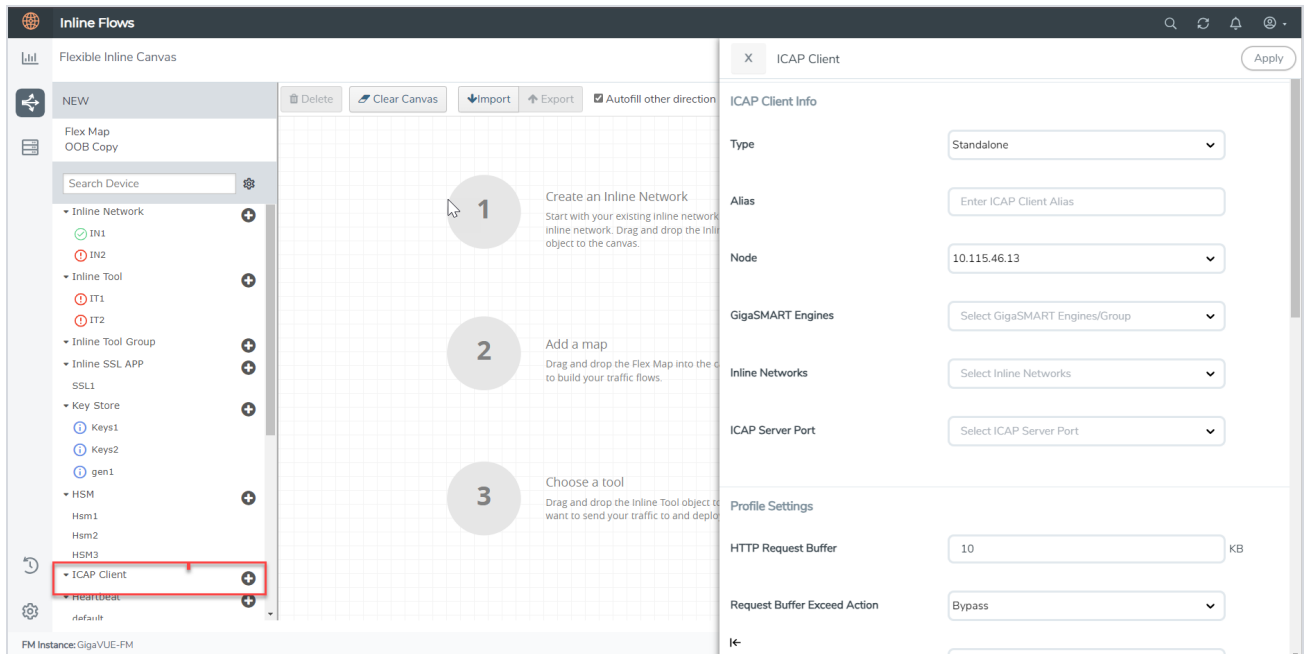
Configure ICAP Client

In an Inline TLS /SSL Decryption Solution with an **ICAP Client** the main choice for your ICAP configuration is :

- Type should be either Same Node or Different Node

To configure the ICAP Client:

1. Go to  > **Physical** > **Orchestrated Flows** > **Inline Flows** > **Configuration Canvas** to create a new Flexible Inline Canvas.
2. In the displayed Flexible Inline Canvas, select the device where you want to configure the ICAP Client.
3. Click the '+' icon next to the **ICAP Client** to create a new entry.
4. Enter a name and description for the inline network in the **Alias** and **Description** fields.



5. In the **ICAP Client** properties pane that appears on the right, complete the required fields in the ICAP Client Info, Profile Settings, and the Server sections. Refer to [Configure ICAP Client for Inline TLS/SSL Decryption Solution](#) for more details.
6. Select one from the following:
 - If ICAP and iSSL are integrated and deployed on the same node, select the **Same Node** option.
 - If ICAP and iSSL are integrated and deployed on different node, select the **Different Node** option.
7. Select the required tool port of Inline SSL profile, which is connected to the inline network of ICAP. (This option will not appear if you select standalone as type.)
8. Click **Apply** to save the configurations.

Create an Inline SSL APP

1. On the left pane, click the '+' icon next to the **Inline SSL APP** option.
2. Enter a name for the Inline SSL APP and select the required GigaSMART engines.
3. ICAP configuration is supported in Inbound, Outbound, and Hybrid deployment types. Select the required deployment type. Refer to [TLS/SSL Sessions](#) for more details.
 - **Outbound** - Add the configured primary and a secondary signing Certificate Authorities (CA).
 - **Inbound** - Add a new Server Key Mapping. Enter the domain name or IP address of the server, and then select the required Key Pair Alias.
 - **Hybrid** - Add a new Server Key Mapping, and a primary and a secondary signing CA.

4. Under **Configurations**, for Default Action select one of the following options:
 - **Decrypt**—Decrypt all the traffic that is guided into the Inline SSL APP.
 - **No Decrypt**—Do not decrypt the traffic that is guided into the Inline SSL APP.
5. For **URL Cache Miss Action**, select one of the following options:
 - **Decrypt**—Decrypt all the traffic that is guided into the Inline SSL APP.
 - **No Decrypt**—Do not decrypt the traffic that is guided into the Inline SSL APP.
 - **Defer**—Delay the decryption until the Defer Timeout seconds provided.
6. Under **Security Expectations**, choose to either decrypt or drop the traffic for the following certificates:
 - Self-signed certificate
 - Unknown CA certificate
 - Invalid certificate
 - Expired certificate
7. Under **Network Access**, select DHCP or IP Address as the network access configuration mode. If you select IP Address as the mode, enter the IP Address, Netmask, Gateway, DNS, MTU, and VLAN.

NOTE: It is recommended to use static IP address option when configuring ICAP Client.

8. Click **OK**. You have successfully created the Inline SSL APP.

To explore additional options during configuration, refer to [Inline SSL App—Field References](#).

Deploy the Inline SSL Solution

1. Drag and drop the required inline network configured for Inline TLS/SSL into the flexible inline canvas.
2. Drag and drop the Flexible Inline Map into the canvas, then in the Properties pane, click **Add Rule** and set the rule condition to **Bi-directional**.
3. In the rule description, add the protocol as TCP. Add the required rules for the inline map, and then click OK to save the configuration.
4. Drag and drop the Inline SSL APP into the canvas.
5. Drag and drop the required inline tools configured for Inline TLS/SSL into the canvas.
6. Click **Deploy**. You get two options to select your Traffic path during Deployment . It could be either **Logical Bypass** or **Keep as is**. Select an option based on your requirement and then click **OK**.

If the configuration is correct and the source ports of ICAP are properly linked to the Inline Tool port of Inline SSL, the canvas will display the inline tool indicating the ICAP client.

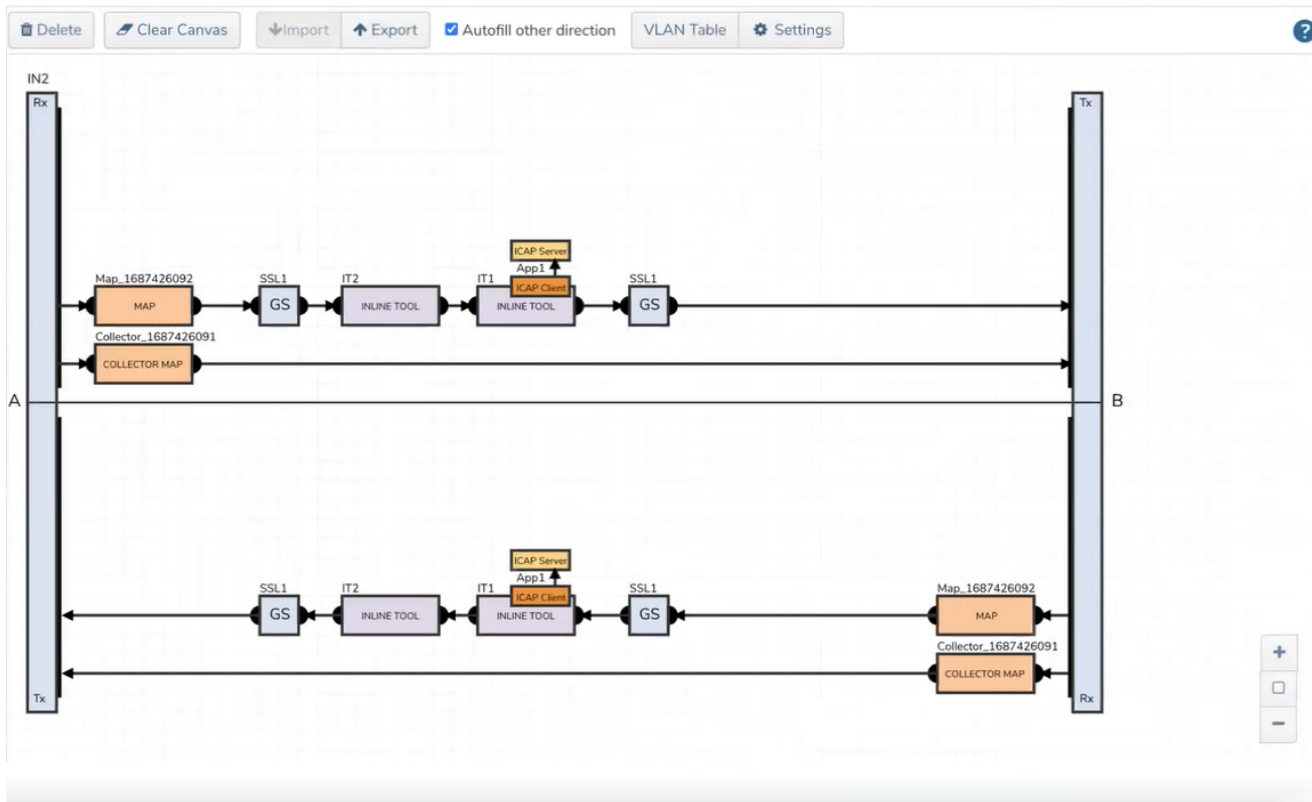


Figure 22 ICAP Client APP—Deployed

Verify the Solution

- Confirm the solution shows as Deployed on the Flexible Inline Canvas (**Physical > Orchestrated Flows > Inline Flows > Configuration Canvas**); ensure both Inline Networks exist: one attached to the Inline SSL app and a separate one attached to the ICAP client.
- Verify ICAP client wiring and health
 - Open the ICAP client properties and confirm:
 - The ICAP client is attached to the intended Inline Network (the ICAP-specific inline network you created).
 - Source Port/Interface points to the correct inline or tool port that reaches the ICAP server (as per your design).
 - If you created an IP Interface on a tool port to reach the ICAP server, verify:
 - IP/subnet/gateway/VLAN are correct and the interface shows Up.
 - Basic reachability to the ICAP server (no Events/Alerts indicating ARP/route failures).

What to Do Next

After deployment, you can view statistics details, refer to [View Inline Solution Status and Statistics](#).

View Inline Solution Status and Statistics

The flexible inline canvas provides you with the ability to view the status of the flexible inline flow deployments, port statistics, and the details of the cluster-level maps used in the deployments. You can use these details to troubleshoot any issues or failures in your flexible inline flows. The inline flows has the following tabs:

- Status
- Statistics

Refer to the following sections for more details:

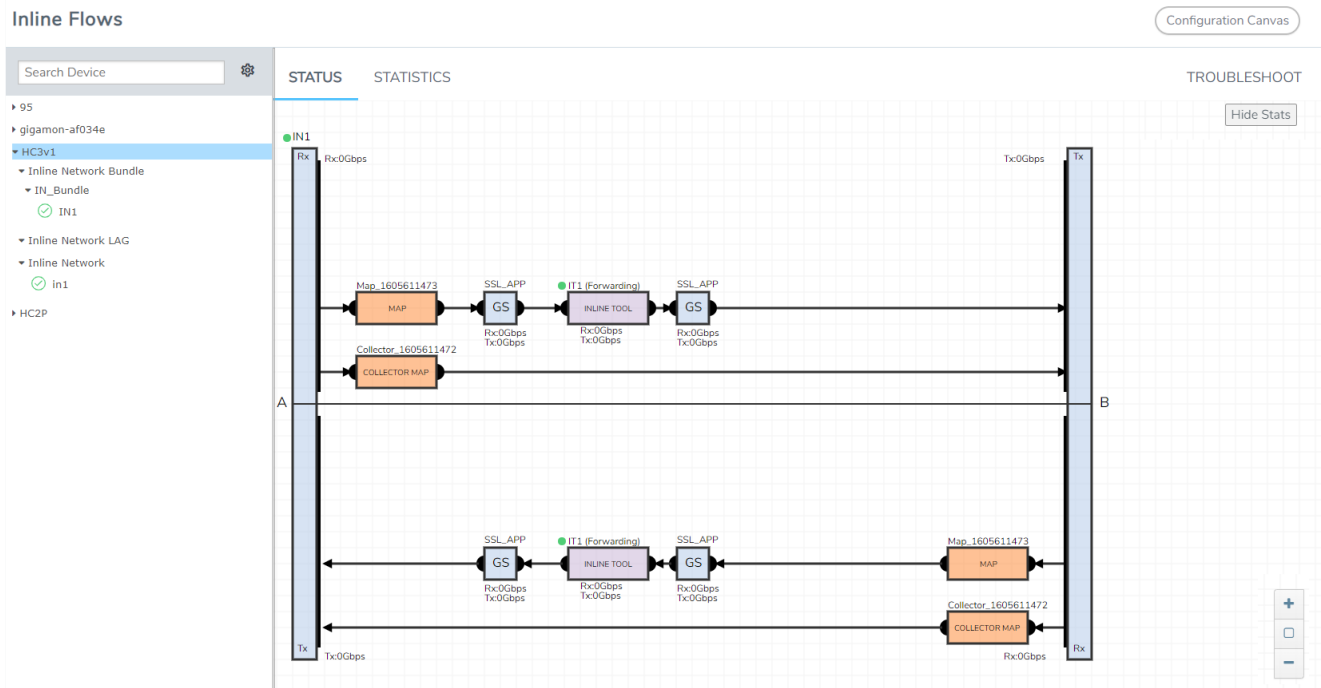
- [View Inline Solution Status](#)
- [View Inline TLS/SSL Session Statistics](#)
- [View Inline TLS/SSL Monitor Statistics](#)
- [View Inline TLS/SSL Certificate Statistics](#)
- [View HSM Statistics](#)
- [View ICAP Statistics](#)

View Inline Solution Status

The Status tab provides details of the forwarding states of inline network. Click the required component that is part of the selected inline network to view the component's properties.

It also provides the status of the components that are part of the selected inline network. Hover over the status to view the description.

Click the **Show Stats/Hide Stats** toggle button to view the Rx/Tx rate for the components that are part of the flexible inline flow deployment. Refer to the following figure for details.



Rules and Notes

Keep in mind the following points when you are viewing the details in the Status tab:

- The ability to view the Rx/Tx rate for the components is supported only for GigaVUE-HC1, GigaVUE-HC3 and GigaVUE-HC2 devices.
- The Rx/Tx rate for inline components are displayed in GigaVUE-FM only for flexible inline deployments. In addition, the historical trends are not displayed in GigaVUE-FM. However, you can view the Rx/Tx rate for classic inline components using the GigaVUE-OS CLI commands. For details, refer to the following topics in the *GigaVUE-OS CLI Reference Guide*:
 - show
 - ib pathway
 - inline tool group
 - inline tool
 - inline serial
 - inline network group
 - inline network
 - icap

- The Rx/Tx rate that is displayed is not for a map or a flexible inline flow, but it is a cumulative value that is shared across multiple maps and flexible inline flows.
- The Rx/Tx rate for a GigaSMART group is a cumulative value for the traffic flowing between both a-b and b-a directions.
- The Rx/Tx rate for OOB copy is supported only for single tool.
- You cannot view the health status of GigaSMART.
- The near real time data is not displayed for LED's health status and failover state representation of the inline component. The data gets updated during the GigaVUE-FM configuration synchronization period. Alternatively, when the Rx/Tx rate for an inline component drops to zero, you can choose to refresh the Status tab to view the updated data.

View the Forwarding States of Inline Networks

To view the forwarding states of inline networks in the flexible inline canvas, choose the required inline network, and then click **Status**. Refer to the following figure.

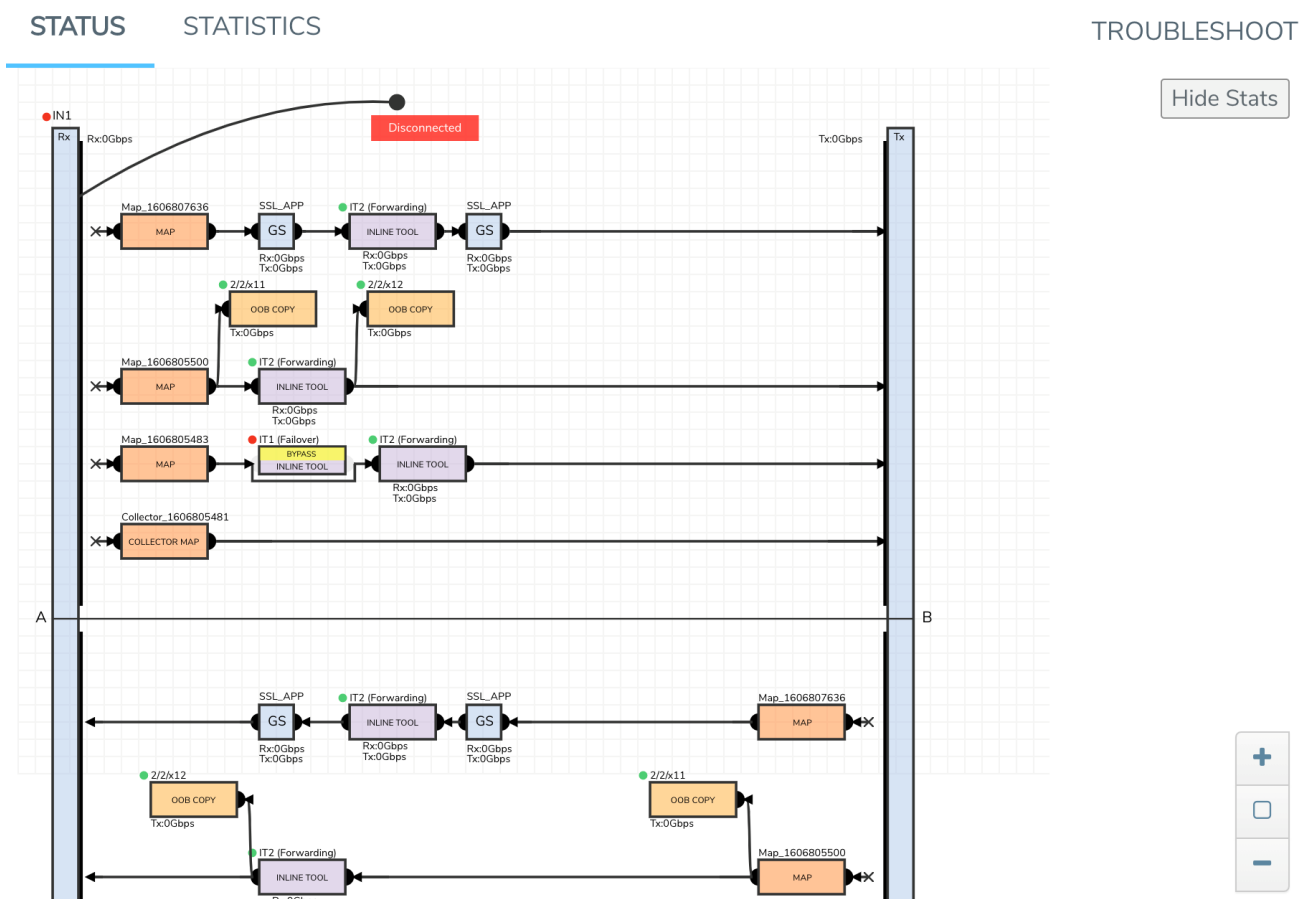


Figure 23 Inline Network Forwarding States

Following inline network states are not explicitly shown in the flexible inline canvas:

- Normal—If the state of all inline tools are up, the inline network is in Normal state.
- Abnormal—If any inline tool involved in flexible inline maps (directly or indirectly as a member of an inline tool group) is operationally down and there is no network-level failover action in effect, the inline network is in an Abnormal state.

Following table provides the list of forwarding states of inline network and their description.

Table 7: Forwarding States of Inline Networks

Inline Network Physical Bypass	Inline Network Traffic Path	Far-End Status of Links Connected to Inline Network Ports	Operational State of Not Forced Inline Tools and Inline Tool Groups Involved in Maps from the Inline Network	Forwarding State	Description
enable	any inline network traffic path configuration	any combination of far-end ports status	any combination of operational state of the inline tools or inline tool groups involved in the maps originating from the inline network	PHYSICAL BYPASS	all traffic exchanged directly between the end nodes without being noticed by the switching fabric (GigaVUE-FM,GigaVUE HC Series node acting as a wire or fiber)
disable	traffic path set to drop	any combination of far-end ports status	any combination of operational state of the inline tools or inline tool groups involved in the maps originating from the inline network	DISABLED	all traffic arriving at the inline network ports is dropped
disable	traffic path set to bypass, monitoring, or to-inline-tool	at least one far-end port is down	any combination of operational state of the inline tools or inline tool groups involved in the maps originating from the inline network	DISCONNECTED	No traffic is exchanged between the nodes

Inline Network Physical Bypass	Inline Network Traffic Path	Far-End Status of Links Connected to Inline Network Ports	Operational State of <i>Not</i> Forced Inline Tools and Inline Tool Groups Involved in Maps from the Inline Network	Forwarding State	Description
disable	traffic path set to bypass	both far-end ports are up	any combination of operational state of the inline tools or inline tool groups involved in the maps originating from the inline network	FORCED BYPASS	All traffic that matches any of the maps originating from the inline network is redirected through a logical bypass
disable	traffic path set to monitoring	both far-end ports are up	any combination of operational state of the inline tools or inline tool groups involved in the maps originating from the inline network	FORCED BYPASS WITH MONITORING	A copy of the traffic originating from the inline network bypasses the sequence of inline tools and inline tool groups and is re-directed to the opposite-side inline network port. Another copy of the traffic is directed to the sequence of inline tools and inline tool groups, except that no traffic of the second copy is sent to the exit port.
disable	traffic path set to to-inline-tool	both far-end ports are up	all inline tools involved (directly or indirectly as members of inline tool groups) in the maps originating from the inline network are in the <i>up</i> operational state	NORMAL	The traffic is guided between the source inline network port and the destination inline network port according to the status of the inline tools and inline tool groups. NOTE: The state of all inline tools must

Inline Network Physical Bypass	Inline Network Traffic Path	Far-End Status of Links Connected to Inline Network Ports	Operational State of <i>Not</i> Forced Inline Tools and Inline Tool Groups Involved in Maps from the Inline Network	Forwarding State	Description
					be <i>up</i> , including inline tools configured as spare in an inline tool group, inline tools or inline tool group members in the a-to-b and b-to-a lists configured with any traffic path other than to-inline-tool.
disable	traffic path set to to-inline-tool	both far-end ports are up	at least one of the inline tools or inline tool groups involved in the maps originating from the inline network configured with the traffic path parameter to-inline-tool and failover action of network-port-forced-down is in the <i>down</i> operational state	NETWORK PORTS FORCED DOWN	No traffic is exchanged between the inline network ports, and the inline network ports are brought down
disable	traffic path set to to-inline-tool	both far-end ports are up	none of the inline tools or inline tool groups involved in the maps originating from the	FAILURE INTRODUCED DROP	All traffic arriving at the inline network ports is dropped

Inline Network Physical Bypass	Inline Network Traffic Path	Far-End Status of Links Connected to Inline Network Ports	Operational State of Not Forced Inline Tools and Inline Tool Groups Involved in Maps from the Inline Network	Forwarding State	Description
			inline network configured with to-inline-tool and failover action network-port-forced- down is in the down operational state at least one of the inline tools or inline tool groups involved in the maps originating from the inline network configured with to-inline-tool and failover-action of network-drop is in the down operational state		
disable	traffic path set to to-inline-tool	both far-end ports are up	none of the inline tools or inline tool groups involved in the maps originating from the inline	FAILURE INTRODUCED BYPASS	All traffic that matches any of the maps originating from the inline network is redirected through a logical bypass

Inline Network Physical Bypass	Inline Network Traffic Path	Far-End Status of Links Connected to Inline Network Ports	Operational State of Not Forced Inline Tools and Inline Tool Groups Involved in Maps from the Inline Network	Forwarding State	Description
			network configured with to-inline-tool and failover action of network-port-forced-down or network-drop is in the <i>down</i> operational state at least one of the inline tools or inline tool groups involved in the maps originating from the inline network configured with to-inline-tool and failover action of network-bypass is in the <i>down</i> operational state		
disable	traffic path set to to-inline-tool	both far-end ports are up	any combination of conditions not listed for the forwarding state definitions of PHYSICAL BYPASS, DISABLED,	ABNORMAL	The traffic is guided between the source inline network port according to the status of the inline tools and inline tool groups NOTE: If any inline

Inline Network Physical Bypass	Inline Network Traffic Path	Far-End Status of Links Connected to Inline Network Ports	Operational State of <i>Not</i> Forced Inline Tools and Inline Tool Groups Involved in Maps from the Inline Network	Forwarding State	Description
			DISCONNECTED, FORCED BYPASS, FORCED BYPASS WITH MONITORING, NORMAL, NETWORK PORTS FORCED DOWN, FAILURE-INTRODUCED DROP, or FAILURE-INTRODUCED BYPASS		tool involved in flexible inline maps (directly or indirectly as a member of an inline tool group) is in the <i>down</i> operational state and there is no network-level failover action in effect, the inline network is in the ABNORMAL state.

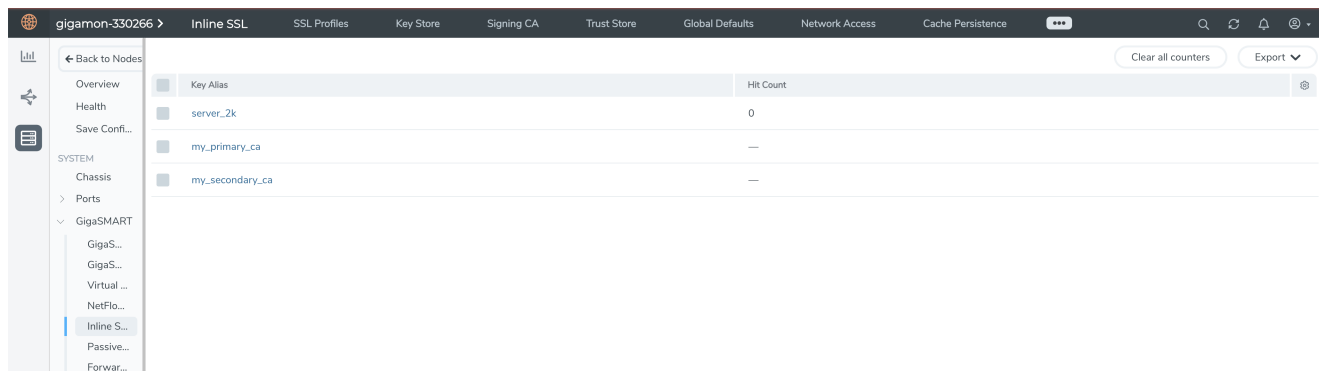
NOTE: When the Inline Network traffic path is set to monitoring and the Inline Tool Failover action is configured as 'Network Port Force Down,' the Inline Tool will continue to receive traffic, even if it is disabled or in an operational down state. This behavior is expected.

View Inline TLS/SSL Session Statistics

The Statistics tab provides statistical information of the inline network ports, inline tool ports, and the virtual ports used in the selected inline network. It also provides the inline decryption session statistics for the inline network. The inline network, inline tools, ICAP Client, and the ports aliases are displayed as clickable links. Use these links to access the quick view of the respective component. Refer to the following figure for details.

To display the inline TLS/SSL summary details, go to **GigaSMART > Inline SSL > Session Statistics**, view the Summary details under **Summary** tab which is displayed initially. Refer to [Figure 24 Inline TLS/SSL Session Statistics in GigaVUE-FM](#).

There are four sections: Session Statistics, Performance Statistics, Policy Statistics, and Certificate Statistics. Click **Show Summary** to view these sections. Click **Clear Session Summary** to clear all the displayed summary details.



Key Alias	Hit Count
server_2k	0
my_primary_ca	—
my_secondary_ca	—

Figure 24 Inline TLS/SSL Session Statistics in GigaVUE-FM

To view the inline TLS/SSL session details, go to **GigaSMART > Inline SSL > Session Statistics**. Click on the **Sessions** tab. The list of available sessions will be displayed. To search and filter the session details, click **Filter** and enter an IPv4 source or destination, an L4 port source or destination, or a host name.

View Inline TLS/SSL Monitor Statistics

To display monitor statistics, go to **GigaSMART > Inline SSL > Monitor Statistics**. Select the required GigaSMART engine from the drop-down menu.

There are three sections. The first section, which has a graph for INTERFACE TRAFFIC and Interface Packet statistics, is displayed initially. To return to this display, click the small graph, TOTAL INCOMING PACKETS. Refer to [Figure 25 Inline TLS/SSL Session Monitor—Interface Packet Statistics](#).

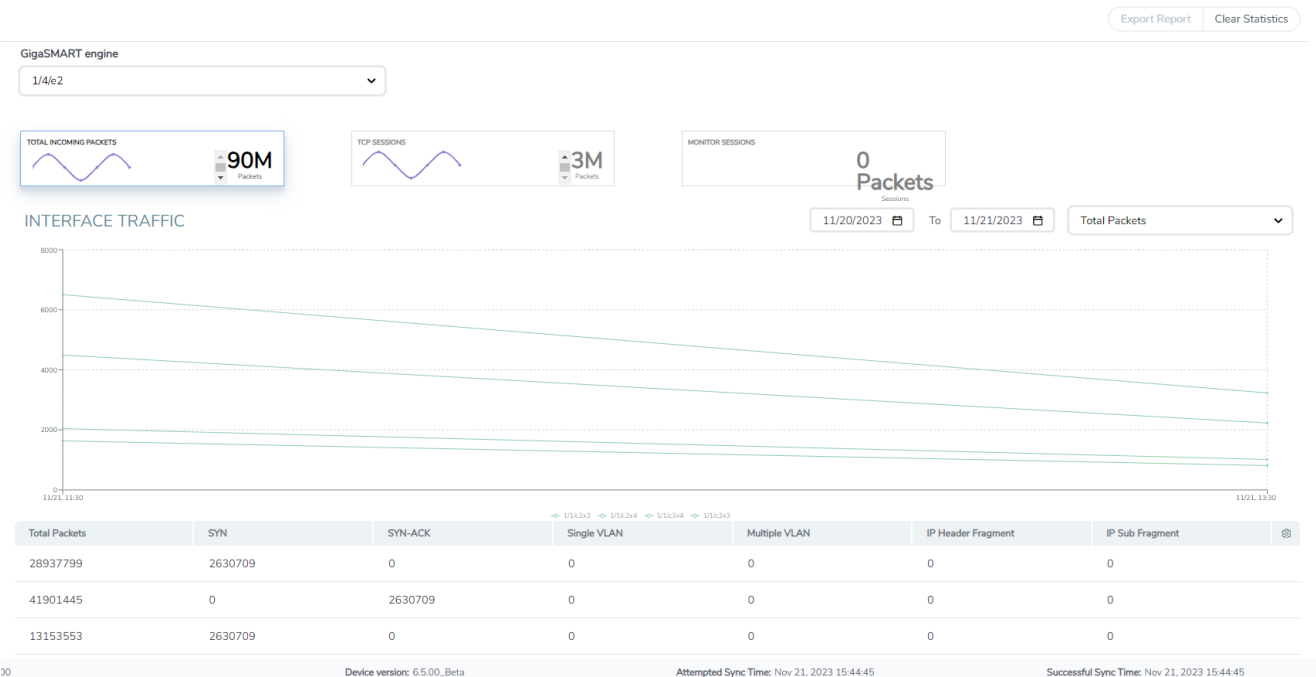


Figure 25 Inline TLS/SSL Session Monitor—Interface Packet Statistics

To display the graph and statistics for TCP Sessions, click the small graph, TCP SESSIONS. Refer to [Figure 26 Inline TLS/SSL Session Monitor—TCP Sessions](#).

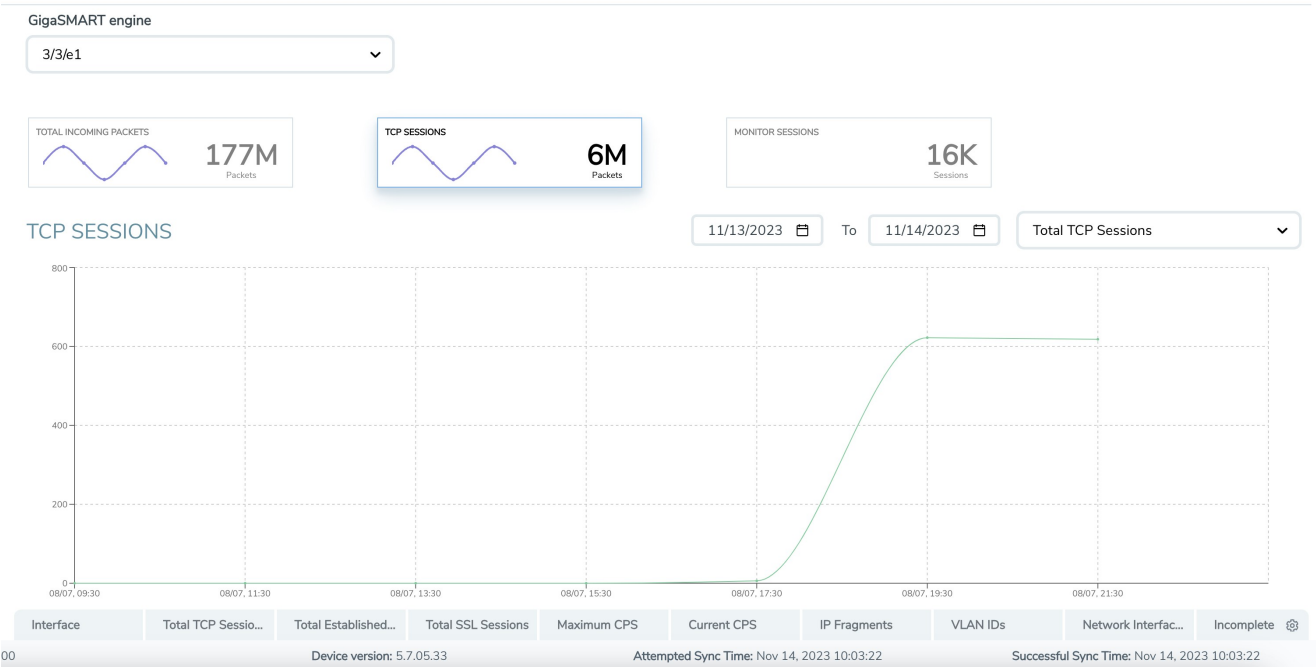


Figure 26 Inline TLS/SSL Session Monitor—TCP Sessions

To display Monitor Sessions, click the small graph, MONITOR SESSIONS. Refer to [Figure 27 Inline TLS/SSL Session Monitor—Monitor Sessions](#).

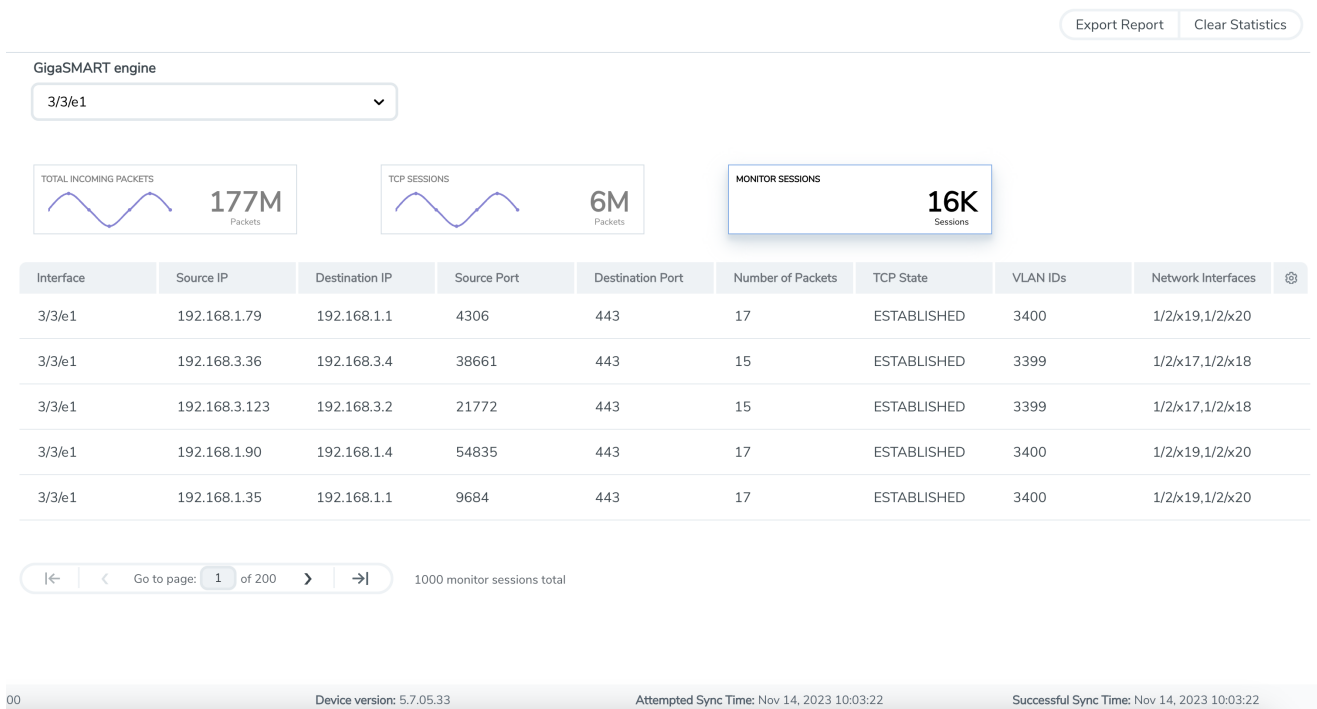


Figure 27 Inline TLS/SSL Session Monitor—Monitor Sessions

Click **Clear Statistics** to clear all the displayed statistics details.

View Inline TLS/SSL Certificate Statistics

To view certificate statistics, go to **GigaSMART > Inline SSL > Certificate Statistics**. The page displays the hit count of each key store certificate and allows to track whether the certificate is actively used or not. The hit count is numbered only if the policy is set for decryption. If the policy is set to no-decryption or if the deployment is outbound, the hit count will not be considered.

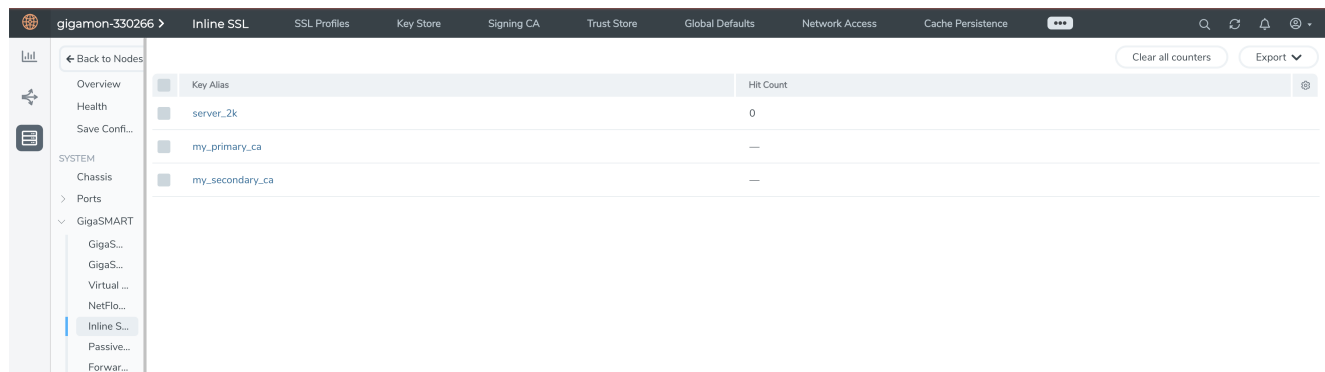


Figure 28 Inline SSL - Certificate Statistics

Click **Clear all Counters** to clear the hit counter of all the certificates. Click **Export** to export the available hit count details.

View HSM Statistics

1. In the **Inline Flows** page, select the required device for which you want to view the statistics.
2. Click **Statistics > View HSM Statistics**. You can view the following statistics details for **Entrust nShield HSM** under Client Statistics and Server Statistics:
 - o Number of Request(s) Received
 - o Number of Response(s) Sent
 - o Metric values
 - o Error details
 - o Number of Request(s) Sent
 - o Number of Response(s) Received
 - o Delay time
 - o Average Round Trip Time

The screenshot shows the GigaVUE Inline Solutions interface. On the left, there is a sidebar with a search bar and a tree view of devices. The main area has tabs for STATUS, STATISTICS, and TROUBLESHOOT. Under the STATISTICS tab, there are sections for SSL APP, Engine Port, and Monitor Statistics. The Monitor Statistics section contains three tables: Sessions (Active), Traffic, and Performance Metrics. The 'View HSM Stats' button is highlighted in a red box.

Metric	Value
Established Sessions	0
SSL Sessions	0
Incomplete Sessions	0
Multi VLAN Sessions	0

Metric	Value
Packets/sec Rx	2
Drop Packets/sec	0
SYN Received	0
SYN ACK Received	0

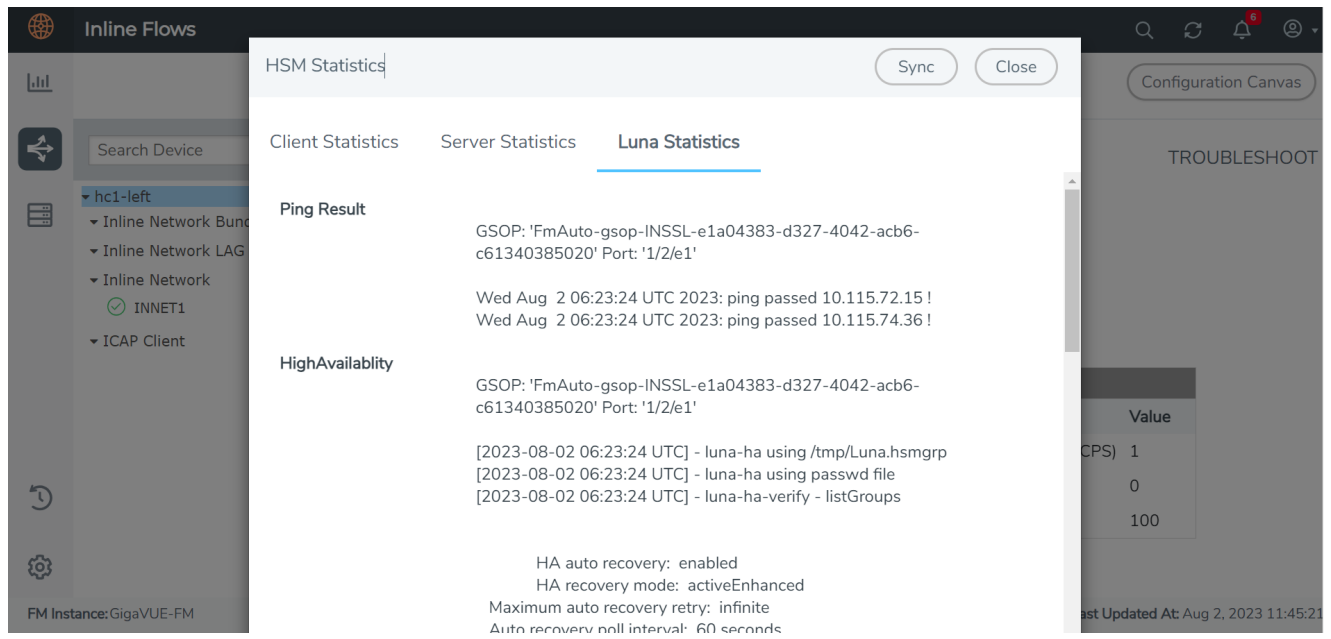
Metric	Value
Active Connections Per Second (CPS)	1
CPU Utilization%	0
CPU Idle Time%	100

FM Instance: GigaVUE-FM

Last Updated At: Aug 2, 2023 11:45:21

The HSM Statistics window includes the following tabs:

- **Client Statistics** tab, which includes information on number of requests received and responses sent, metrics, and error details.
- **Server Statistics** tab, which includes details on the number of requests sent and responses received, delay, and average time drop details.
- **Luna Statistics** is included in the HSM Statistics window. The **Luna Statistics** tab provides statistical information on the Ping Result, High Availability, and the verification details.



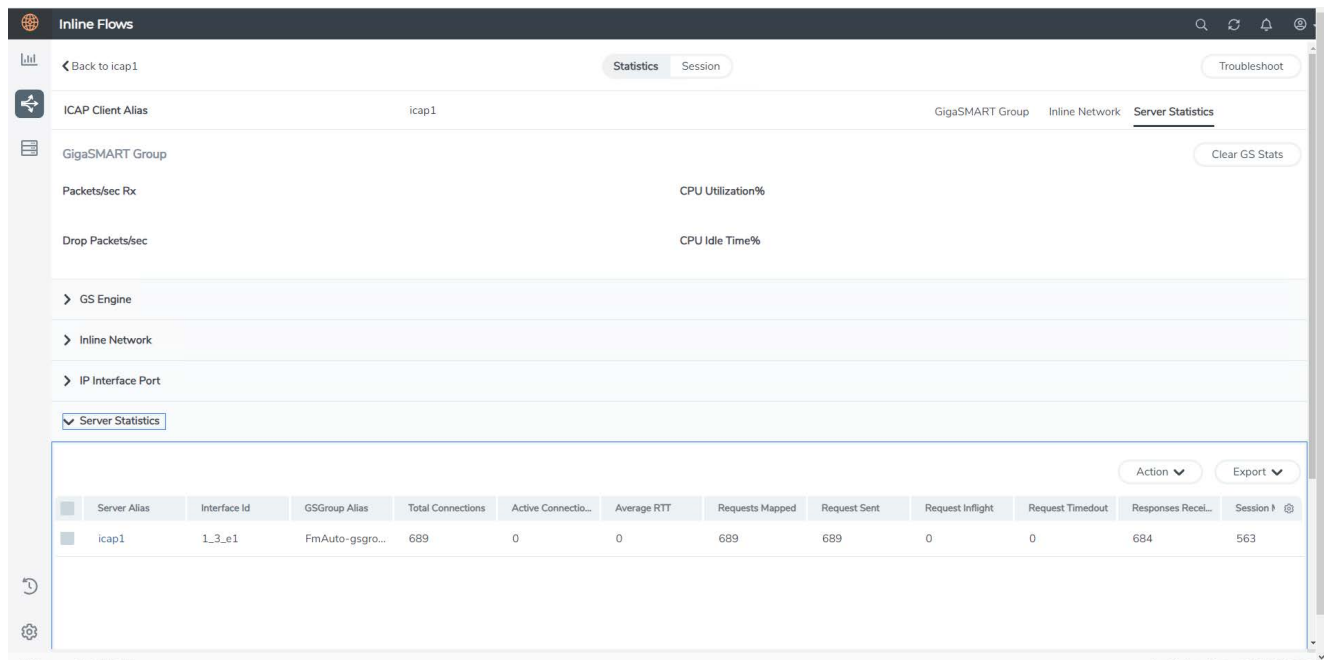
View ICAP Statistics

The Show Stats option will be displayed after the ICAP Client app is configured and deployed. The Show Stats option has the following tabs:

- Statistics
- Session

The **Statistics** tab provides statistical information on the GigaSMART group, GS engines, inline network, IP interface port, and server statistics. Click the drop-down menu of each component listed on the statistics page to know more about the configuration details. You can also view the statistics from the sidebar on the Inline Flows page.

The GS Engine drop-down menu provides information on the ICAP session statistics. Click **Clear GS Stats** to clear the statistics of the GS group.



To view ICAP session statistics details, click the **Sessions** tab.

The screenshot shows the 'Sessions' tab in the GigaVUE Inline Flows interface. The interface displays a table of session statistics for the 'icap1' client alias. The table includes columns for Interface Id, GigaSMART Group, ICAP Server, Source IP, Destination IP, Source Port, Destination Port, Protocol, TCP Status, ICAP Session, Error, ICAP Status, Start Time, Total Duration, C2S Total Pkt Co., and S2C Total Pkt Co. The table shows 14 sessions in total.

Interface Id	GigaSMART Group	ICAP Server	Source IP	Destination IP	Source Port	Destination Port	Protocol	TCP Status	ICAP Session	Error	ICAP Status	Start Time	Total Duration	C2S Total Pkt Co.	S2C Total Pkt Co.
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	34.107.221.82	38840	80	http1.1	BYPASS	BYPASS	ERR	REQMOD	1970-01-01 0...	28	7	4
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	104.254.148...	39350	443	http1.1	BYPASS	BYPASS	ERR	REQMOD	1970-01-01 0...	14	18	17
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	204.79.197.2...	43952	443	tcp	NO	NO	NO ERR		1970-01-01 0...	23	1	0
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	40.126.62.130	47740	443	http1.1	YES	YES	NO ERR	RESPMOD	1970-01-01 0...	16	14	13
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	52.37.154.49	54204	443	http1.1	YES	YES	NO ERR	RESPMOD	1970-01-01 0...	28	4	3
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	34.117.65.55	43502	443	http1.1	BYPASS	BYPASS	ERR	REQMOD	1970-01-01 0...	26	6	5
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	20.189.173.12	37036	443	http1.1	YES	YES	NO ERR	REQMOD	1970-01-01 0...	16	16	15
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	20.189.173.12	37038	443	http1.1	YES	YES	NO ERR	RESPMOD	1970-01-01 0...	12	11	8
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	20.189.173.12	36046	443	http1.1	YES	YES	NO ERR	REQMOD	1970-01-01 0...	20	16	15
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	40.126.62.130	47736	443	http1.1	BYPASS	BYPASS	ERR	REQMOD	1970-01-01 0...	16	10	9
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	68.67.129.19	33634	443	http1.1	BYPASS	BYPASS	ERR	REQMOD	1970-01-01 0...	14	136	136
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	23.37.116.6	47334	443	http1.1	YES	YES	NO ERR	RESPMOD	1970-01-01 0...	15	48	48
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	34.107.221.82	38830	80	http1.1	BYPASS	BYPASS	ERR	REQMOD	1970-01-01 0...	28	7	4
1/3e1	FmAuto-gsgr...	icap1	5.5.5.5	69.192.139.2...	50548	443	http1.1	YES	YES	NO ERR	RESPMOD	1970-01-01 0...	20	4	3

Refer to the below table for more details on the sessions tab.

Field	Description
Filter	To view the statistics of a particular IP with selected parameters.
Action	Upload to server: To export the log details to an external server.
Export	To export the current session details to local.

View Inline TLS/SSL Dashboards

GigaSMART Inline TLS/SSL Dashboards offer insights into session performance, network capacity, traffic decryption, compliance analysis, and historical data. Monitoring decryption statuses and anomalies helps organizations enhance security.

These dashboards provide real-time alerts and detailed reports for network security administrators to maintain data integrity and security compliance. It allows you to visualize the information with GigaVUE-FM. These dashboards are supported only for Gen 3 GigaSMART card platforms.

A few of the use case scenarios where the Inline TLS/SSL Dashboard could detect and manage anomalies:

- Alert administrators when a TLS handshake involves certificates signed with insecure hash algorithms.
- Alerts can be triggered when CBC mode is used, especially in older versions of TLS (for example, TLS 1.0 and TLS 1.1), advising an upgrade to more secure cipher modes like GCM (Galois/Counter Mode).
- Identify and report the use of certificates with weak signatures in the network traffic, facilitating a swift response to enhance security.
- Automatic detection and reporting of expired certificates help maintain continuous security compliance and trust.
- Monitoring and analyzing trends in decryption success and failure rates can pinpoint disruptions or anomalies in encrypted traffic handling.
- Ensure only approved cryptographic standards are used and generate compliance reports for auditing purposes.

Access TLS/SSL Dashboards

To access the dashboard:

1. Go to  -> **Analytics -> Dashboards.**
2. Click on the required dashboard to view the visualizations.

Inline TLS/SSL Dashboard can be categorized into two types:

- [Basic Dashboards](#)
- [Advanced Dashboards](#)

Basic Dashboards

The Basic dashboards are available by default and provides an overall information on the session. You can use the below control filters and specify the time period to visualize and filter the dashboard information:

- Host Name
- GigaSMART Groups Alias (GSGroup Alias)
- GigaSMART Engine ID (GSEngine ID)

The following are the basic dashboards and its visualizations:

Table 8: Session Overall Dashboard-Displays visualizations on the overall details of encrypted traffic.

Visualizations	Details
Total Intercepted Sessions	Displays overall count of intercepted sessions by the node over time period. This page does not display per engine unless specified by a filter.
Sessions Trend	Displays the trend of all Inline TLS/SSL session that has been received over a specified time period and per specified GigaSMART engines. The trend included the visualization of the Intercepted/Decrypted/Non-SSL Sessions.
Average Decryption Rate	Displays the average rate of Inline TLS/SSL sessions that have been decrypted over the specified time period..
Average CPU	Displays an average CPU utilization of all engines in Session Overall Page.
Client TLS Version Trend	Displays an overview of the incoming traffic's TLS version of the incoming data.

Visualizations	Details
Server TLS Version Trend	Provides an insight into the TLS version distribution at the server side.
Policy based Intercepted Session	Displays the trend of decryption status of Inline TLS/SSL session based policy.
Intercepted Sessions By Policy Rules	Displays the trend of Inline TLS/SSL session based on Policy rules such as; Domain ,Category, Issuer, URL Cache Miss, Network and Default. NOTE: The no. of sessions that gets matched to a Network Policy Rule will not be displayed in the Total Intercepted Session widget.

Table 9: Session Engine Overview Dashboard-Displays visualizations related to Inline TLS/SSL Sessions per Engine

Visualizations	Details
Sessions Rate per Engine	Displays the rate at which Inline TLS/SSL sessions are intercepted per engine.
Average Decryption Rate per Engine	Displays the average rate of sessions that got decrypted per engine.
Average CPS per Engine	Displays the average Connections per Second (CPS) performance metric per engine.
Average CPU per Engine	Displays the average CPU utilization per engine.
Engine Metric Table	Displays the Decryption rate per engine, average CPS and average CPU rate in a tabular format. The details are displayed as Host Name/Engine ID. For example; FHA-HC1 (Host Name)_1/3/e11(GSEngine ID)

Table 10: Traffic Insights Dashboard-Displays visualizations related to the traffic that is handled with a Inline TLS/SSL sessions

Visualizations	Details
Client and Server Throughput (bps)	Displays the traffic throughput that is received from the client and the throughput that is handled at the server side. This throughput is displayed in bits per second (bps)value.
Overall Volume(Bytes)	Displays the volume of traffic that is being handled in Bytes. This takes into account both TCP and SSL sessions.

Visualizations	Details
Overall Decrypted Volume (Bytes)	Displays the overall decrypted volume of all engines unless filtered by engine ID control filter in Bytes unit
Average CPU Per Engine	Displays the average CPU performance per engine
Max CPU Per Engine	Displays the maximum CPU utilization that was observed per engine. This is static rate and is not displayed based on a time frame.
Max CPS Per Engine	Displays the maximum Connection Per Second (CPS) rate that was observed per engine. This is static rate and is not displayed based on a time frame.
Average & Peak value of CPU & CPS	Displays the average and peak values of CPU and CPS observed per engine in a tabular format.
CPU Trend per Engine	Displays a trend of CPU utilization that was achieved over a time period per engine.
CPS Trend per Engine	Displays a trend of the Connections per Second that was achieved over a time period per engine.
CPS Trend & CPU Trend Correlation	Displays a correlation between the CPU and CPS trend of the engine within a time period.
Throughput Trend on Network	Display the throughput trend of traffic that was received from both client and server side.
Throughput Trend on Tool	Displays the throughput trend of traffic that was received on the Tool.

Table 11: Certificate Insights Dashboard-Provides mTLS-focused certificate visibility for Inline TLS/SSL sessions, showing how server and client certificates—and their revocation status

Visualizations	Details
Server Certificate Trends	Displays how server certificate usage and status evolve over time across Inline TLS/SSL sessions.
Client Certificate Trends	Displays how client certificate usage and status evolve over time for mTLS enabled Inline TLS/SSL sessions.
Server Certificate OCSP Trend	Displays the trend of OCSP revocation-check results for server certificates (for example, good, unknown, or failed) over time in mTLS sessions.

Visualizations	Details
Client Certificate OCSP Trend	Displays the trend of OCSP revocation-check results for client certificates over time in mTLS sessions.
Server Certificate CRL Trend	Displays the trend of CRL based revocation-check results for server certificates over time.
Client Certificate CRL Trend	Displays the trend of CRL based revocation-check results for client certificates over time in mTLS sessions.

Table 12: Engine Diagnostics Dashboard-Displays the certificates and SSL alerts related to a GigaSMART engine

Visualizations	Details
Certificates verified in Cache	Displays the number of certificates that were verified in cache over a time period
SSL Alerts	Displays the number of SSL alerts that were received both from client and server.

Advanced Dashboards

Advanced Dashboards are available only if you enable it while configuring your Inline TLS/SSL Decryption session.

Refer the following sections for more details:

- [System Requirements to configure Inline TLS/SSL Advanced Dashboards](#)
- [Rules and Notes](#)
- [Configure Advanced dashboard](#)
- [View Inline TLS/SSL Dashboards](#)

System Requirements to configure Inline TLS/SSL Advanced Dashboards

The system requirements for utilizing Inline TLS/SSL Advanced Dashboards are as shown below.

Requirements	Support up to 100 Devices (GigaVUE-FM Standalone)	Support up to 100 Devices (GigaVUE-FM HA Mode)
Memory	128GB	128GB
Virtual CPU	Minimum 12 CPU NOTE: It is recommended to have 16 CPU for continuous traffic with maximum supported limit of 18k sessions/second for three Advanced Statistics enabled GigaSMART engines.	Minimum 12 CPU NOTE: It is recommended to have 16 CPU for continuous traffic with maximum supported limit of 36k sessions/second for six Advanced Statistics enabled GigaSMART engines.
Disk Space	Refer to "Large Configuration" category under "Virtual Computing Resource Requirement in Scaled Environments" section in GigaVUE-FM Installation and Upgrade Guide for disk space details.	Refer to "Large Configuration" category under "Virtual Computing Resource Requirement in Scaled Environments" section in GigaVUE-FM Installation and Upgrade Guide for disk space details.
Virtual Network Interface	1	1
Number of GigaVUE-FM nodes	1	3

Rules and Notes

Keep in mind the following rules and notes when using the Advanced Dashboard:

- Advanced Dashboard data will be retained only for 24 hours.
- For a standalone GigaVUE-FM node, the Advanced Dashboard is available for a maximum of three GigaSMART engines.
- In a GigaVUE-FM High Availability group with three GigaVUE-FM nodes, a maximum of eight GigaSMART engines will be supported.
- Configure NTP time sync or ensure that your device and GigaVUE-FM are synchronized with the date and time zone.

Configure Advanced dashboard

To configure advanced dashboards:

- Go to, **Traffic**  **>Configuration Canvas >Select the device>Inline SSL APP.**
- Enable the toggle option **Advanced Session Statistics.**

View Advanced Dashboards

You can use the below control filters and specify the time period to visualize and filter the dashboard information:

- Host Name
- GigaSMART Engine ID (GSEngine ID)
- URL (Only for Session Table Dashboard)
- Source IP
- Destination IP
- URL Category (Only For Session Table Dashboard)

The following are the advanced dashboards and its visualizations:

Table 13: Session Insight Dashboard-Displays visualizations on the details of an Inline TLS/SSL session.

Visualizations	Details
Decryption Status	Displays the number of Inline TLS/SSL sessions that were decrypted and not decrypted.
SSL Mode	Displays the distribution of TLS/SSL Session modes. The modes are as follows: • TLS/SSL Outbound- : Sessions decrypted due to ISSL inbound deployment. • TLS/SSL Inbound-Sessions decrypted due to ISSL outbound deployment. • TLS/SSL Bypass- The session mode that is neither inbound or outbound. • Non-SSL - TCP sessions that are not an TLS/SSL session.
SSL State	Displays the distribution of TLS/SSL Session statuses.
Policy Match By Rules	Provides an insight into the TLS/SSL session that matches the Policy Rules. NOTE: The Policy Rule CATEGORY indicates the URL category.
TLS Version	Displays the TLS version of the sessions. NOTE: The counter “Bypass/Error” denotes sessions that were not able to determine the TLS version.
Top URLs (Max 10)	Displays the top 10 URLs that were accessed during the Inline TLS/SSL Session.
Top URL Category (10 Max)	Displays the Category of top 10 URLs accessed in Inline TLS

Visualizations	Details
	sessions NOTE: 'Uncategorized' signifies SNIs that could not be categorized or Non TLS sessions. NOTE: 'Unknown' signifies TLS Bypass and IP address based URLs.
Top Ciphers (Max 10)	Displays the top 10 Ciphers that performed the Inline TLLS/SSL Decryption.
Certificates by Type	Displays the certificates received are valid or non-valid.

Table 14: Session Table Dashboard-Displays visualizations related to Inline TLS/SSL Sessions per Engine in a tabular format.

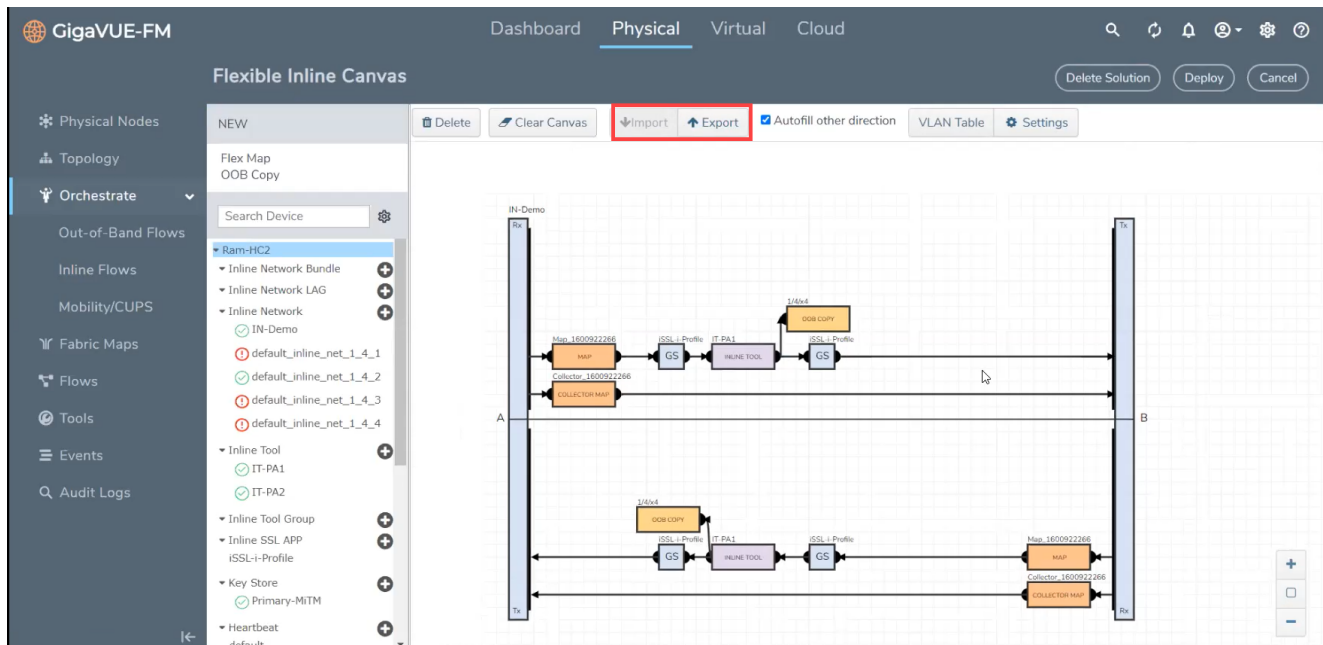
Visualizations	Dashboard
Session Debug Table	Displays the entire Sessions Debug details throughout the system that has enabled Advanced Session Statistics. Each field can be added or removed as a customized filter option by using   button.
Session Policy Debug Table	Displays the entire Sessions Policy Debug details throughout the system that has enabled Advanced Session Statistics. It points out to the policy rules that got matched or the policy verdict of Decryption or non decryption. Each field can be added or removed as a customized filter option by using   button.

The flexible inline canvas allows you to import and export a flexible inline solution. The exported solution gets downloaded in to your local folder as an YAML file, which can be imported and deployed again in the following scenarios:

- Retrieve a solution that was deleted unintentionally
- Deploy the solution in another device
- Re-deploy a solution in the device after GigaVUE-FM is upgraded to a new version (in case of issues in the existing solution)

The downloaded YAML file contains the following information:

- Software version of the GigaVUE-FM instance and the device on which the solution was created
- Member, port and configuration information of the various inline configurations such as the Inline Network Alias, Member Ports, Inline Tool Group Alias, and other such details.



Import and Export Flexible Inline Solution — Rules and Notes

- When deploying a solution after GigaVUE-FM is upgraded to a new version, the source port in the target device must not have been used in any solution.
- When importing an YAML file, the following configurations specified in the YAML file must match the configurations in the target device:
 - Inline network alias
 - Inline network bundle alias
 - Inline tool alias
 - Inline network LAG alias
 - Inline SSL App alias

Import and Export a Flexible Inline Solution

To import a file, ensure you have the .YAML file ready of the flexible Inline solution:

1. Click the **Import** on the canvas.
2. Select the .YAML file, containing the required flexible inline solution, saved in your local folder. The solution appears in the canvas.
3. Click **Deploy** to deploy the solution, again.

You can also edit an imported solution on the canvas, and re-export the same as a new solution.

To export a solution, from the Flexible Inline Canvas select the solution:

1. Click the **Export** button. The solution is downloaded as an YAML file.
2. Save the file to the required location.

Backup and Restore Flexible Inline Flows

You must backup the devices and GigaVUE-FM at the same time. Ensure that the devices are not undergoing configuration edits during backup or restore. For more information, refer to the “*Restore Devices and GigaVUE-FM for Traffic Management Solutions*” section in the “*GigaVUE Administration Guide*”.

Troubleshoot Inline TLS/SSL Decryption Solution Issues

In the **Inline Flows** page, select the required device for which you want troubleshoot. Click the **Troubleshoot** button to view more on the below map configuration details for the ICAP Client app:

- Map Alias
- From
- To
- GSOP

The Troubleshoot tab provides details about the device-level maps that are created for the selected inline network. The details include the source of the map, inline tools or inline tool groups used in the A to B and B to A directions, tool side and network side VLAN tags, and OOB copies. Click the required component to view its configuration details. It also provides details about the map statistics. In case of inline tool group, you can view the list of inline tools that are associated with the inline tool group. Click the required inline tool from the list to view its configurations. Refer to the following figure for details.

To troubleshoot any issue or failure in your flexible inline flow:

1. From the flexible inline canvas, go to the **Status** tab to check the forwarding states of the required inline network.
2. Go to the **Statistics** tab to check the port statistics to ensure that there are no drops, errors, or discards.

NOTE: Click the **Statistics** tab again to refresh the data.

3. Go to the **Troubleshoot** tab to check the required map configurations and isolate the issue.

Example: Troubleshoot Traffic Issues Between Side A and Side B

This section provides you an example of how to troubleshoot a specific issue using the flexible inline canvas.

Consider that you have an inline network IN1 with one by-rule map and one collector map. The traffic is not flowing from Side A to Side B. To troubleshoot this issue:

1. Go to **Physical > Inline Flows**.
2. Select the required device, and then drill down to the inline network that has the traffic issue.
3. Click **Status** to view the forwarding states of the inline network. Ensure that the forwarding state of the inline network is Normal. For details of the forwarding states, refer to [View the Forwarding States of Inline Networks](#).
4. Click **Statistics** to view the total packet count of the inline network. The Rx count of Port A of the inline network must match the Tx count of Port B. If the count does not match, the traffic is blocked between Port A and Port B.

NOTE: To refresh the statistical data, click **Statistics** again.

5. Click **Troubleshoot** to view the configurations of the by-rule and collector maps configured for the inline network.
 - a. Check that the by-rule map has packet count.
 - b. If the by-rule map has packet count, check the inline tools from A to B and B to A directions of the by-rule map to ensure that the inline tools are in up state and the **Flex Traffic Path** is set to **To inline tool**.
6. Click **Statistics** to view the port statistics of the required inline tool. If the Rx count of Port A of the inline tool does not match the Tx count of Port B of the inline tool, the traffic is dropped at the inline tool. Check the inline tool and take the required action.
7. If the Rx count of Port A of the inline tool matches the Tx count of Port B of the inline tool, repeat steps 5 and 6 for the collector map configured for the inline network.
8. If the Rx count of Port A of the inline tool configured for the collector map matches the Tx count of Port B of the inline tool, contact Gigamon Technical Support.

Inline Configurations using Inline Bypass Solutions (Classic)

This chapter provides the following information about inline bypass solutions:

- [Inline Bypass Solutions](#)
- [Configure Inline Bypass](#)

Inline Bypass Solutions

Security tools such as firewalls and intrusion protection systems (IPSs) are often connected inline on production networks, with traffic flowing from the network segment through the tool and then back onto the production network.

Inline bypass solutions involve bidirectional traffic between two networks, intercepted by a Gigamon node, and guided through one or more inline tools.

Inline bypass is a pillar of the GigaSECURE Security Delivery Platform.

Inline bypass is supported on GigaVUE-FM, GigaVUE HC Series® HC Series nodes: GigaVUE-HC3, GigaVUE-HC1 and GigaVUE-HC1-Plus.

This section describes inline bypass solutions. Refer to the following sections for details:

- [Introduction to Inline Bypass Solutions](#)
- [Logical Bypass and Physical Bypass](#)
- [Types of Inline Networks](#)
- [Simple and Complex Inline Bypass Solutions](#)
- [Types of Inline Networks](#)
- [Inline Network Groups](#)
- [Inline Tools](#)
- [Heartbeats](#)
- [Inline Tool Groups](#)
- [Inline Serial Tools](#)
- [Associate Inline Networks with Inline Tools Using Inline Maps](#)
- [Configure Inline Bypass](#)

NOTE: The configuration of inline bypass solutions can be complex. Follow the order of configuration outlined in [Configure Inline Bypass](#) and demonstrated in [Inline Bypass Solution Examples](#).

Introduction to Inline Bypass Solutions

Inline bypass solutions place the Gigamon node inline between two sides of a network. The Gigamon node sends uninspected traffic from one side of the network to an inline tool (such as an IPS), and then sends the inspected traffic to the other side of the network.

The reasons for deploying Gigamon's inline bypass solutions are as follows:

- to protect against inline tool failures (including loss of link to inline tools and any inline tool problems detected through heartbeat monitoring)
- to bypass the inline tools for traffic that does not need to be examined by the tools or that cannot be processed by the tools
- to distribute the traffic load among multiple tools
- to send specific traffic to specialized inline tools
- to guide traffic serially through the inline tools, with the traffic from one tool flowing to the next, so that all tools see the same traffic
- to share inline tools among multiple inline network links
- to implement tiered network security by combining inline and out-of-band, allowing the traffic to be examined by both types of tools

For improved reliability and ease of maintenance, the inline bypass solutions also provide the following:

- protection against power loss through physical bypass
- protection against power loss through the high availability solution, Gigamon Resiliency for Inline Protection (GRIP™)

Capabilities of Inline Bypass Solutions

The Inline Bypass solution offers the following capabilities:

- Guides traffic through one or more inline tools according to user-defined bidirectional connectivity arrangements among respective inline network ports and inline tool ports.
- Reacts to failure conditions, such as the failure of inline tools, or the failure of links leading to the end-point devices between which the inline tool is inserted.
- Configures maps to associate inline networks with inline tools and inline tool groups.

- Supports bidirectional heartbeat and negative heartbeat to monitor inline tool health.
- Supports protected and unprotected inline networks.
- Supports physical bypass with specialized hardware on GigaVUE-HC3, , GigaVUE-HC1 and GigaVUE-HC1-Plus(bypass combo modules equipped with optical protection switches)
- Supports physical bypass on and GigaVUE-HC1 (TAP modules equipped with electrical relays).
- Distributes traffic across multiple inline tools, providing load sharing and traffic redistribution in the event of a tool failure.
- Supports out-of-band maps for selective forwarding of inline traffic to monitoring tools.
- Supports the sharing of inline tools by multiple inline networks.
- Supports N+1 and 1+1 inline tool redundancy for inline tool groups.
- Supports guiding inline traffic through inline tools in a serial fashion.
- Supports inline Flow Mapping® through rule-based and shared collector inline maps.
- Provides a high-availability solution, Gigamon Resiliency for Inline Protections (GRIP).

Logical Bypass and Physical Bypass

Logical bypass lets traffic bypass the inline tool should it experience a failure. A failure is declared if the GigaVUE-FM,GigaVUE HC Series node either loses connectivity to the inline tool or fails to receive a heartbeat from the tool.

Logical inline bypass does not require any specialized hardware and can be facilitated on regular ports on GigaVUE-HC3, GigaVUE-HC1 and GigaVUE-HC1-Plus modules. On GigaVUE-HC1, logical inline bypass can be configured on the base module.

Physical bypass provides protection against failure of the GigaVUE-FM,GigaVUE HC Series node, such as if power is lost. On GigaVUE-FM,GigaVUE HC Series® HC Series nodes, it is implemented with specialized hardware called bypass combo modules.

The specialized hardware triggers a bypass when power is lost to the node. When the physical bypass is activated, traffic flows from one side of the network to the other, but without monitoring.

The GigaVUE-HC3 bypass combo module is a bypass switch (BPS) module, as follows:

- Bypass Combo Module with two 100Gb/40Gb SR4 MPO inline network port pairs and sixteen regular SFP+ (10Gb) port cages (BPS-HC3-C25F2G)
- Bypass Combo Module with two 40Gb or 100Gb LR4 inline network port pairs and sixteen 10Gb/25Gb cages (BPS-HC3-Q35C2G, and BPS-HC3-C35C2G).

The GigaVUE-HC1 bypass combo module is a bypass switch (BPS) module, as follows:

- Bypass Combo Module with two SX/SR (50/125µm multimode) inline network port pairs and four regular SFP+ (1Gb/10Gb) port cages (BPS-HC1-D25A24)
- Bypass Combo Module with six single-mode LR 1Gb/10Gb inline network port pairs BPS-HC1-D35C60 (LX/LR) and BPS-HC1-D25A60 (SX/SR) .

The following bypass modules are available for the GigaVUE-HC1-Plus:

- Bypass Combo Module with two SX/SR (50/125µm multimode) inline network port pairs and four regular SFP+ port cages (BPS-HC1-D25A24). It requires GigaVUE-HC1-Plus to be running software version 6.3 or higher. It provides both physical and logical inline bypass, with automatic failover protection in case of power failure. The ports can operate at 1Gb/10Gb speeds and can be configured as any port type
- Bypass modules with six inline network port pairs each, supporting multi-mode SR and single-mode LR, respectively, at 1Gb/10Gb speeds (BPS-HC1-D25A60 (SX/SR) and BPS-HC1-D35C60 (LX/LR)).

All these modules are hot-swappable and provide physical bypass protection, ensuring network continuity in the event of a power failure or module removal. The BPS modules provide optical bypass, while the TAP-HC1-G10040 provides copper bypass functionality.

Physical bypass is also supported on the following copper TAP modules on GigaVUE-HC1 and GigaVUE-HC1-Plus:

- On the GigaVUE-HC1 copper TAP module, TAP-HC1-G10040
- On the GigaVUE-HC1-Plus copper TAP module with 8 x 1Gb ports for either four TAPs or bypass copper (BPC) port pairs (TAP-HC1-G10040). It can be used as a copper bypass module, providing protected inline networks for copper ports. It requires GigaVUE-OS version 6.4 or higher.

The GigaVUE-HC3, GigaVUE-HC1 and GigaVUE-HC1-Plus offer physical and logical inline bypass. Physical bypass provides automatic failover protection in the case of a power failure. On the GigaVUE-FM, GigaVUE HC Series nodes, the bypass combo modules provide the physical bypass function. Or on GigaVUE-HC1, the copper TAP modules provide the physical bypass function.

The physical bypass function, as it applies to a single pair of inline network ports, is as follows:

- When the module is not powered, (either the entire node is powered down or the module is removed from the node), the inline network port pair is in the physical bypass mode. That means that traffic is exchanged directly between network Port A and network Port B of the inline network pair.

- When the module is powered, the mode (inline or bypass) of the inline network port pair is controlled through software. In the physical bypass mode, the inline network port pair behaves exactly as if the module was not powered. In the inline mode, the inline network port pair behaves as any other inline network port pair configured for working with an inline tool.

For information on the bypass combo module on GigaVUE-HC3, refer to the *GigaVUE-HC3 Hardware Installation Guide*. This document also contains procedures for installing, removing, and replacing modules in the GigaVUE-HC3.

For information on the bypass combo module or the TAP-HC1-G10040 module on GigaVUE-HC1, refer to the *GigaVUE-HC1 Hardware Installation Guide*. This document also contains procedures for installing, removing, and replacing modules in the GigaVUE-HC1.

For information on the bypass combo module on GigaVUE-HC1-Plus, refer to the *GigaVUE-HC1-Plus Hardware Installation Guide*. This document also contains procedures for installing, removing, and replacing modules in the GigaVUE-HC1-Plus Hardware Installation Guide.

Refer also to [Figure 29 Physical Bypass Protection](#) and [Protected Inline Network](#).

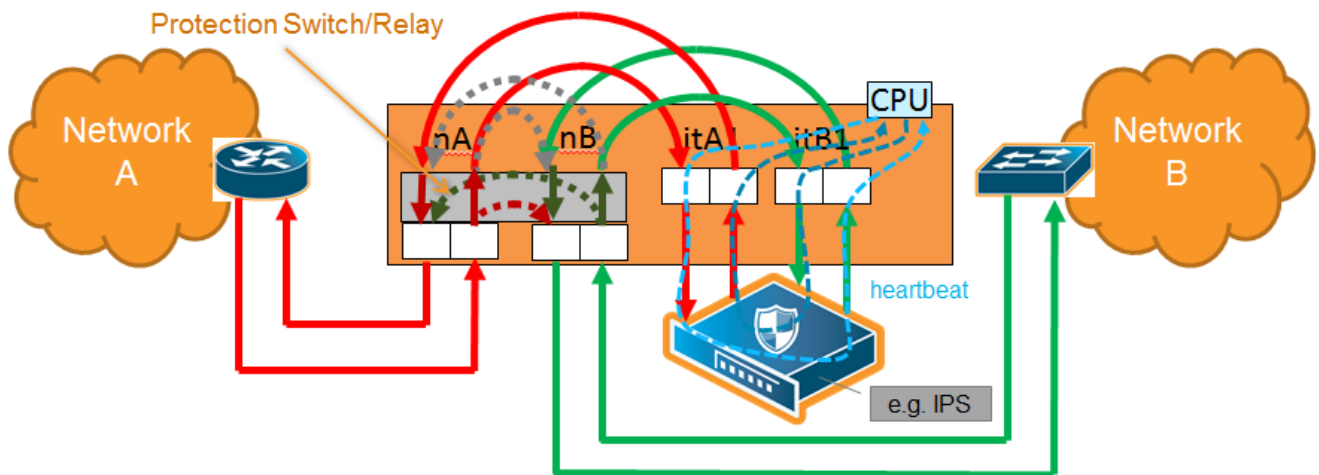


Figure 29 Physical Bypass Protection

Simple and Complex Inline Bypass Solutions

Simple and complex inline bypass solutions are described in the following sections:

- [Typical Configuration](#)
- [Distribution to Multiple Inline Tools](#)
- [Inline Tools in a Series](#)

- Multiple Inline Networks
- Inline Flow Mapping®
- Send Traffic to Out-of-Band Tools

Typical Configuration

In the typical or most common configuration, a single inline tool is inserted in a Network A to Network B link. All traffic is sent to the inline tool and inspected in both directions.

A typical configuration is shown in [Figure 30 Simple Configuration](#). The physical protection switch is optional and present only when using bypass combo modules or copper TAP modules.

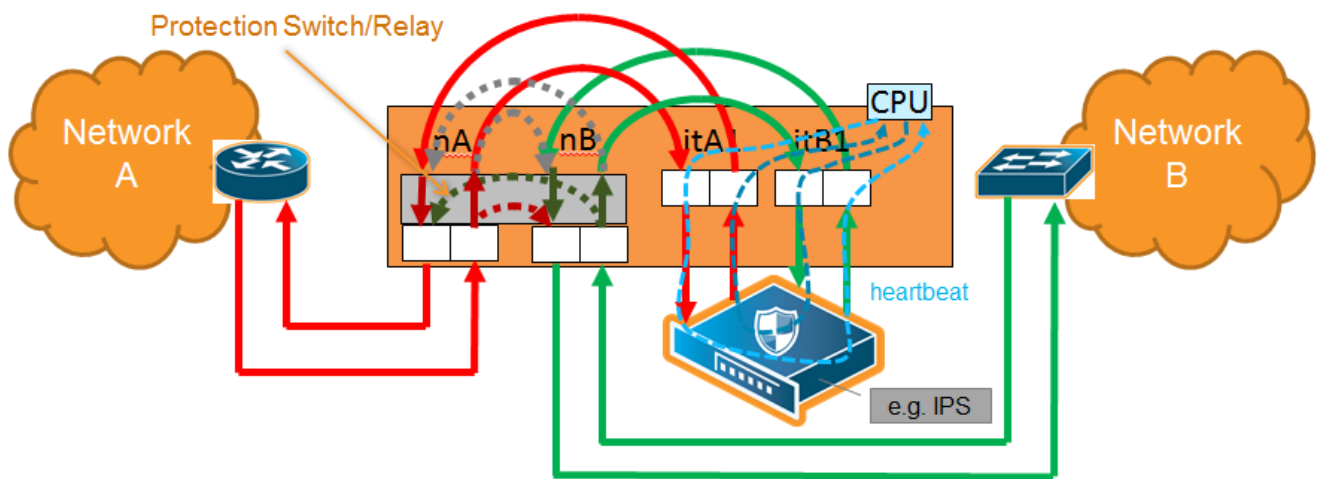


Figure 30 Simple Configuration

Distribution to Multiple Inline Tools

One of the challenges to inline monitoring is scaling the throughput of the inline tools with the speed of the network. One way to do this is to share the load across multiple inline tools.

Because inline inspection of network traffic is processor-intensive, it is common to combine the power of multiple inline tools to monitor traffic. This is especially true for 10Gb, 40Gb, and 100Gb networks and tools that only support 1Gb or 10Gb interfaces.

An inline tool group is an arrangement of multiple inline tools which share the traffic load. Traffic is sent to the tools based on standard hashing parameters. This is referred to as hash-based distribution. If a single tool in the group of tools fails, the packets will be redistributed to other tools. This ensures that all packets are inspected.

A multiple inline tool arrangement is shown in [Figure 31 Multiple Tool Arrangement](#).

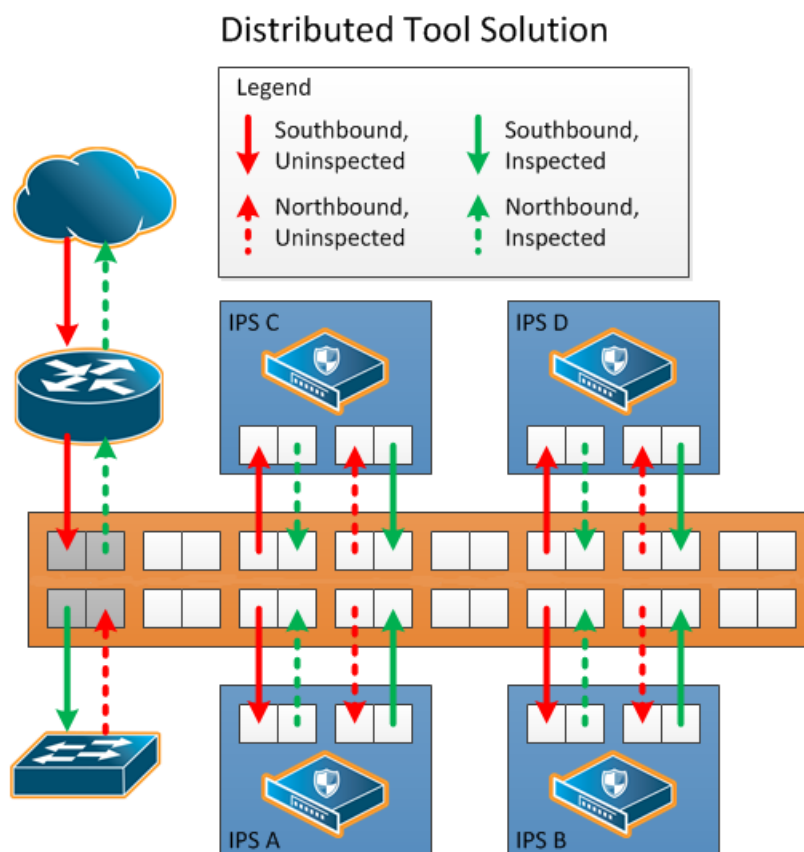


Figure 31 Multiple Tool Arrangement

Multiple tool distributions can be non-redundant or have 1+1 or N+1 redundancy. [Inline Tool Groups](#)

Inline Tools in a Series

Tools can form an inline series, in which the traffic from one tool flows to the next, so all tools see the same traffic.

Refer to [Figure 32 Inline Tool Series](#) for an inline tool series. In [Figure 32 Inline Tool Series](#), traffic is only shown from A-to-B.

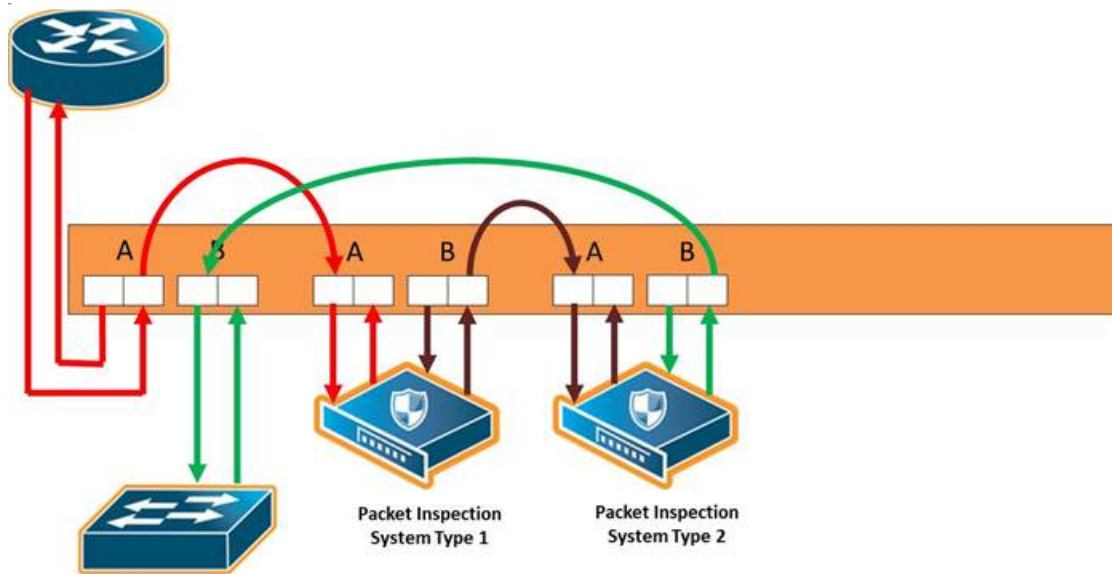


Figure 32 *Inline Tool Series*

For more information on inline tool series, refer to [Inline Tools in a Series](#).

Multiple Inline Networks

An inline network group is an arrangement of multiple inline networks that share the same inline tool, inline tool group, or inline tool series. The numbers of networks to tools can be many-to-one as shown in [Figure 33 Inline Network Group](#) or many-to-many. Traffic is guided to a particular inline network through internal VLAN ID tagging.

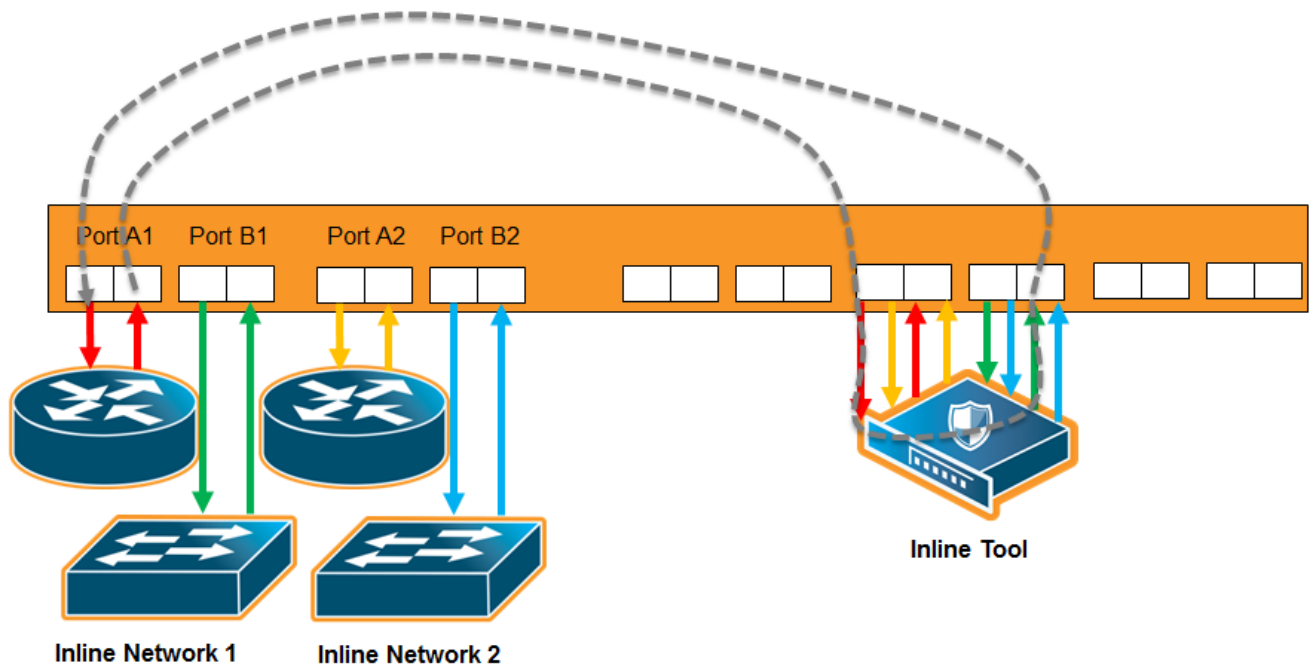


Figure 33 *Inline Network Group*

For more information on inline network groups, refer to [Inline Configurations using Inline Bypass Solutions \(Classic\)](#).

Inline Flow Mapping®

Some tools are optimized for particular inline traffic. With inline flow mapping, the GigaVUE-FM, GigaVUE HC Series node forwards packets to different inline tools based on criteria, such as TCP/UDP port number, or any other rule that can be defined in a map. Using these map rules, selected traffic can be sent to specific tools.

When inline flow mapping is combined with distribution to multiple tools, one application, such as Web traffic, can be sent to one tool or group of tools, while another application, such as email traffic, can be sent to another tool or group of tools. If there is traffic, such as encrypted traffic, that does not need to be or cannot be inspected, it can be bypassed.

An inline flow mapping based traffic distribution is shown in [Figure 34 Inline Flow Mapping® Based Traffic Distribution](#). In [Figure 34 Inline Flow Mapping® Based Traffic Distribution](#), traffic is only shown from A-to-B.

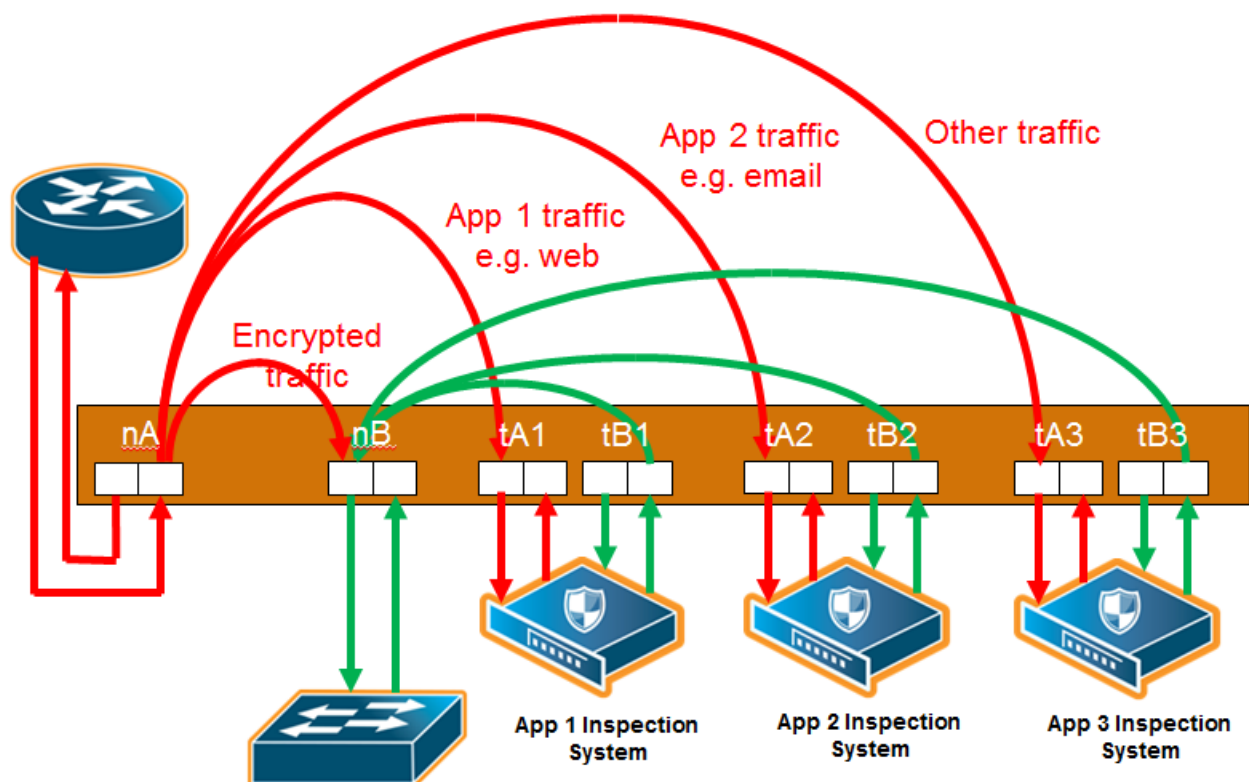


Figure 34 *Inline Flow Mapping® Based Traffic Distribution*

Send Traffic to Out-of-Band Tools

Traffic can be sent to out-of-band (OOB) tools. Any port used for inline functionality can be used as a source for a map to an out-of-band tool. This includes any inline network port or inline tool port. For example, you can use inline tool ports to inspect packets that have passed through the IPS.

An out-of-band arrangement is shown in [Figure 35 Out-of-Band Arrangement](#).

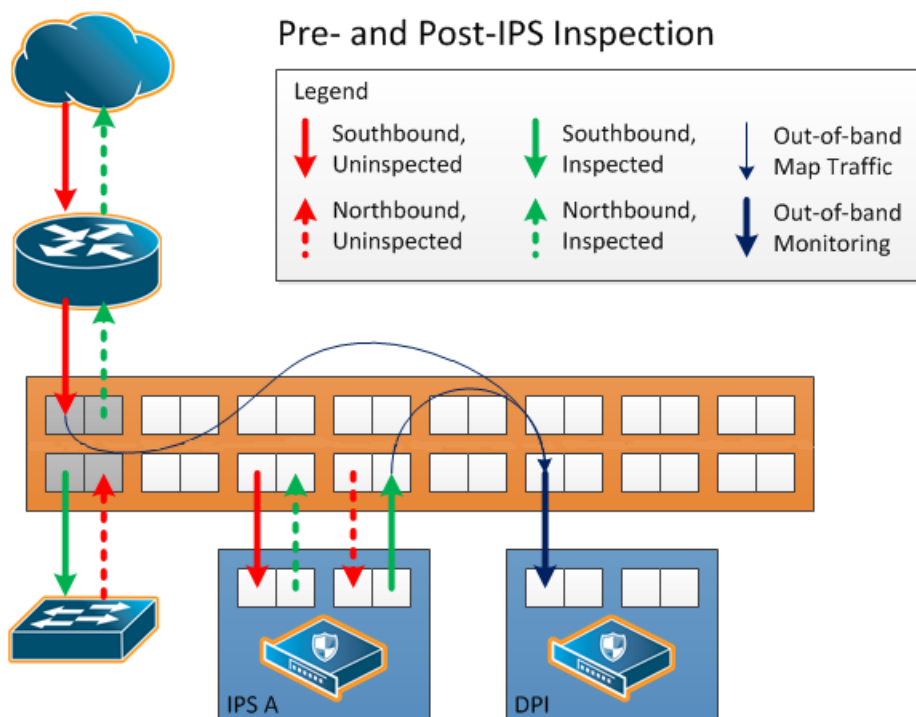


Figure 35 Out-of-Band Arrangement

Types of Inline Networks

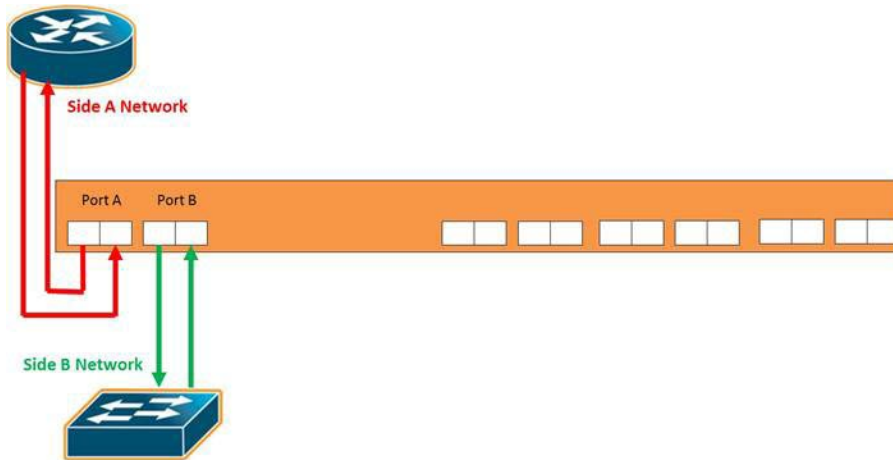
The types of inline networks are described in the following sections:

- [Unprotected Inline Network](#)
- [Protected Inline Network](#)
- [Mix of Protected and Unprotected](#)

Unprotected Inline Network

An unprotected inline network consists of two ports of the inline-network type, which facilitate access to a bidirectional link between two networks (or more precisely, two far-end network devices).

Any available network type ports on a GigaVUE-FM, GigaVUE HC Series HC Series node can be configured to be inline-network type ports and combined to form an unprotected inline network. An unprotected inline network is shown in the following figure.



Inline Network Groups

Use the **Inline Network Group** configuration page to configure an inline network group. An inline network group is an arrangement of multiple inline networks that share the same inline tool or tools. Use this page to specify the list of inline networks in the inline network group.

The inline network ports that make up the inline networks participating in the inline network group are always in pairs, running at the same speed, on the same medium (fiber or copper). All inline network ports of the inline network group must be on the same GigaVUE-HC3, or GigaVUE-HC1 or GigaVUE-HC1-Plus node. The inline networks participating in the inline network group can be different speeds and different mediums.

An inline network group can share an inline tool, or tools in an inline tool group or inline tool series. Many-to-one means from an inline network group to an inline tool and is shown in [Figure 36 Inline Network Group Many-to-One](#). Many-to-many means from an inline network group to an inline tool group or inline tool series.

Figure 36 *Inline Network Group Many-to-One*

When an inline tool or inline tool group is configured between several pairs of networks, each pair operates independently of the others. The traffic coming from the inline tool or tools must be segregated into individual substreams according to the traffic source.

For example, the traffic that came into the GigaVUE-FM, GigaVUE HC Series node on inline network port net_A_3 must be sent through inline network port net_B_3 (with net_A_3 and net_B_3 belonging to the same inline tool that is the third member of the inline tool group). Refer to [Figure 37 Inline Tool Inserted in Multiple NetA-NetB Links](#).



Figure 37 Inline Tool Inserted in Multiple NetA-NetB Links

To accomplish the segregation, packets are tagged coming from an individual side A inline network port before they are sent to the inline tool or tools. When tagged packets come back from the inline tool or tools, the tag identifies the respective side B inline network port through which the packets should be sent. The tags are removed before the packets are sent through the side B inline network ports.

Traffic is guided to a particular inline network through internal VLAN ID tagging. This VLAN tagging affects packets only on their way from inline tool ports to the attached inline tool and back from the attached inline tool to the inline tool ports. The packets sent out from inline network ports remain untagged. Refer to [Figure 36 Inline Network Group Many-to-One](#).

NOTE: Internal VLAN ID tagging creates hidden VLAN ID tags. Explicit VLAN ID tagging is not needed, however starting in software version 4.6, explicit VLAN tagging is also available. Refer to [Configurable VLAN Tagging](#).

Inline Tool Sharing

Inline network groups require inline tool sharing to be enabled on the inline tool or the members of the inline tool group or inline tool series specified in the inline map.

When shared is enabled (true), the inline tool can receive traffic from multiple sources (the inline networks in the inline network group) and can be used in a map in which the source is an inline network group.

An inline tool group or inline series does not have its own shared setting. The shared setting is derived from the inline tools. Therefore all the members in an inline tool group or inline series must have the same setting. For example, if an inline tool group has three inline tool members, the shared setting of all three inline tools must be the same.

Configurable VLAN Tagging

Explicit VLAN tagging for inline network groups can be configured. For example, you can use VLAN tags for managing policies. A mixture of internal and explicit VLAN tags is supported.

The VLAN tags are configured on the ports of inline networks. They can be configured at any time, but are only applied when the inline networks are part of an inline network group. Across the inline network group, the VLAN tags must be unique; however, both ports of an inline network can have the same VLAN tag. Refer to [Tools in Bridge Mode](#).

An error message is displayed if the same VLAN tag is used for more than one inline network in an inline network group.

Refer also to [Ingress and Egress VLAN](#).

NOTE: For inline SSL decryption, the inline network group does not support ingress VLAN tagging on the member links.

For out-of-band maps from inline network group ports or inline tool ports mapped from an inline network group, the out-of-band tool ports will receive the following:

- tagged packets, if they originally come from an inline network port with an ingress VLAN tag configured
- untagged packets, if they originally come from an inline network port without an ingress VLAN tag configured

Add VLAN Tag

The following are the steps for adding a VLAN Tag.

1. Go to **System > Ports > Ports > All Ports**.
2. Select the port to configure as an inline network port and click Edit.
3. Set the following parameters to configure an inline network port with VLAN tagging:
 - Select **Inline Network** or **Network** for Type.
 - Enter a VLAN ID in the **VLAN Tag** field.
4. Click **Save**.

Tools in Bridge Mode

The same VLAN tag can be assigned to both ports in an inline network port pair.

The following example configures the same ingress port VLAN tag on the net-a and net-b ports of an inline network. When the net-a and net-b ports have the same VLAN tag, an inline tool will send packets back to the network from which it came.

1. Go to **System > Ports > Ports > All Ports**.
2. Configure the net-a port.
 - a. Select the port (for example, 1/1/x17) and click **Edit**.
 - b. Enter inline-network-port-a in the **Alias** field.
 - c. Select **Inline Network** for **Type**.
 - d. Enter 123 in the VLAN Tag field.
 - e. Click **Save**.
3. Configure the net-b port.
 - a. Select the port (for example, 1/1/x18) and click **Edit**.
 - b. Enter inline-network-port-a in the **Alias** field.
 - c. Select **Inline Network** for **Type**.
 - d. Enter 123 in the VLAN Tag field.
 - e. Click **Save**.
4. Configure the Inline Network.
 - a. Select Inline **Bypass > Inline Networks**.
 - b. Click **New**.
 - c. Enter an alias in the **Alias** field.
 - d. Select port 1/1/x17 for Port A.
 - e. Select port 1/1/x18 for Port B.
 - f. Click **Save**.

Inline Tools

There are two meanings to the term inline tool. The inline tool software construct consists of a pair of inline tool ports plus the inline tool attached to the ports. The software construct has attributes that are configured on the GigaVUE-FM, GigaVUE HC Series® HC Series node.

The term inline tool also refers to the pass-through device itself that performs packet inspection and selective forwarding, such as an Intrusion Protection System (IPS). This is a physical device, external to the GigaVUE-FM, GigaVUE HC Series node.

Use the Inline Tool page to configure the inline tool software construct. An inline tool consists of inline tool ports, always in pairs, running at the same speed, on the same medium (fiber or copper). The inline tool ports must be on the same GigaVUE-HC3, or GigaVUE-HC1 or GigaVUE-HC1-Plus node. The inline tool ports must also be on the same GigaVUE-HC3, or GigaVUE-HC1 or GigaVUE-HC1-Plus node as the inline network ports.

Inline tool ports are ports to which inline tools are attached. Inline tool ports are always in pairs, and must have the same line rate. Inline tool ports must be on the same GigaVUE-HC1 node as the inline network ports.

An inline tool consists of a pair of inline tool ports plus the inline tool attached to the ports. Refer to [Figure 38 Inline Tool and Inline Tool Ports](#).

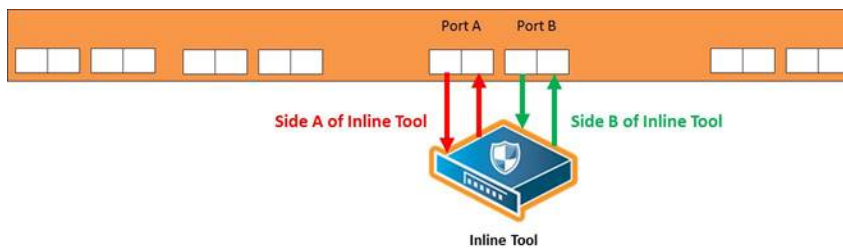


Fig. 3 Inline Tool

Figure 38 *Inline Tool and Inline Tool Ports*

Use the Inline Tools page to display of configuration of inline tools.

Inline Tool Failover Action

One of the parameters of inline tools is failover action, which controls the action taken when a tool is unhealthy or in response to a failure of an inline tool. You can configure one of the following failover actions:

- **ToolBypass**—when the inline tool fails, the traffic that normally was directed to the inline tool is redirected to the bypass path. Use this failover action for configurations involving multiple inline tools associated with an inline network or inline network group using rule-based maps. For configurations using map passalls, tool-bypass is the same as network-bypass.
- **NetworkBypass**—when the inline tool fails, all traffic that would not have been dropped when the inline network or networks had a NORMAL forwarding state is directed to the bypass path. That is, all such traffic arriving at the side A inline

network port or ports is forwarded to the side B inline network port or ports and all traffic arriving at the side B inline network port or ports is forwarded to the side A inline network port or ports.

- **ToolDrop**—when the inline tool fails, the traffic that normally was directed to the inline tool is dropped. Use this failover action for configurations involving multiple inline tools associated with an inline network or inline network group using rule-based maps. For configurations using map passalls, tool-drop is the same as network-drop.
- **NetworkDrop**—when the inline tool fails, all traffic coming to the respective inline network (or inline network group) is dropped.
- **NetworkPortForcedDown**—when the inline tool fails, the inline network ports of the respective inline network (or inline network group) are forced down.

NOTE: However, after the device reload, the inline network ports become operationally up, whereas the inline tool is still down. You need to manually force down the inline network ports.

The default is **ToolBypass**.

The bypass path is between side A and side B of the inline network ports.

Inline Tool Failover Action with Inline Flow Mapping®

When the inline bypass solution uses inline flow mapping, the failover actions of inline tools are as follows:

- **ToolBypass**—when the inline tool fails, the traffic that normally was directed to the inline tool is redirected to the bypass path. The traffic going to the healthy inline tools (through rule-based maps) remains unchanged.
- **ToolDrop**—when the inline tool fails, the traffic that normally was directed to the inline tool is dropped. The traffic going to the healthy inline tools (through rule-based maps) remains unchanged.

Inline Tool Recovery Mode

An inline tool detects failures in the traffic path between port pairs and automatically diverts traffic away to avoid disruption. After an inline tool goes down, the following modes specify how to bring it back up after it has recovered:

- **automatic**—Specifies automatic recovery, which redirects traffic back to the inline tool as soon as it has recovered from all faulty conditions.
- **manual**—Specifies manual recovery, which lets you control when to put an inline tool back into service after the tool has recovered. For example, you may wait for a maintenance window to return the inline tool to service.

The default is automatic.

By selecting the tool and selecting the Recover button, users can set the recovery of the inline tools to manual or automatic.

Refer to [Figure 39 Automatic and Manual Inline Tool Recovery from Failover](#) for automatic and manual inline tool recovery from failover.

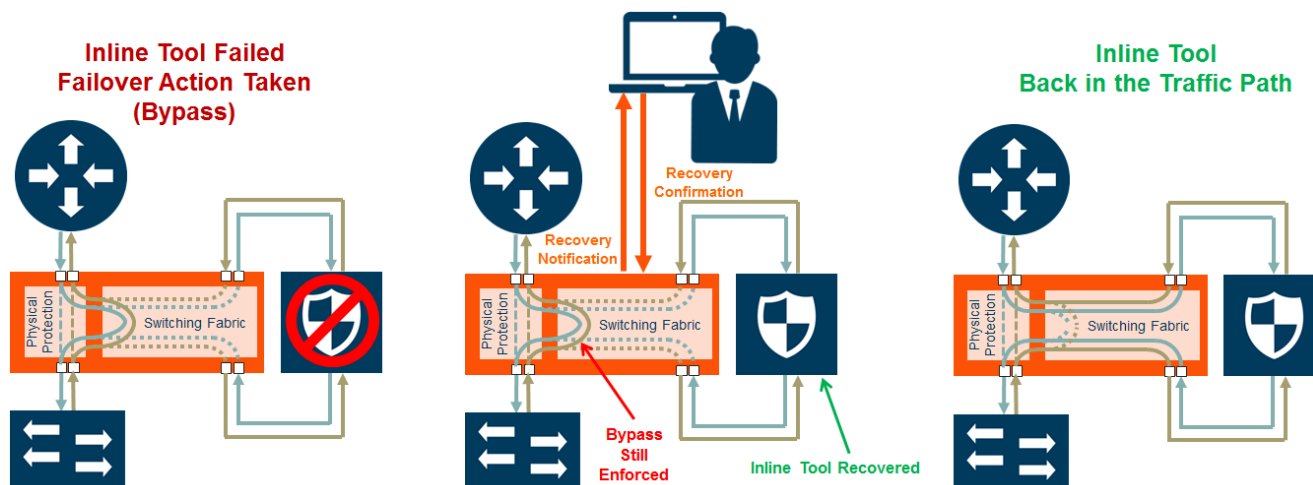


Figure 39 Automatic and Manual Inline Tool Recovery from Failover

The left side of [Figure 39 Automatic and Manual Inline Tool Recovery from Failover](#) shows an inline tool that has failed and the bypass failover action has been executed.

Automatic recovery is shown on the right side of [Figure 39 Automatic and Manual Inline Tool Recovery from Failover](#). When the inline tool recovers, traffic is automatically directed back to it.

Manual recovery is shown in the center of [Figure 39 Automatic and Manual Inline Tool Recovery from Failover](#). When the recovery mode is configured as manual, an SNMP notification, if enabled, will send a notification when the inline tool is ready to be put back into service. The failover action, in this case, bypass, will be enforced until you manually put the inline tool back into service.

When the recovery mode is configured as manual, an SNMP notification, when enabled, will notify you when the inline tool is ready to be put back into service.

Use the following steps to configure notification that will be sent when the inline tool is ready:

1. Select **Settings > SNMP Traps**.
2. Click **Trap Settings**. The Edit SNMP Trap Settings page displays.
3. On the Edit SNMP Trap Settings page, select **Enable** for **Inlinetool Recovery**.
4. Click **Save**.

The default for **Inlinetool Recovery** is disabled.

Use the following steps to put an inline back in service when the recovery mode is manual and the inline tool has an operational state of ready.

1. Select Inline **Bypass > Inline Tools**.
2. On the Inline Tools page, select the inline tool.
3. Click **Recover**.

NOTE: Also use **Recover** after the GigaVUE-FM, GigaVUE HC Series® HC Series node is reloaded or rebooted (even though the inline tool has not failed). Issue the **Recover** on all the inline tools that are configured with manual recovery after a reload or **Actions > Shut Down** from the Chassis page on a selected card in Chassis Table View followed by **Actions > Start Up**. Refer to the “Chassis” section in the *GigaVUE Administration Guide* for more details.

NOTE: In certain circumstances while using classic inline, if the recovery mode is set to "manual" and the inline-tool is in "ready" state, traffic may still be forwarded to the inline-tool ports. This occurs because the recovery state shifts from "ready" to "up" when "inline-tool disable/enable" is used. When the recovery mode for the inline-tool is "manual" and is in "ready" state, do not disable/enable the inline-tool. Instead, disable/enable the port.

The **Inline Tool** page displays the operational state of each inline tool as up, down, disable, or ready. Refer to [Aggregate Inline Tool States](#) for detailed descriptions of the states.

Inline Tool Sharing Mode

Inline tool sharing mode specifies how an inline tool is going to be shared as follows:

- **Enable**—Specifies that the inline tool is going to be shared by different sources.
- **Not enabled**—Specifies that the inline tool will not be shared by different sources.

The default is **not enabled**.

When sharing is enabled, the inline tool can receive traffic from multiple sources (the inline networks in the inline network group) and can be used in a map in which the source is an inline network group.

An inline tool group or inline series does not have its own shared setting. The shared setting is derived from the inline tools. Therefore all the members in an inline tool group or inline series must have the same setting. For example, if an inline tool group has three inline tool members, the shared setting of all three inline tools must be the same.

When an inline tool has sharing mode enabled, the traffic will be VLAN tagged. The connected inline device is expected to receive VLAN tagged packets. When an inline tool does not have sharing mode enabled, the extra VLAN tag is not added.

Go to **Inline Bypass > Inline Tools** and select an inline tool or click **New**. Under Configuration, Inline tool sharing mode, select Enable.

How to Use SNMP Polling to Obtain Inline Tool State

The inline tool state can also be obtained through SNMP polling using an SNMP-compliant network management application or a MIB browser. The names of the MIB files that need to be loaded in order to poll the inline tool state are: GIGAMON-COMMON-SMI and GIGAMONINLINEBYPASS.

The inline tool states are described in [Table 15: Aggregate Inline Tool States](#). They are an aggregate of the inline tool port statuses and the heartbeat status.

Table 15: Aggregate Inline Tool States

Status	Description
up	The heartbeat is up and all the inline tool ports are up. The inline tool is operational and is forwarding traffic to the tool.
down	Either the heartbeat is down or one or more of the inline tool ports are down or disabled. The inline tool is in a failed state and is not ready to recover. The tool is not receiving any traffic.
disable	The inline tool is disabled.
ready	The inline tool is in a failed state but is ready to recover. The tool is not receiving any traffic.

Heartbeats

When heartbeat packets are sent to an inline tool, they are expected to be received back when the inline tool is healthy. Negative heartbeat packets complement heartbeat packets to verify the health of inline tools. When negative heartbeat packets are sent to an inline tool, they are not expected to be received back when the inline tool is healthy.

When some inline tools begin to fail, they allow packets though that should have been dropped. A negative heartbeat detects such a failure by sending a packet that should not pass through an inline tool. If the negative heartbeat packet passes through an inline tool, the tool is deemed to have failed. Therefore, a negative heartbeat packet received back from an inline tool indicates a tool failure.

Heartbeat packets and negative heartbeat packets can be used in any combination: heartbeat only, negative heartbeat only, neither, or both.

Rules and Notes

Keep in mind the following rules and notes when you configure the heartbeat mechanism between GigaVUE nodes:

- The heartbeat mechanism is supported in GigaVUE-HC1, GigaVUE-HC3 and GigaVUE-HC1-Plus devices.
- Negative heartbeat profiles are supported.
- Both standard and custom heartbeat packets are supported.
- Both protected and unprotected inline network pairs are supported.
- The heartbeat mechanism is not supported on inline netlag and inline network group components. However, it is supported on the underlying inline networks.
- The heartbeat mechanism is not supported for classic inline bypass solution.
- The minimum timeout for heartbeat sessions is 200 milliseconds, if the tool type is configured as GigaVUE Node.
- The size of a custom heartbeat packet must be less than 128 bytes.

Heartbeat Profiles

A heartbeat profile supports health monitoring of inline tools and inline networks. A heartbeat profile is a group of attributes applied to an inline tool or inline network to configure its heartbeat operation. Multiple inline tools can share a heartbeat profile. However, for inline network, heartbeat is supported only within an inline network pair; it is not supported on inline netlag or inline network groups.

To display the configured heartbeat profiles, select **Inline Bypass > Heartbeats** to open the Heartbeats page. An example is shown in [Figure 40Heartbeats Page with Heartbeat Profiles](#).

Heartbeats

Heartbeat Profiles

Statistics

New

Clone

Edit

Delete

☐	Alias	Type	Packet Fo...	Custom P...	Direction	Period (ms)	Timeout (...)	Recovery...	Re...	⊕
☐	DBL_hbpr...	regular	arp		aToB	900	200	5	3	
☐	DBL_hbpr...	regular	arp		both	900	200	5	3	
☐	DBL_hbpr...	regular	arp		bToA	900	200	5	3	
☐	default	regular	arp		both	1000	500	30	3	

Figure 40 Heartbeats Page with Heartbeat Profiles

The Heartbeats page includes a default heartbeat profile that has the following settings:

- Alias—default
- Type—Regular
- Packet Format—arp or custom
- Custom Packet—URL from which a PCAP file can be imported
- Direction—bi-directional
- Period—1000 milliseconds
- Timeout—500 milliseconds
- Recovery Period—30 seconds
- Retries—3

The highest frequency heartbeat that can be configured is as follows:

- period—30 milliseconds
- timeout—20 milliseconds
- retry-count—0

The heartbeat mechanism supports the maximum number of inline tools, at the highest frequency, which is 48 on the GigaVUE-HC3, 16 on the GigaVUE-HC1, and 48 in GigaVUE-HC1-Plus.

To display the heartbeat profile associated with an inline tool and the heartbeat status, open the Inline Tools page by selecting **Inline Bypass > Inline Tools**. There is also a combined heartbeat status, which combines heartbeat and negative heartbeat statuses and indicates the tool health used for inline tool failover actions or SNMP traps. The combined heartbeat status is the combination of both heartbeat statuses. If both are configured and one is down, the combined status will be down.

Standard Heartbeat

The standard heartbeat is a packet sent by the GigaVUE-FM, GigaVUE HC Series node that passes through the inline tool to verify that it is passing traffic, even if the link is *up*. If the packet is not passed through the tool, the tool is considered to have failed and a bypass action is triggered.

Even when the tool is considered down, heartbeat packets continue to be sent so that the bypass action can be reversed when the tool is healthy again.

Heartbeats are sent bidirectionally to the inline tool.

Standard or Custom Heartbeat Packet

The format of the heartbeat packet can be the standard ARP packet or a custom packet. For a custom packet, you must provide a URL from which a PCAP file can be imported. If the PCAP file contains several packets, the first packet present in the file is taken as the heartbeat packet. The size of a custom heartbeat packet must be less than 128 bytes.

NOTE: The system will overwrite the MAC address portion of the custom heartbeat packet.

If the inline tool through which the heartbeat packets are passed is expecting IPv6 traffic exclusively, you must select a custom heartbeat packet.

Custom heartbeat packets are needed in situations in which inline tools do not reliably pass standard ARP packets. For example, if an inline tool is configured to pass only IPv6 traffic, an ICMPv6 ARP packet might be appropriate.

If a custom heartbeat packet is specified, the **Heartbeats** page displays the name of the PCAP file from which it was imported.

Detect Inline Tool Failure

The health of the inline tool is critical to the proper handling of traffic. An inline tool is determined to have failed if:

- link is lost to the tool
- inline heartbeat fails

When the tool fails in one direction, it is considered to have failed in both directions. For example, if the heartbeat stops flowing in the northbound direction, neither northbound or southbound packets are sent to the tool.

Negative Heartbeat Profiles

A negative heartbeat profile is a group of attributes applied to an inline tool to configure its negative heartbeat operation. Multiple inline tools can share a negative heartbeat profile. The content of a negative heartbeat is configurable using the same PCAP file mechanism as for a custom heartbeat packet.

Use the **Add Heartbeats** page shown in [Heartbeats](#) to configure a negative heartbeat profile. A negative heartbeat profile can be created by selecting **Negative** in the **Type** field. The profile will have the following settings:

- **PacketFormat** set to **Custom**
- **Direction** set to **Bi-directional**
- **Period** set to **1000** (period is specified in milliseconds)
- **Recover Time** set to **30** (recovery is set in seconds)

You must provide a valid PCAP file when Packet Format is set to Custom before the negative heartbeat profile can be applied to an inline tool.

When a negative heartbeat is configured, the system will send packets specified by the **Custom Packet Format**, in the time specified by **Period**, in the direction specified by **Direction**. The inline tool absorbs the negative heartbeat packets until the number of seconds specified by **Recovery Time** has passed. **Recovery Time** specifies the number of seconds of not receiving negative heartbeat packets in order for the inline tool to be declared healthy.

The negative heartbeat mechanism supports the maximum number of inline tools, which is 48 on the GigaVUE-HC3, 16 on the GigaVUE-HC1, and 48 on the GigaVUE-HC1-Plus.

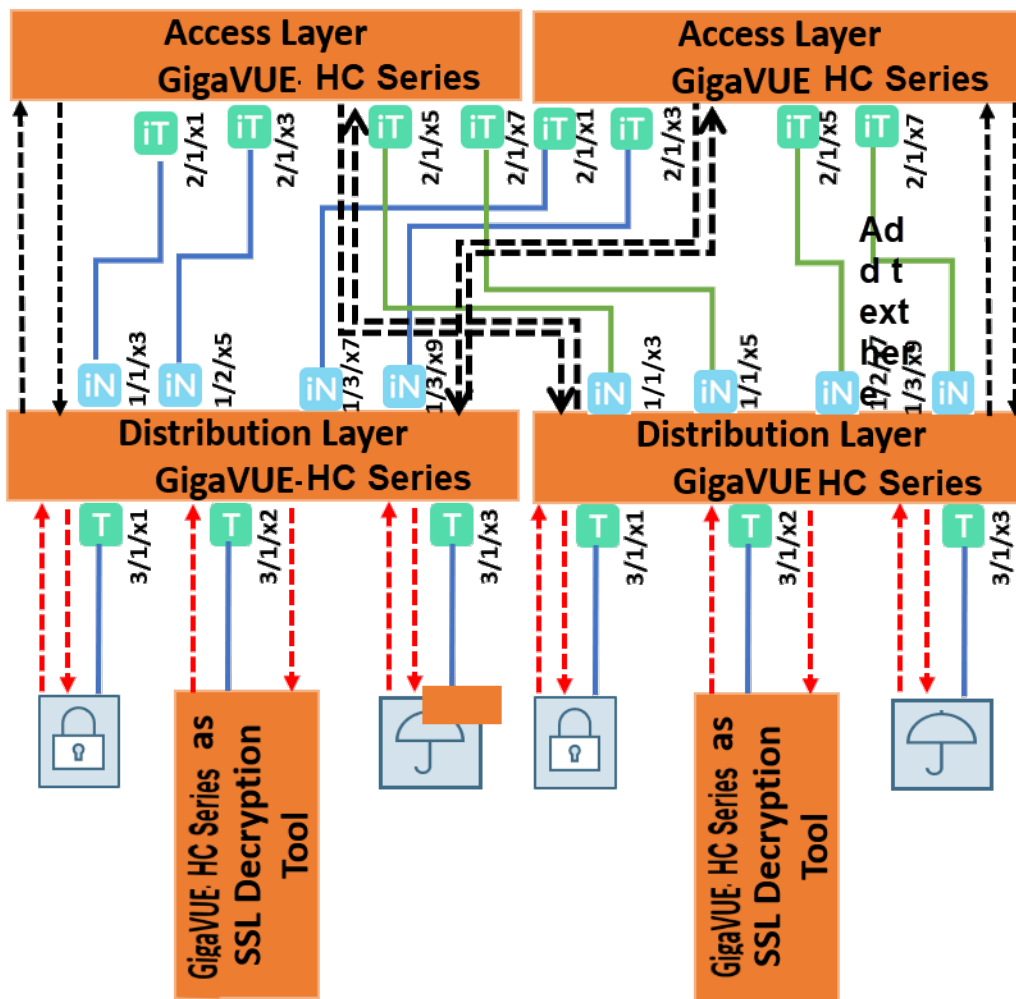
Use the Heartbeat page to display the configured negative heartbeat profiles. Use the Inline Tool page to display the negative heartbeat profile associated with an inline tool, the negative heartbeat status, and the counters of received packets in each direction. There is also a combined heartbeat status, which combines heartbeat and negative heartbeat statuses and indicates the tool health used for inline tool failover actions or SNMP polling. The combined heartbeat status is the combination of both heartbeat statuses. For example, if both are enabled and both are up, the combined status is up. If both are enabled and one is down, the combined status is down.

Heartbeat Support Between GigaVUE Nodes

The heartbeat mechanism focuses on providing extended heartbeat capability to monitor the following types of devices when the devices are connected to the inline-tool pair of ports as a tool:

- GigaVUE nodes
- GigaVUE nodes with GigaSMART operations configured

Following figure illustrates an example of a topology with GigaVUE nodes placed at three different layers.



- > Heartbeat (Access Layer -> Distribution Layer -> Access Layer)
- > Heartbeat (Distribution Layer -> Tool -> Distribution Layer)
- Traffic

GigaVUE HC Series means it can be either GigaVUE-HC3, GigaVUE-HC1 or GigaVUE-HC1-PLUS

The GigaVUE node at the access layer accesses the network traffic, gets the traffic processed by the tools at the tool layer, and transmits the processed traffic back to the network.

The GigaVUE node at the distribution layer distributes the traffic from the access layer to the tool layer.

The GigaVUE node at the tool layer acts as the SSL decryption tool.

In this topology, heartbeats are essential to monitor the traffic integrity at the distribution layer and to ensure automatic failover in case of a tool failure. In the access layer device, the ports that are connected to the distribution layer device are configured as inline tool ports because they face the tool side. In the distribution layer device, the ports that are connected to the access layer device are configured as inline network ports because they face the network side of the topology. The heartbeat packets will be sent from the inline tool port pair of the access layer device to the inline network port pair of the distribution layer device. If the forwarding state of the inline network pair is normal, the heartbeat packet is sent back to the inline tool port pair of the access layer device. Else, the packet is dropped.

The heartbeat mechanism is extended to support the GigaVUE node at the distribution layer to monitor the GigaVUE node that acts as a tool at the tool layer. In the distribution layer device, the ports that are connected to the tool layer device are configured as inline tool ports. In the tool layer device, the ports that are connected to the distribution layer device are configured as inline network ports. The heartbeat packets that are sent from the distribution layer device to the tool layer device will monitor the availability of both, the tool layer device and its GigaSMART engines.

Troubleshoot Heartbeat Failures

In your topology, you may sometimes notice heartbeat packets getting dropped at the inline network or the heartbeat status of the inline tool is not up. For details about how to isolate and troubleshoot such failures, refer to the following sections:

- [Heartbeat Status of Inline Tool is Not Operationally Up](#)
- [Heartbeat Packets are Dropped](#)

Configure a Heartbeat Profile

Use the Add Heartbeats page shown in the below figure to configure a regular heartbeat profile or a negative heartbeat profile by selecting **Inline Bypass > Heartbeats > Heartbeats**, and then clicking **New**.

Add HeartBeat Profile

OK

Cancel

Alias	Alias
Type	
Packet Format	
Direction	
Timeout	20-1000
Period	30-5000
Recovery Time	5-60
Retries	0-5

View Heartbeat Profile Statistics

Statistics about heartbeat profiles are displayed on the heartbeats statistics page. To open the Statistics page, select **Inline Bypass > Heartbeats > Statistics**. The page shows the following information:

Column	Description
Alias	The alias of the inline tool or inline network to which the heartbeat profile is associated with.
Inline Type	The inline type to which the heartbeat profile is associated with. The valid values are Inline Tool or Inline Network.
Heartbeat Profile	The alias of the heartbeat profile
Heartbeat Type	Indicates the type of heartbeat profile: Regular or Negative
A to B Packets	The number of packets sent/received from port A to port B of the inline tool.
B to A Packets	The number of packets sent/received from port B to port A of the inline tool.
A to B Packet Drops	The number of packets dropped from port A to port B of the inline tool or inline network.
B to A Packet Drops	The number of packets dropped from port B to port A of the inline tool or inline network.

You can clear the statistics for a specific heartbeat profile or all heartbeat profile. To clear the statistics for a heartbeat profile, select the required row, and then click **Clear**.

To clear the statistics for all heartbeat profiles, select **Clear All**, and then choose one of the following options:

- Select **Clear All Inline Network Heartbeat Stats** to clear the heartbeat statistics for all inline networks.
- Select **Clear All Inline Tools Heartbeat Stats** to clear the heartbeat statistics for all inline tools.
- Select **Clear All Negative Heartbeat Stats** to clear only the statistics for negative heartbeat profiles. The statistics for regular heartbeat profiles will remain.

Heartbeat Status after System Reload

Following a reload, there is a 5-minute delay for the system to stabilize before heartbeat packets are sent or received. During this delay, the heartbeat status is down.

Inline Tool Groups

Use the **Inline Tool Groups** configuration page to configure an inline tool group, which is an arrangement of multiple inline tools to which traffic is distributed based on hashing. In an inline tool group, traffic is shared. Each inline tool in the group receives a portion of the traffic. The distribution mechanism includes a way of dealing with failures of individual tools through traffic redistribution to the remaining healthy tools.

The inline tool ports that make up the inline tools participating in the inline tool group are always in pairs, running at the same speed, on the same medium (fiber or copper). All inline tool ports of the inline tool group must be on the same GigaVUE-HC3, or GigaVUE-HC1 and GigaVUE-HC1-Plus node, but can be on different modules on the node. The inline tool ports must also be on the same GigaVUE-HC3, or GigaVUE-HC1 and GigaVUE-HC1-Plus node as the inline network ports.

Inline tool groups can be configured as follows:

- non-redundant—multiple inline tools with no spare inline tool. Refer to [Figure 41Inline Tool Group With No Spare, Non-Redundant](#).
- 1+1 redundancy—single inline tool with a spare inline tool. Refer to [Figure 42Inline Tool Group With Spare, Redundant 1+1 Scenario](#).
- N+1 redundancy—multiple inline tools that are considered active, with a standby inline tool that is only used if one of the active inline tools fails. Refer to [Figure 43Inline Tool Group With Spare, Redundant N+1 Scenario](#).

With 1+1 redundancy, an inline tool is paired with a standby tool. When there is a loss of link or a heartbeat failure on an active tool, the traffic will be sent to the standby tool with no loss. In addition, if the standby tool fails, you can configure what happens to the traffic in that case, such as drop it or forward it.

With N+1 redundancy, one tool is added to a group of N distributed inline tools. When any one of the N tools fails, the traffic from that tool is sent to the standby (or spare) tool with no loss. In addition, if the standby tool fails, you can configure what happens to the traffic in that case, such as redistribute it, send it to another tool, or declare a failure on the tool group.

Refer to [Figure 41 Inline Tool Group With No Spare, Non-Redundant](#) for a non-redundant inline tool group.

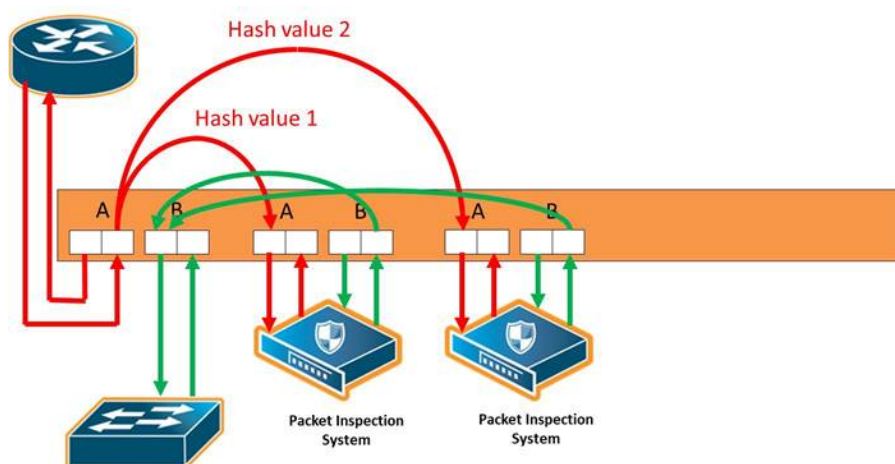


Fig.4 Inline-Tool-Group no-spare-tool scenario
(Only A-to-B traffic shown for diagram clarity)

Figure 41 *Inline Tool Group With No Spare, Non-Redundant*

Refer to [Figure 42 Inline Tool Group With Spare, Redundant 1+1 Scenario](#) for an inline tool group with a single inline tool and a spare inline tool configured. This is also referred to as 1+1 redundancy or N+1 redundancy where N equals 1. In [Figure 42 Inline Tool Group With Spare, Redundant 1+1 Scenario](#), traffic is only shown from A-to-B.

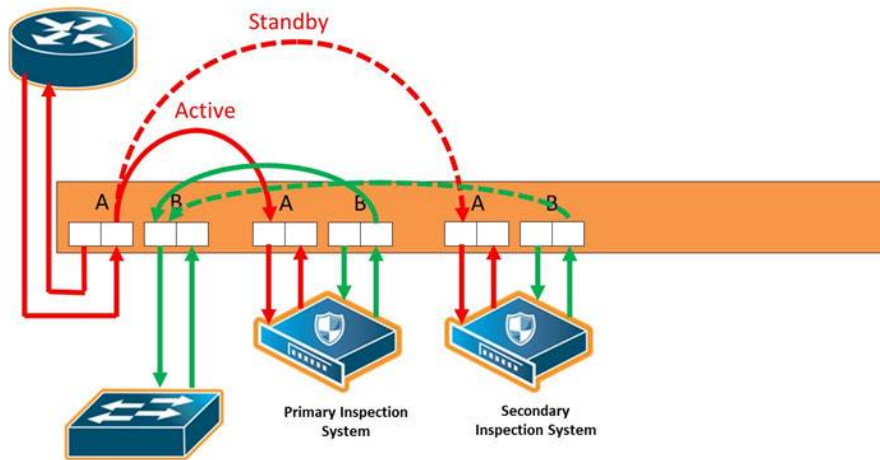


Figure 42 *Inline Tool Group With Spare, Redundant 1+1 Scenario*

Refer to [Figure 43 Inline Tool Group With Spare, Redundant N+1 Scenario](#) for an inline tool group in an N+1 redundant scenario, in which N is greater than 1. In [Figure 43 Inline Tool Group With Spare, Redundant N+1 Scenario](#), traffic is only shown from A-to-B.

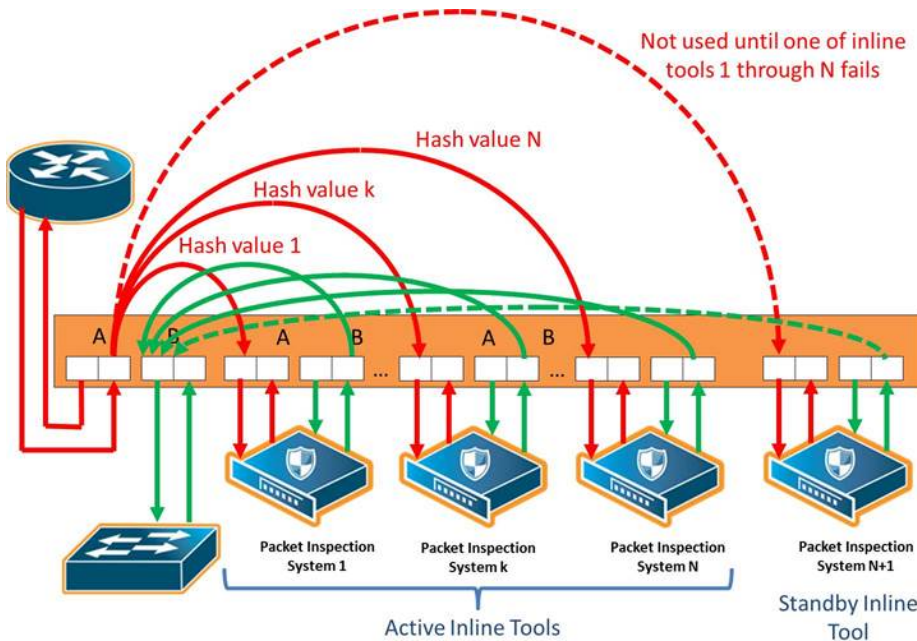


Figure 43 *Inline Tool Group With Spare, Redundant N+1 Scenario*

For details on the parameters of inline tool groups, refer to the following:

- [Inline Tool Group Failover Action](#)
- [Inline Tool Group Spare Inline Tool](#)
- [Symmetrical and Asymmetrical Hashing.](#)
- [Resilient Weighted Hashing](#)

Inline Tool Group Failover Action

One of the parameters of inline tool groups is the failover action, taken in response to a failure of an inline tool group, when the number of healthy inline tools in the inline tool group (including the spare inline tool, if configured) falls below the configured minimum. You can configure one of the following failover actions:

- **ToolBypass**—when the inline tool group fails, the traffic that normally was directed to the inline tool group is redirected to the bypass path. Use this failover action for configurations involving multiple inline tools or inline tool groups associated with an inline network or inline network group using rule-based maps. For configurations using map passalls, tool-bypass is the same as network-bypass.
- **NetworkBypass**—when the inline tool group fails, all traffic that would not have been dropped when the inline network or networks had a NORMAL forwarding state is directed to the bypass path. That is, all such traffic arriving at the side A inline network port or ports is forwarded to the side B inline network port or ports and all traffic arriving at the side B inline network port or ports is forwarded to the side A inline network port or ports.
- **NetworkPortForcedDown**—when the inline tool group fails, the inline network ports of the respective inline network (or inline network group) are forced down.
- **ToolDrop**—when the inline tool group fails, the traffic that normally was directed to the inline tool group is dropped. Use this failover action for configurations involving multiple inline tools or inline tool groups associated with an inline network or inline network group using rule-based maps. For configurations using map passalls, tool-drop is the same as network-drop.
- **NetworkDrop**—when the inline tool group fails, all traffic coming to the respective inline network (or inline network group) is dropped.

The default is tool-bypass.

The bypass path is between side A and side B of the inline network ports.

The failover action of all the inline tools specified by the inline tool list is overwritten by the failover mechanism of the inline tool group. This means that when a given inline tool specified by the inline tool list fails, the traffic originally directed to this inline tool is redirected to the spare inline tool (if one is configured and available) or handled according to the failover mode of the active tools, so long as the total number of healthy inline tools in the inline tool group is not smaller than the minimum required number of healthy inline tools.

When the total number of healthy inline tools in the inline tool group drops below the minimum required number of healthy inline tools, the failover action of the inline tool group determines the action to be taken.

Inline Tool Group Spare Inline Tool

One of the parameters of inline tool groups is a spare inline tool. If a spare is configured, the inline tool group becomes a redundant arrangement of inline tools. When the first failure occurs in a set of active inline tools, traffic will be forwarded to the spare with no loss, thus the spare will replace the failed tool in the active set.

The inline tools in the inline tool list are considered to be active inline tools. The traffic is hash-distributed over the active inline tools as long as all the inline tools are healthy. When one of the active inline tools fails, the spare inline tool takes the place of the failed inline tool and the new set operates as a new active set. If another inline tool fails, the traffic is redistributed according to the failover mode, as if there was no spare.

When the number of failed inline tools is such that the number of healthy inline tools is less than the minimum-group-healthy-size, the group heals itself by re-spreading the traffic over the healthy tools. When the number of healthy tools falls below the minimum-group-healthy-size, the failover action of the inline tool group takes place, while the failover action of the member inline tools is ignored.

The spare inline tool works with another parameter called release-spare-if-possible. When the inline tool that had been replaced with the spare inline tool recovers, the release-spare-if-possible parameter determines if the recovering inline tool is included in the active set of inline tools or if it becomes the new spare inline tool.

The default of the release-spare-if-possible parameter is disabled. Disabled means that even if the original inline tool recovers, the spare that replaced it will remain in the active set of inline tools. Enabled means that after the original inline tool recovers, the spare that replaced it will be released, if possible, from the active set of tools to become the spare again.

Configure the minimum-group-healthy-size and release-spare-if-possible parameters at the same time you configure the spare inline tool.

Symmetrical and Asymmetrical Hashing

One of the parameters of inline tool groups is hashing, which is used for distributing packets across a group of inline tools belonging to the inline tool group. The values for the hash parameter are as follows:

- **advanced**—Specifies symmetrical hashing, which is derived from the combination of packet fields based on the criteria selected for the advanced-hash algorithm configured under the **Ports > Port Groups > GigaStreams > Advanced Hash Settings** page.

For inline bypass applications, the most common choice of criteria for the advanced-hash algorithm is the combination of source IP and destination IP addresses. This produces a hash value that sends all traffic associated with the same session to the same inline tool in the inline tool group.

- **a-srcip-b-dstip**—Specifies asymmetrical hashing, which is derived from the source IP address for side A of the network and the destination IP address for side B of the network. This produces a hash value that sends all traffic associated with the same source address residing on side A to the same inline tool in the inline tool group, regardless of destination or session.
- **b-srcip-a-dstip**—Specifies asymmetrical hashing, which is derived from the destination IP address for side A of the network and the source IP address for side B of the network. This produces a hash value that sends all traffic associated with the same source address residing on side B to the same inline tool in the inline tool group, regardless of destination or session.

The default is **advanced**.

Use asymmetrical hashing if all traffic exchanged between a particular node on one side of the network and any nodes on the other side of the network that communicate with that node need to go to the same inline tool. The asymmetrical hashing options involve only source IP address (srcip) in one direction and only destination IP address (dstip) in the opposite direction. Bi-directional traffic, such as between a given user and all the Internet sites visited by the user, will be sent to the same inline tool in the group.

NOTE: When asymmetric hashing is configured, the portsrc and portdst packet fields are not included in the advanced-hash calculation for any GigaStream and inline tool groups across the GigaVUE-FM,GigaVUE HC Series node.

With symmetrical hashing, the inline network traffic path parameter can be configured to different values on the inline networks. With asymmetrical hashing, there is a restriction. Refer to [Asymmetrical Hashing Restrictions](#).

Refer to [Figure 44Asymmetrical Hashing](#) for asymmetrical hashing.

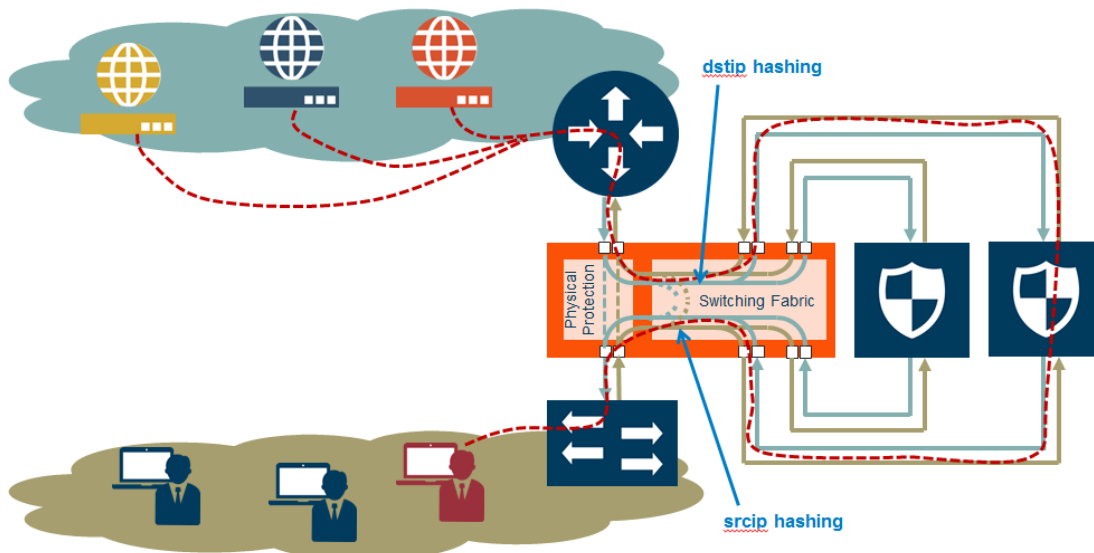


Figure 44 Asymmetrical Hashing

Use the hashing option **a-srcip-b-dstip** if the node is on side A of the network and the Internet is on side B. For example, Node A has IP address A. Traffic from Node A (from side A) will have IP address A. Traffic from side B (the Internet) destined for Node A, will have a destination of IP address A. This traffic will go to the same inline tool in the group.

If the network has the Internet on side A and the node on side B, use the hashing option **b-srcip-a-dstip**.

Asymmetrical Hashing Restrictions

The following are restrictions for asymmetrical hashing:

- If asymmetrical hashing is configured for the inline tool group, only rule-based maps or shared collector maps can be used to send traffic to the inline tool group. Inline map passalls cannot be used to send traffic to the inline tool group.
- For inline networks belonging to an inline network group, mapped to an inline tool group using asymmetrical hashing, the **Traffic Path** must be configured to the same value on all the inline networks, one of **Drop**, **Bypass**, **To Inline Tool**, or **ByPass with Monitoring**.

NOTE: For the inline networks belonging to an inline network group, mapped to an inline tool group using symmetrical hashing, the traffic path parameter can be configured to different values on the inline networks.

- If an inline network is involved in an inline map to an inline tool group configured with asymmetrical hashing, the inline network ports of the inline network cannot be used as the **Source** in any out-of-band maps. Also, if the traffic path parameter for the inline network is configured to **ByPass with Monitoring**, there will not be any bypass traffic. All traffic will be forwarded to the inline tool group.

- When an inline tool group is included as a member of an inline series, asymmetrical hashing is not supported.
- If an inline network is involved in a flex-inline map and the inline tool used in the map is a part of an inline tool group; the traffic path parameter for the inline network or the flex traffic path of the inline tool from the inline tool group is set to **ByPass with Monitoring**, there will not be any bypassed traffic irrespective of the hashing. All traffic will be forwarded to the inline tool used from the inline tool group.

Resilient Weighted Hashing

One of the parameters of inline tool groups is weighting that provides you the ability to distribute traffic to the inline tools by assigning either an equal weighting or a custom weighting to the inline tools. You can assign custom weight in percentage or ratio. If an inline tool in a group goes down and the group maintains the **Minimum Healthy Group Size** that is defined for the group, the traffic is redistributed to the remaining tools based on the equal weighting or the custom weighting assigned to the tools. If the inline tool group does not meet the **Minimum Healthy Group Size** defined for the group, the traffic is redistributed based on the **Failover Action** defined for the group.

NOTE: Resilient hashing is not supported for classic inline maps.

The values for the weighting parameter are as follows:

- **Equal**—Traffic is distributed equally to all the inline tools in the inline tool group.
- **Relative**—Traffic is distributed to the inline tools in the inline tool group based on the relative weight or ratio assigned to the respective inline tools. The valid range is 1–256.
- **Percentage**—Traffic is distributed to the inline tools in the inline tool group based on the percentage assigned to the respective inline tools. The valid range is 1–100.

If you select **Relative** or **Percentage** as the weighting option, enter the hash weights for the inline tools that appear in the table below the **Weighting** drop-down list. Ensure that you assign a hash weight for each inline tool in the inline tool group.

Inline Serial Tools

Use the **Inline Serial Tools Groups** configuration page to configure inline tools in a series, in which the traffic from one side of the inline network is guided through the members of the inline tool series before it is sent out the other side of the inline network. With inline tools and inline tools groups arranged in a series, the traffic from one inline tool or inline tool group flows to the next, so all tools see the same traffic.

The inline tool ports that make up the inline tools and inline tool groups participating in the inline tool series are always in pairs, running at the same speed, on the same medium (fiber or copper). All inline tool ports of the inline tool series must be on the same GigaVUE-HC3, or GigaVUE-HC1 and GigaVUE-HC1-Plus node. The inline tool ports and inline tool groups must also be on the same GigaVUE-HC3, or GigaVUE-HC1 and GigaVUE-HC1-Plus node as the inline network ports.

To view the currently configured inline tool series, select **Inline Bypass > Inline Serial Tools** to open the Inline Serial Tool Groups page shown in the following figure.

Refer to [Figure 45Inline Serial Tools](#) for an illustration of an inline tool series. In [Figure 45Inline Serial Tools](#), traffic is only shown from A-to-B.

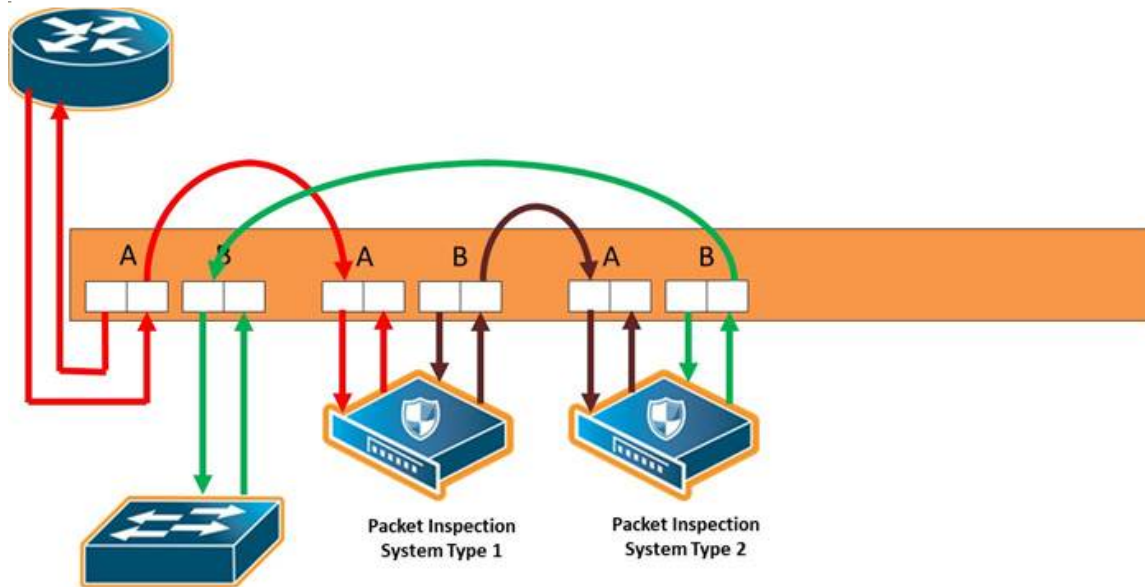


Figure 45 *Inline Serial Tools*

Refer to [Figure 46Inline Tool Series, Including Inline Tool Group](#) for an inline tool series that includes an inline tool group in addition to individual inline tools. The per-direction-order is set to forwarding. In [Figure 46Inline Tool Series, Including Inline Tool Group](#), the inline tool group is placed as the middle member of the series, but it could be placed as the first member of the series or the last member of the series as well. In the inline tool group, traffic is shared.

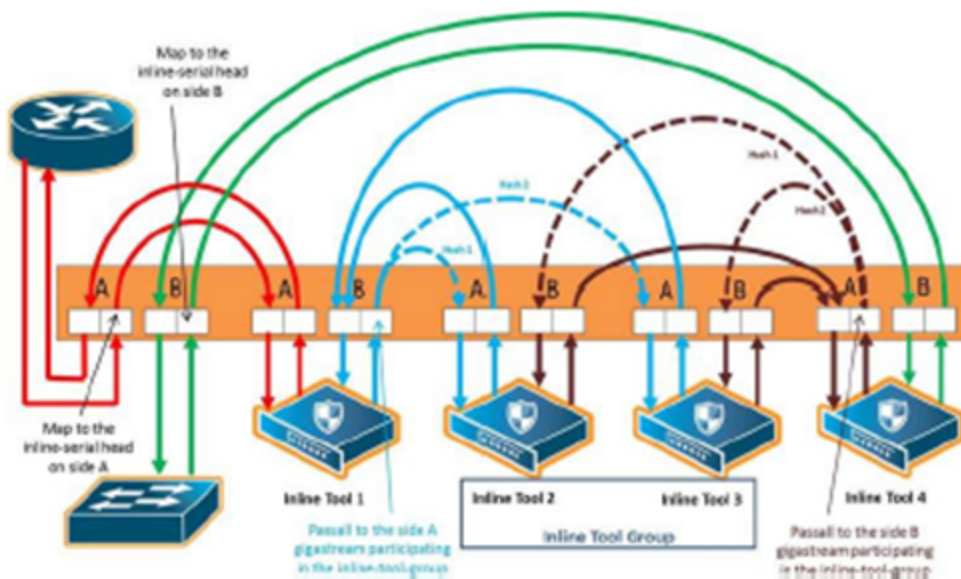


Figure 46 Inline Tool Series, Including Inline Tool Group

NOTE: For inline SSL decryption, the inline tool series does not support an inline tool group in the series.

The number of inline tools and inline tool groups in the inline series is limited only by the number of ports available for creating the inline networks and inline tools participating in the inline bypass solution.

When an inline tool group is included as a member of a inline series:

- a spare inline tool can be configured on the inline tool group
- inline maps to individual members of an inline tool group are not supported
- asymmetrical hashing is not supported, which means that the hash options, ascrip-b-dstip and b-scrip-a-dstip, are not allowed on the inline tool group.

To configure an inline serial tool group, do the following:

1. Open the **Inline Serial Tool Group** configuration page by selecting **Inline Bypass > Inline Serial Tools** from the main navigation pane, and then clicking **New**.
2. Enter a name for the inline serial tool group in the **Alias** field to identify the group and an optional description in the **Description** field.
3. Select and order the inline tools for the inline tool group.
 - a. Click in the **Inline Tools** fields. The drop-down list shows the available inline tools
 - b. Select the inline tools or in or inline tool group to add to the inline serial tool group.

The inline tools are displayed in the order that they are selected. To change the order, click the up and down arrows.

4. Click **Save**.

NOTE: An inline serial tool group cannot be edited after it is saved.

Inline Serial Tools Global Failover Action

One of the parameters of inline tool series is the failover action taken in response to a failure of the inline tool series as a whole. This is referred to as the global failover action.

Each inline tool or inline tool group in the series can also have its own failover action. This is referred to as the local failover action. Refer to [Inline Tool Series Local Failover Action](#) for details.

For global failover actions, an inline tool series is declared to be in a failure condition as soon as any of its member inline tools goes into a failure condition. An inline tool series recovers from a failure condition after all the member inline tools recover from their failure conditions. The failover action attributes of the individual inline tools participating in an inline tool series are ignored. Instead, the **Failover action** configured on the Inline Serial Tool Group page for the inline tool series is executed. The values for global failover actions are as follows:

- **ToolBypass**—when the inline serial tools fails, the traffic that normally was directed to the inline tool is redirected to the bypass path. Use this failover action for configurations involving an inline serial tools that is associated with an inline network using rule-based maps. For configurations using map passalls, tool-bypass is the same as network-bypass. Refer to [Figure 47Inline Tool Series Global Bypass Failover Action](#).
- **NetworkBypass**—when the inline serial tools fails, all traffic that would not have been dropped when the inline network or networks had a NORMAL forwarding state is directed to the bypass path. That is, all such traffic arriving at the side A inline network port or ports is forwarded to the side B inline network port or ports and all traffic arriving at the side B inline network port or ports is forwarded to the side A inline network port or ports. Refer to [Figure 47Inline Tool Series Global Bypass Failover Action](#).
- **NetworkPortForcedDown**—when the inline serial tools fails, the inline network ports of the respective inline network are forced down. Refer to [Figure 48Inline Tool Series Global Network Ports Forced Down Failover Action](#).
- **ToolDrop**—when the inline serial tools fails, the traffic that normally was directed to the inline tool is dropped. Use this failover action for configurations involving an inline serial tools that is associated with an inline network using rule-based maps. For configurations using map passalls, tool-drop is the same as network-drop. Refer to [Figure 49Inline Tool Series Global Drop Failover Action](#).
- **NetworkDrop**—when the inline serial tools fails, all traffic coming to the respective inline network (or inline network group) is dropped. Refer to [Figure 49Inline Tool Series Global Drop Failover Action](#).

The bypass path is between side A and side B of the inline network ports.

The default is **ToolBypass**.

Any failure of any member leads to the failure of the inline serial tools, hence the failover action for an inline serial tools will overwrite the failover action of the inline tool members of the series.

Figure 47 Inline Tool Series Global Bypass Failover Action to Figure 49 Inline Tool Series Global Drop Failover Action show the global failover actions for the inline series when any individual inline tool in the series fails.

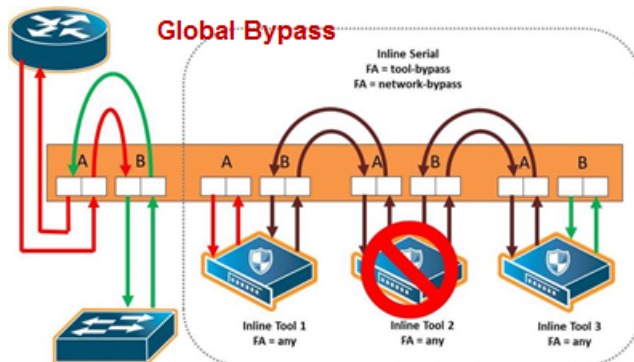


Figure 47 Inline Tool Series Global Bypass Failover Action

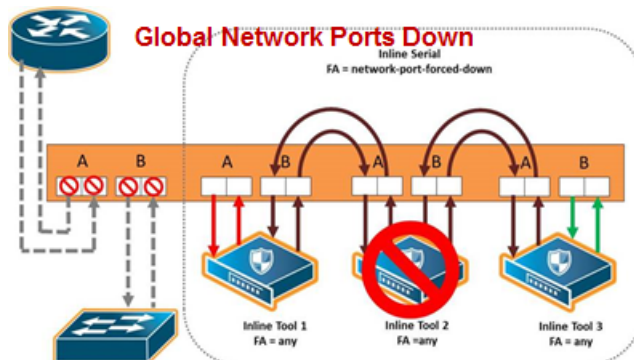


Figure 48 Inline Tool Series Global Network Ports Forced Down Failover Action

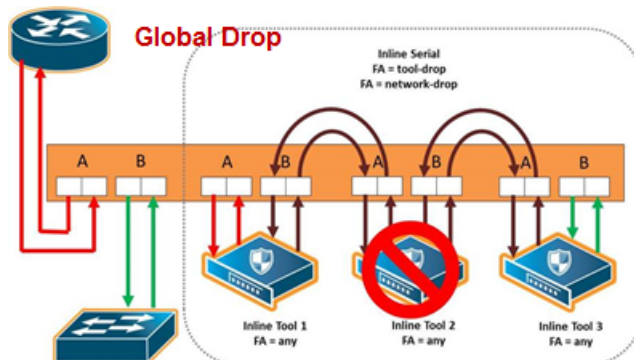


Figure 49 Inline Tool Series Global Drop Failover Action

Inline Tool Series Local Failover Action

Each inline tool in the series can have its own local failover action. When an individual inline tool or inline tool group in the series fails, the action taken depends on the failover action of the individual inline tool.

To configure local failover actions, configure a failover action of **Per Tool** for the series as a whole. Then the individual failover action for each inline tool in the series, as configured with the **inline Tool failover action**, takes effect. For details on the values, refer to [Inline Tool Failover Action](#).

For example, if the failover action of the inline series is configured as **Per Tool** and the failover action of an individual inline tool in the series is configured as **ToolBypass**, when that tool in the series fails, the traffic will skip over the failed tool.

NOTE: For inline SSL decryption, the **Per Tool** failover action is not supported.

The values for local failover actions are as follows:

- **ToolBypass**—when the inline tool fails, the traffic bypasses the failed tool. That is, the traffic originally coming to the inline tool is diverted to the next inline tool in the series or to the appropriate inline network port if the inline tool is the last in the series. Refer to [Figure 50Inline Tool Series Local Tool Bypass Failover Action](#).

NOTE: When all the inline tools in a series are configured as **ToolBypass** and they all fail, this is the same as the failover action of **ToolBypass** for the series.

- **ToolDrop**—when the inline tool fails, traffic to this inline tool stops being forwarded. Effectively, this has the same result as the failover action of **ToolDrop** for the series as a whole, although the healthy members of the series will still receive traffic in one of the directions. Refer to [Figure 51Inline Tool Series Local Tool Drop Failover Action](#).
- **NetworkBypass**—when the inline tool fails, a bypass is established between the inline network ports. Refer to [Figure 52Inline Tool Series Local Network Bypass Failover Action](#).
- **NetworkDrop**—when the inline tool fails, traffic is dropped at the inline network ports. Refer to [Figure 53Inline Tool Series Local Network Drop Failover Action](#).
- **NetworkPortForcedDown**—when the inline tool fails, the links for the inline network ports are brought down. Refer to [Figure 54Inline Tool Series Local Network Ports Forced Down Failover Action](#).

[Figure 50Inline Tool Series Local Tool Bypass Failover Action](#) to [Figure 54Inline Tool Series Local Network Ports Forced Down Failover Action](#) show the local failover actions when an individual inline tool in a series fails

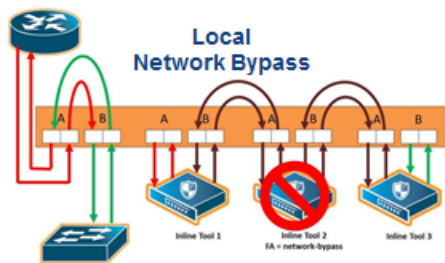


Figure 50 *Inline Tool Series Local Tool Bypass Failover Action*

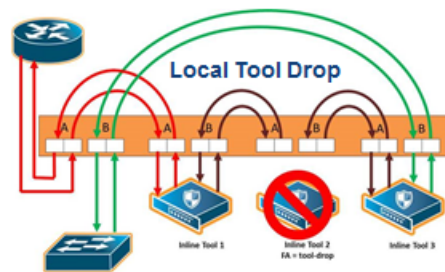


Figure 51 *Inline Tool Series Local Tool Drop Failover Action*

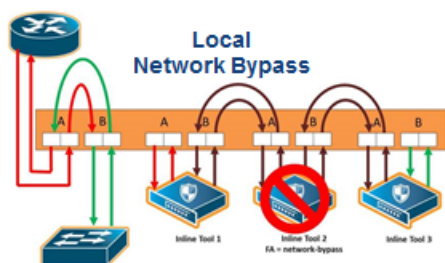


Figure 52 *Inline Tool Series Local Network Bypass Failover Action*

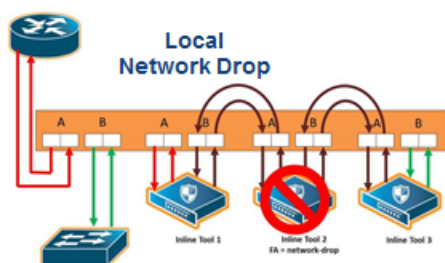


Figure 53 *Inline Tool Series Local Network Drop Failover Action*

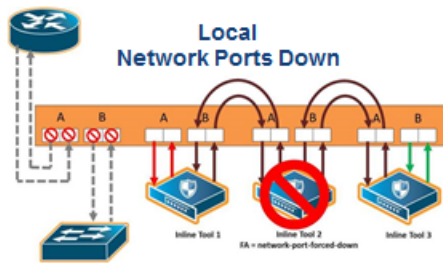


Figure 54 *Inline Tool Series Local Network Ports Forced Down Failover Action*

Figure 55 Inline Tool Series Local Failover of Two Tools shows the failure of two individual inline tools in a series with different configured failover actions.

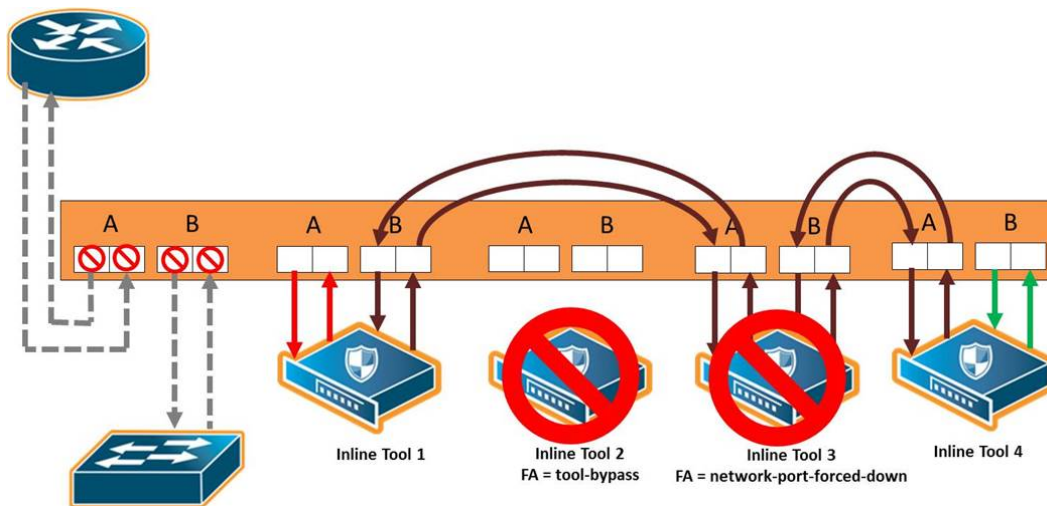


Figure 55 *Inline Tool Series Local Failover of Two Tools*

Inline Tool Series Per-Direction Order

One of the parameters of inline tool series is the per-direction order of the inline tool series. This parameter configures the traffic direction order of side B traffic with respect to the inline tool list, that is, the direction of the return traffic.

The **Return Direction** options on the Inline Serial Tool Group page specify the per-direction order of the side B traffic of the inline tool series as follows:

- **Reverse** specifies that the traffic from network B will flow through the inline tool list in reverse order, for example, from the third tool, to the second tool, to the first tool. This specifies the reverse order of inline tools for both directions.
- **Forward** specifies that the traffic from network B will flow through the inline tool list in the order it which it is defined, for example, from the first tool, to the second tool, to the third tool. This specifies the same order of inline tools for both directions of traffic.

The default is **Reverse**.

Figure 56 Inline Tool Series Per-Direction Order: Simplified Reverse and Forward shows a simplified view of the flow through the tools:

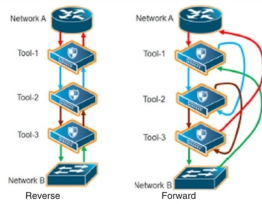


Figure 56 Inline Tool Series Per-Direction Order: Simplified Reverse and Forward

In Figure 56 Inline Tool Series Per-Direction Order: Simplified Reverse and Forward, **Reverse** is on the left and **Forward** is on the right. Traffic from network side A to network side B for both reverse and forward flows from the first tool, to the second tool, to the third tool. But traffic from network side B to network side A with reverse, flows from the third tool, to the second tool, to the first tool, whereas traffic from network side B to network side A with forward, flows from the first tool, to the second tool, to the third tool.

Figure 57 Inline Tool Series Per-Direction: Reversed shows the reverse direction with the tools connected to the GigaVUE-FM, GigaVUE HC Series node.

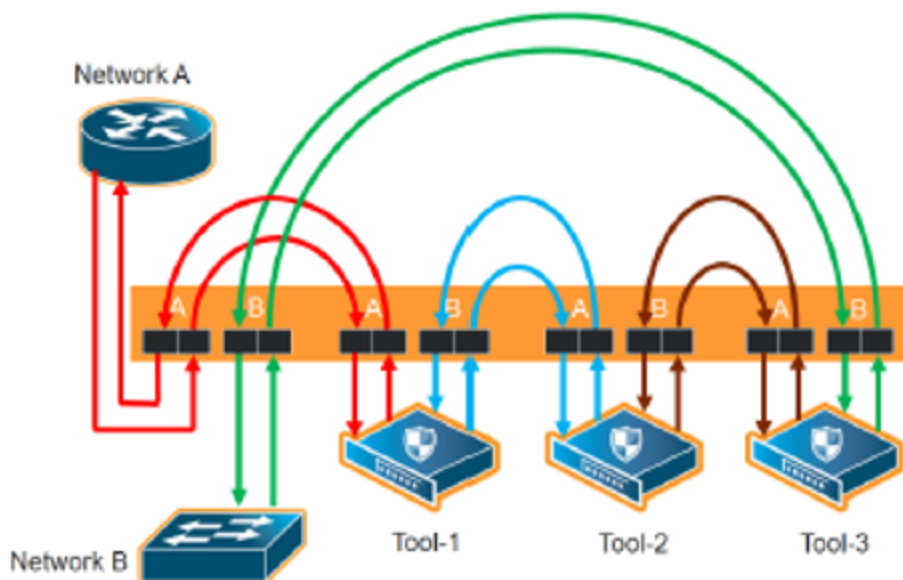


Figure 57 Inline Tool Series Per-Direction: Reversed

Figure 57 Inline Tool Series Per-Direction: Reversed shows the forward direction with the tools connected to the GigaVUE-FM, GigaVUE HC Series node.

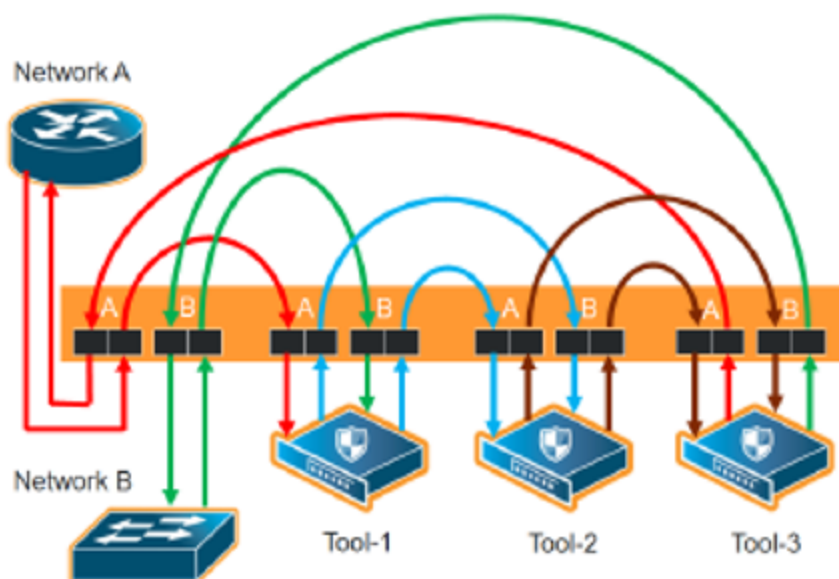


Figure 58 *Inline Tool Series Per-Direction: Forward*

Associate Inline Networks with Inline Tools Using Inline Maps

Inline networks and inline network groups are associated with inline tools, inline tool groups, and inline serial tools through inline maps. An inline map is a regular map, but the **Source** and **Destination** fields specify inline software constructs instead of port lists.

On the **Edit Map** or **New Map** page, the **Source** field specifies the inline network alias or inline network group alias. The **Destination** field specifies an inline tool alias, an inline tool group alias, an inline tool series alias, or an inline bypass. An inline bypass is a special construct that is used as a pseudo-inline tool to allow a portion of traffic to bypass any inline tools.

Maps can associate a network with multiple inline tools or they can associate multiple inline networks with the same inline tool or with multiple inline tools.

With inline maps, only the traffic that meets the map rules is sent to the tools, to bypass, or to shared collectors. For example, you can send traffic to tools for which they are specialized and send the rest to bypass. Or, if there is a type of traffic in which the tools are not interested or do not understand, that traffic can be sent to a shared collector.

NOTES:

- When an inline network is mapped to an inline tool or inline tool group, a second inline network cannot be mapped to the same inline tool. (In other words, an inline tool can be used in only one map.) However, when there are multiple inline networks, use an inline network group to map to the same inline tool.

- If an inline tool is already specified in a map, that tool cannot be included in an inline tool group (unless the map is first deleted).
- Inline network ports, inline tool ports, and out-of-band tool ports that are used in map configuration must all be configured on the same GigaVUE-HC3, or GigaVUE-HC1 or GigaVUE-HC1-Plus node. Even if nodes are in a cluster, the inline ports cannot be on different nodes.

Refer to the following sections:

- [Inline Map Passall](#)
- [Inline Map](#)
- [Inline Map Shared Collector](#)
- [Inline Maps to Individual Members of an Inline Tool Group](#)
- [Out-of-Band \(OOB\) Map](#)
- [Symmetric and Asymmetric Maps](#)

Inline Map Passall

Use the **Pass All** subtype to configure a type of inline map that passes all traffic. Map-passalls facilitate the sending of traffic between inline network ports (through inline tools or bypass). All of the inline network ports and inline tool ports involved in an inline map must be located on the same Gigamon node.

Use the **Source** of the **Pass All** to specify a single inline network.

Use the **Destination** of the **Pass All** to specify an inline tool alias, an inline tool group alias, an inline tool series alias, or an inline bypass. An inline bypass is a special construct that is used as a pseudo inline tool to allow a portion of traffic to bypass any inline tools.

An inline bypass, using the physical bypass option, is only valid if the **Source** is an inline network port. This applies only to the **Pass All** subtype for asymmetrical scenarios.

Inline Map

Use the **New Map** page to configure a type of inline map that uses rules to direct traffic. These inline maps are referred to as rule-based maps. All of the inline network ports and inline tool ports involved in an inline map must be located on the same GigaVUE-FM, GigaVUE HC Series node.

Use the **Source** field to specify an inline network alias or an inline network group alias.

Support for rule-based maps is limited to symmetric scenarios, which means that the **Destination** of rule-based inline maps can only be aliases of inline networks or inline network groups (not individual ports).

Use the **Destination** to specify an inline tool alias, an inline tool group alias, an inline tool series alias, or an inline bypass. An inline bypass is a special construct that is used as a pseudo inline tool to allow a portion of traffic to bypass any inline tools.

For rule-based maps, the **Destination** can be configured to inline bypass with no restrictions, so long as the **Source** specifies either an inline network or an inline tool.

Use the **Priority** to order inline maps by priority. For example, you can specify the highest priority map to be for encrypted traffic and lowest priority map to be for a shared collector. You can also place inline maps before or after one another using the **Priority**.

Use the **Type** to specify any map rule.

Inline Map Shared Collector

Use the **Collector** subtype to configure a shared collector to which to send any packets that do not match the map rules in the inline maps. Use a shared collector with one or more rule-based inline maps. All of the inline network ports and inline tool ports involved in an inline shared collector map must be located on the same GigaVUE-FM,GigaVUE HC Series node.

Use the Source argument to specify an inline network alias or an inline network group alias.

Use the Destination argument to specify an inline tool alias, an inline tool group alias, an inline tool series alias, or an inline bypass. An inline bypass is a special construct that is used as a pseudo inline tool to allow a portion of traffic to bypass any inline tools.

For shared collector maps, the **Source** field can be configured to inline bypass with no restrictions, so long as the **Destination** field specifies either an inline network or an inline tool.

Support for shared collector inline maps is limited to symmetric scenarios, which means that the **Destination** field of rule-based inline maps can only be aliases of inline networks or inline network groups (not individual ports).

Inline Maps to Individual Members of an Inline Tool Group

Prior to software version 4.4, the **Map** page was used to configure an inline map that directed traffic to the inline tool group as a whole. The map could be rule-based or passall. There was only one type of hashing available, which distributed the traffic across the tools in the inline tool group.

Starting in software version 4.4, the **Map** page can also be used to configure inline maps to the individual members of an inline tool group. The maps must be rule-based. There are also more hashing options that can be specified for traffic that does not match any of the map rules. The hashing options are described in [Inline Tool Groups](#).

The rule-based maps are defined with the inline tool group sharing the same source, either an inline network or an inline network group in the **Source** field of the map. The map destinations (the **Destination** field of the map) are the individual inline tools in the group. Traffic not matching any of the map rules is sent to a shared collector to be distributed according to the specified hashing value.

The shared collector must also have the same source as the maps to the individual members of the inline tool group. The destination for the shared collector is the inline tool group. The shared collector map is a mandatory part of the configuration.

Both configurations are available: either a single map to the inline tool group as a whole, or multiple rule-based maps to the individual members of the inline tool group plus a shared collector; however, they cannot both be configured at the same time.

Refer to [Figure 59 Rule-Based Maps to Individual Tools in an Inline Tool Group](#) for the rule-based maps to the individual members of the inline tool group. In [Figure 59 Rule-Based Maps to Individual Tools in an Inline Tool Group](#), traffic is only shown from A-to-B.

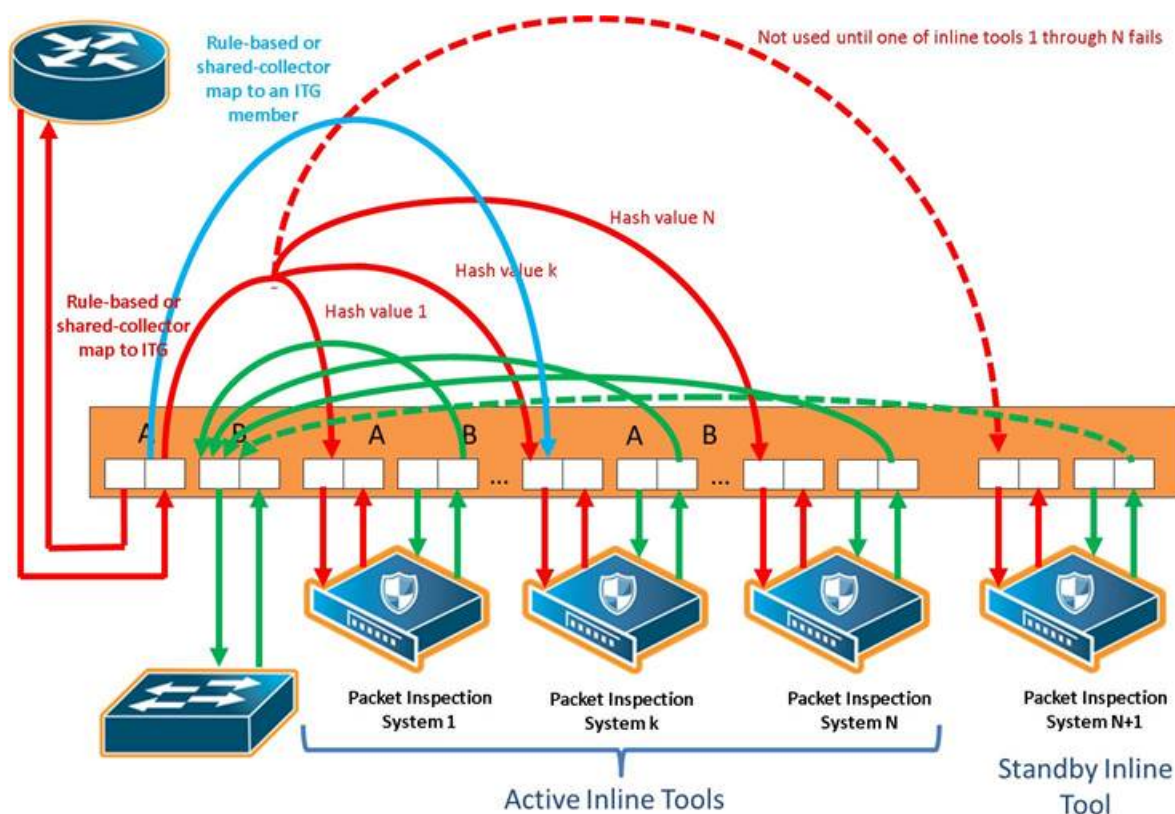


Figure 59 Rule-Based Maps to Individual Tools in an Inline Tool Group

Map, Inline Tool, and Inline Tool Group Configuration Restrictions

The following are map, inline tool, and inline tool group configuration restrictions for the rule-based maps to the individual members of the inline tool group:

- If there is a map to the inline tool group as a whole, there cannot also be rule-based maps to the individual inline tools in the group.
- Maps to the individual inline tools in a group must be rule-based. Map passalls to the individual tools cannot be configured.
- The source of rule-based maps to the individual inline tools in a group must be the same (either the same inline network or the same inline network group). The shared collector must have the same source as well.
- If there is a map configured to the individual inline tools in a group, the inline networks must have their traffic path set to **to-inline-tool**. This applies to individual inline networks as well as to inline networks involved in an inline network group.
- For the individual inline tools in a group, the recovery mode of the individual inline tools must be configured as **automatic**. A recovery mode of **manual** cannot be configured.
- For the inline tool group, the failover action must be either **NetworkBypass** or **NetworkDrop**. A failover action of either **ToolBypass** or **ToolDrop** for the inline tool group cannot be configured.
- Only one inline shared collector map can be configured (among the set of inline maps).
- Maps must be created in a specific order. The shared collector map must be configured last. For example, if there are three inline tools in the group, configure the three maps to the individual members of the group first, then configure the shared collector map.
- Maps must be deleted in a specific order. The shared collector map must be deleted first. Then the maps to the individual members of the group can be deleted.
- Once the shared collector map is configured, any changes to the maps to the individual members of the group are restricted. Only the map rules can be edited.

NOTE: All the rules in a map cannot be deleted. All maps must have attributes for **Source**, **Destination**, and at least one **rule** configured.

- When an inline tool group is included as a member of an inline series, inline maps to individual members of an inline tool group are not supported.
- If one of the inline tools is disabled in an inline-network-group to inline-tool-group map that has the same ingress VLAN tag on the ports of an inline-network pair then the traffic will be looped back to the same network. This behavior is seen only with passall maps. In above scenarios use rule-based maps instead of passall maps.

Inline Tool Failures and Failover Actions

An inline tool group has a failover action for the group as a whole. The failover action is taken in response to a failure when the number of healthy inline tools in the inline tool group (including the spare inline tool, if configured) falls below the configured minimum. In addition, the individual inline tools in the group have failover actions.

When there are maps to individual inline tool members of the group, an inline tool has both a group failover action and an individual failover action.

Refer to [Failover Actions When an Individual Tool in an Inline Tool Group Fails](#) for the failover actions when an individual inline tool in an inline tool group fails.

Table 16: Failover Actions When an Individual Tool in an Inline Tool Group Fails

Inline Tool Group Spare	Number of Healthy Tools	When Individual Inline Tool Fails:	
		Traffic to Inline Tool Group	Traffic to Failed Tool
no spare	equal to or greater than the configured minimum healthy size	is redistributed among the remaining healthy tools in the group	no action—the failover action of the individual inline tool is ignored. If there is an inline map to the failed inline tool, the connectivity arrangements supporting the individual map are maintained as if nothing happened.
	less than the configured minimum healthy size	fails over according to the failover action for the inline tool group	no action—the failover action of the individual inline tool is ignored. If there is an inline map to the failed inline tool, the connectivity arrangements supporting the individual map are maintained as if nothing happened.
spare	equal to or greater than the configured minimum healthy size	is redistributed among the remaining healthy tools	no action—the failover action of the individual inline tool is ignored. If there is an inline map to the failed inline tool, the connectivity arrangements supporting the individual map are maintained as if nothing happened.
	less than the configured minimum healthy size	fails over according to the failover action for the inline tool group	no action—the failover action of the individual inline tool is ignored. If there is an inline map to the failed inline tool, the connectivity arrangements supporting the individual map are maintained as if nothing happened.
failed spare	N/A	no action, if there is no inline map configured to the spare	no action—the failover action of the individual inline tool (in this case, the spare) is ignored. If there is an inline map to the failed inline tool, the connectivity arrangements supporting the individual map are maintained as if nothing happened.

Maps That May Lead to Selective Traffic Drops

With inline bypass solutions based on inline flow mapping, the use of rule-based maps can lead to selective traffic drops. Traffic drops can occur as follows:

- if a shared collector from the inline network or inline network group has not been configured. Packets not matching the criteria specified by the rules in the configured rule-based maps will be dropped.
- if drop rules have been included in the rule-based maps configured from the inline network or inline network group

In most inline flow mapping solutions, all traffic exchanged between the two end nodes of a given inline network are expected to be processed by the inline tool or tools associated with this inline network through the configured maps. Therefore, it is recommended to always configure a shared collector and to not include drop rules in the rule-based maps.

Out-of-Band (OOB) Map

All inline network ports and inline tool ports can be subject to monitoring by listen-only tools. This means that an inline network port or inline tool port can be listed in the **Source** field in which the **Destination** field is an arbitrary tool type of port located anywhere in the system and not limited to the same node.

Inline network ports and inline tool ports involved in rule-based inline maps can be used as network ports for monitoring (or out-of-band) maps.

Out-of-band (OOB) maps are supported as follows:

- If the inline bypass solution use passalls, the OOB arrangements can use any rule-based maps or map shared collectors, or passalls. Refer to [Figure 60Out-of-Band Rule-Based Maps](#).
- If the inline bypass solution use rule-based maps or map shared collectors, the OOB arrangements can use only map passalls. Refer to [Figure 61Out-of-Band Map Passalls](#).
- When the source port of an OOB map is associated with an inline network, a list of inline ports is supported in the port list (the **Source** field of the Map page).

The following restrictions apply to OOB maps:

- When the source port of an OOB map is associated with an inline network group, only a single inline port (network or tool) is supported in the port list. In this case, multiple OOB maps are needed because each OOB map only accepts one inline port (network or tool) in the **Source** field on the Map page.

- OOB maps from inline network ports of inline networks involved in maps to inline tool groups configured with asymmetrical hashing are not allowed. If an inline network is involved in an inline map to an inline tool group configured with asymmetrical hashing, the inline network ports of the inline network cannot be used as the **Source** attribute in any out-of-band maps.

Prior to software version 4.4, if an inline network was part of an inline network group, sending traffic to an out-of-band tool was not allowed.

Starting in software version 4.4, out-of-band maps from inline ports involved in inline network groups are supported. You can configure OOB maps originating from inline network ports or inline tool ports when these ports are involved in an inline network group, except for the following:

- GigaSMART operations
- tool ports located on a different node

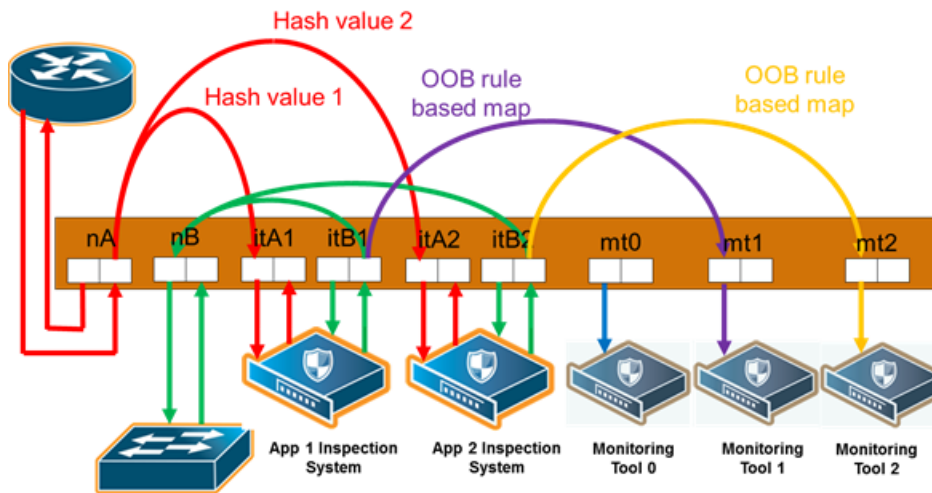


Figure 60 Out-of-Band Rule-Based Maps

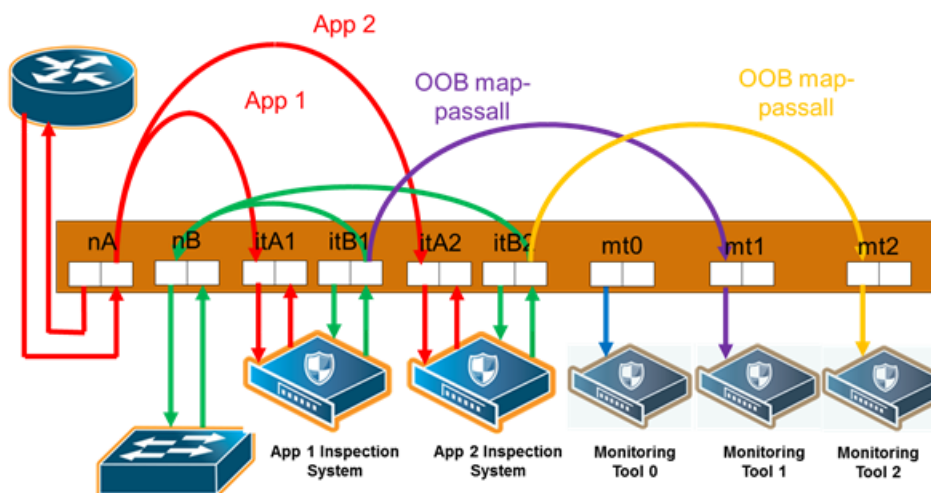


Figure 61 Out-of-Band Map Passalls

Symmetric and Asymmetric Maps

In a symmetric map configuration, the southbound and northbound forwarding to the tools is the same. For example, traffic from A to B goes through an inline tool, as does traffic from B to A. Rule-based maps are limited to symmetric configurations.

In an asymmetric map configuration, the southbound traffic is distributed to the inline tools, but northbound traffic can be sent through uninspected. For example, traffic from A to B goes through an inline tool, but traffic from B to A bypasses it.

Asymmetric configurations are only supported with map passalls. Traffic can come from individual inline networks, be sent to individual inline tools or inline tool groups, or to bypass.

Symmetrical combinations of two asymmetrical arrangements (that is, with both side A and side B pointing to the inline tool or to bypass) are not allowed.

Some IPSs do not need to inspect northbound traffic. For example, those focused on preventing Denial of Service (DoS) attacks, may not need to keep track of session flows and may only be concerned about southbound traffic.

Conversely, data loss prevention systems, those that are more concerned about what sensitive data is leaving the protected network than what is coming in, may focus solely on northbound traffic.

Configure Inline Bypass

The steps to configure inline constructs are only applied to GigaVUE-FM, GigaVUE HC Series® HC Series nodes. In a cluster environment, these steps are only applied to GigaVUE-FM, GigaVUE HC Series® HC Series nodes through the cluster leader.

The inline constructs must all be configured on one GigaVUE-HC3, GigaVUE-HC1-Plus, or one GigaVUE-HC1 node, not across nodes, even if the nodes are in a cluster.

In addition to the steps listed, a map passall, map, or map shared collector is part of the configuration. For more information, refer to [Associate Inline Networks with Inline Tools Using Inline Maps](#).

For out-of-band maps, refer to [Out-of-Band \(OOB\) Map](#).

For the order in which to configure the software constructs associated with inline bypass solutions, refer to [Associate Inline Networks with Inline Tools Using Inline Maps](#).

The configuration steps in summary for an inline bypass solution are as follows:

1. Configure inline network ports. (Optional for protected inline network.)
2. Configure inline network. (Optional for protected inline network.)
3. (Optional) Configure inline network group.
4. (Optional) Configure heartbeat or negative heartbeat profile.
5. Configure inline tool ports.
6. Configure inline tool.
7. (Optional) Configure inline tool group.
8. (Optional) Configure inline tool series.
9. Configure inline maps, either passall, map (rule-based), map shared collector, or bypass.
10. Configure non-default values for parameters of the inline networks or inline tools.

The summary steps are shown in [Figure 62 Configuration Steps for Inline Bypass Solutions](#).

Figure 62 *Configuration Steps for Inline Bypass Solutions*

Configuration Step Details

This section provides detailed steps for configuring inline bypass.

Configure Inline Network Ports

Use the following procedure to create inline network ports:

1. Go to **System > Ports > Ports > All Ports**.
2. Open Quick Port Editor by clicking the **Port Editor** button.
3. Use the Quick search field to Find the ports to configure.
4. In the Alias field enter a name to help identify the inline port.
5. For Type, select **Inline Network**.

An Inline Network (unprotected) is a software arrangement of two network-type ports allocated to facilitate access to a bidirectional link between two networks (far end network devices) that are linked to inline tool ports.

6. Click **OK**.

NOTE: Any available network-type ports on a Gigamon node can be used to form an unprotected inline network.

Configure Inline Network (Unprotected)

An Inline Network Group is an arrangement of multiple inline network ports to which traffic is distributed based on calculated hash values used by a Gigamon node.

Perform the steps to configure an inline network:

1. After configuring the Inline Network ports, select **Inline Bypass > Inline Networks**.
2. Click **New**.
3. In the **Alias** field, enter an alias for the inline network to help identify the inline network.
4. From the **Port A** drop-down list select an inline network port.
5. An inline network port is automatically selected for **Port B**. To select a different port, select one from the **Port B** drop-down list if there is more than one inline network port.
6. Select a traffic path from the **Traffic** Path drop-down list. The types of traffic paths are:
 - **Bypass** — All traffic arriving at the Port A inline network port is directly forwarded to the Port B inline network port and all traffic arriving at the Port B inline network port is directly forwarded to the Port A inline network port.
 - **Drop** — No traffic is exchanged through the inline network ports (all traffic coming to these ports is dropped).
 - **ByPass with Monitoring** — All traffic is forwarded as a forced bypass value and a copy of the traffic is also forwarded to the inline tools. A traffic map must first be configured between the inline network and the inline tool to have the traffic forwarded with no traffic taken from the inline tools.
 - **To Inline Tool** — The traffic received at the inline network ports is forwarded based on:
 1. The traffic map between the inline network and the respective inline tools.
 2. The failover action attributes of the inline tools
 3. The health state of the inline tools.
7. Select the **Link Propagation** check box to enable whether the inline network link on one side of the inline network gets propagated to the other side.
8. Click **Save**.

Configure Inline Network Group

An Inline Network Group is an arrangement of multiple inline network ports to which traffic is distributed based on calculated hash values used by Gigamon node.

Perform the following steps to configure an Inline Network Group:

1. After configuring the Inline Network Ports, select **Inline Bypass > Inline Network Groups**.
2. Click **New**.
3. In the **Alias** field, enter a name for the network group.
4. From the **Inline Network** drop-down list, select the Inline Network ports.
5. Click **Save**.

Create Heartbeat Profile

The Heartbeat Profile is a data structure that contains the heartbeat attributes that are applied to an Inline Tool for configuring its heartbeat. The Create Heartbeat Profile wizard allows you to apply attribute values for the heartbeat profile. Use the following procedure:

1. Select **Inline Bypass > Heartbeats**.
2. Click **New**.
3. In the **Alias** field, enter a name for your heartbeat profile.
4. In the **Type** field, select **Regular**.
For details about regular heartbeats, refer to [Heartbeats](#).
5. Use **Packet Format** drop-down list to select a packet type. The formats are:
 - **ARP**—This protocol (Address Resolution Protocol) is used for resolution of network layer address into link layer addresses, which is critical for multiple-access network operation. ARP is the default.
 - **Custom**—This format is a binary packet content associated with a packet capture (pcap) file. For details about custom packet format, refer to [Heartbeats](#).
[Heartbeats](#)
When you select **Custom**, a **Custom Format** field displays with a **Browse** button. Use the **Browse** button to upload the pcap file.
6. Use the **Direction** drop-down menu to select the direction for sending heartbeat. The directions are:
 - **A to B**—From Port A to Port B of the inline tool.
 - **B to A**—From Port B to Port A of the inline tool.
 - **Bi-directional**—Both directions.
7. In the **Timeout** field, enter a number in milliseconds to indicate a timeout period for heartbeat packets between sending and receiving. The acceptable range is 20 to 1000 milliseconds. The default is 500 milliseconds.
8. In the **Period** field, enter a number in milliseconds for sending subsequent heartbeat packets. The acceptable range is 30 to 5000 milliseconds. The default is 1000 milliseconds.

9. In the **Recovery Time** field, enter a number in seconds to indicate that the inline tool is declared up with successfully receiving packets. The acceptable range is 5 to 60 seconds. The default is 30 seconds.
10. In the **Retries** field, enter the number for consecutive timed-out heartbeat packets at which the system will trigger (retry) a fail over condition.
11. Click **Save**.

The heartbeat profile appears in the Heartbeat Profile table.

NOTE: Highlight the heartbeat profile and click **Edit** to modify the parameters, if needed.

Create Negative Heartbeat Profile

The Negative Heartbeat Profile is a data structure that contains the negative heartbeat attributes that are applied to an Inline Tool for configuring its negative heartbeat. The Create Heartbeat Profile wizard allows you to apply attribute values for the negative heartbeat profile. Use the following procedure:

1. Select **Inline Bypass > Heartbeats**.
2. Click **New**.
3. In the **Alias** field, enter a name for your heartbeat profile.
4. In the **Type** field, select **Negative**

This is a negative heartbeat profile. For details about negative heartbeats, refer to [Heartbeats](#).

5. Use **Browse** button in the **Custom Format** field to upload binary packet content associated with a packet capture (pcap) file. For details about the custom format, refer to [Heartbeats](#).
6. Use the **Direction** drop-down menu to select the direction for sending heartbeat. The directions are:
 - **A to B**—From Port A to Port B of the inline tool.
 - **B to A**—From Port B to Port A of the inline tool.
 - **Bi-directional**—Both directions.
7. In the **Period** field, enter a number in milliseconds for sending subsequent negative heartbeat packets. The acceptable range is 30 to 5000 milliseconds. The default is 1000 milliseconds.
8. In the **Recovery Time** field, enter the minimum number of seconds since the last negative heartbeat packet is received to declare that the inline tool is up.

The inline tool is up from the standpoint of the negative heartbeat if the negative heartbeats sent are *not* received. When a tool is declared down, sent heartbeats should not be received for a number of seconds in order to declare the tool as being up.

The acceptable range for the Recovery Time field is 5 to 60 seconds. The default is 30 seconds.

9. Click **Save**.

The heartbeat profile appears in the Heartbeat Profile table.

NOTE: Highlight the heartbeat profile and click **Edit** to modify the parameters, if needed.

Configure Inline Tool Ports

Use the following procedure to create inline tool ports:

1. Go to **System > Ports > Ports > All Ports**.
2. Open Quick Port Editor by clicking the **Port Editor** button.
3. Use the Quick search field to Find the ports to configure.
4. In the Alias field enter a name to help identify the inline port.
5. For **Type**, select **Inline Tool**.

An Inline Tool represents a pair of inline tool ports.

6. Click **OK**.

Configure Inline Tool

An Inline Tool represents a pair of inline tool ports. To configure an Inline Tool, do the following:

1. Select **Inline Bypass > Inline Tools**.
2. Click **New**.
3. If needed, click **Port Editor** to open the Quick Port Editor to configure the inline tool ports.
4. Select the inline tool ports for the inline tool.
 - o For **Port A**, select an inline tool port configured in the previous procedure, [Configure Inline Tool Ports](#).
 - o For **Port B**, select another inline tool port configured in the previous procedure, [Configure Inline Tool Ports](#).
5. Select **Enabled** to set the inline tool ports as enabled for inline bypass traffic.
6. For **Failover action**, select one of the following:

- **Tool Bypass** — When the inline tool fails all traffic coming to the respective inline tool is directed via the bypass path.
 - **Network Bypass** — When the inline tool fails the traffic is directed to multiple inline tools associated with an inline network or inline network group using rule-based inline maps.
 - **Tool Drop** — When the inline tool fails all traffic coming to the respective inline tool is dropped.
 - **Network Drop**—When the inline tool fails all traffic coming to the respective inline tool is dropped.
 - **Network Port Forced Down**—When the inline tool fails the inline network ports of the respective inline network are forced as "down".
7. Select the **Recovery Mode**. The recovery mode can be one of the following:
- **automatic**—Specifies automatic recovery, which redirects traffic back to the inline tool as soon as it has recovered from all faulty conditions.
 - **manual**—Specifies manual recovery, which lets you control when to put an inline tool back into service after the tool has recovered. For example, you may want to wait for a maintenance window to return the inline tool to service.
8. Select **Enable Heartbeat** to set the heartbeat.
- If the heartbeat is enabled, do the following:
- a. From **Profile**, select the desired heartbeat profile. The available heartbeat profiles are existing profiles from other inline tools. Once a heartbeat profile is selected, its attributes are displayed.
 - b. In the **HB IP Address A** field, enter the server's IP address to send the heartbeat packets.
 - c. In the **HB IP Address B** field, enter the server's IP address to send a second heartbeat packet.
9. Click **Save**.

Create Inline Tool Group

An Inline Tool Group is an arrangement of multiple Inline Tools to which traffic is distributed based on calculated hash values used by Gigamon node.

To configure an Inline Tool Group, do the following:

1. Use the **Quick Port Editor** to configure the inline tool ports.
2. Select **Inline Bypass > Inline Tool Groups**.
3. Click **New**.
4. In the **Alias** field, enter a name to help identify the inline tool group.
5. For **Inline Tools**, select the inline tool ports for the inline tool group.
6. (Optional) For the **Inline Spare Tool**, select another inline tool port.

If a spare is selected, the inline tool group becomes a redundant arrangement of inline tools. When the first failure occurs in a set of active inline tools, traffic will be forwarded to the spare with no loss, thus the spare will replace the failed tool in the active set.

7. Select **Enable** to enable the inline tool group.
8. Select the **Failover Action**. The failover actions are:
 - **Tool Bypass**—When the inline tool group fails all traffic coming to the respective inline network is directed via the bypass path.
 - **Tool Drop**—When the inline tool group fails all traffic coming to the respective inline network is dropped.
 - **Network Bypass**—When the inline tool group fails all traffic coming to the respective inline network is directed to the inline tool group via the bypass path.
 - **Network Drop**—When the inline tool group fails all traffic coming to the respective inline network group is dropped.
 - **Network Port Forced Down**—When the inline tool group fails the inline network ports of the respective inline network are forced as "down".
9. For **Minimum Healthy Group Size**, select a number that represents the minimal amount of inline tools that are required to have a state of Normal.
10. Select the **Hash** for the inline tool group.

Hashing, which is used for distributing traffic across the inline tools in an inline tool group. The values for the hash parameter are as follows:

- **advanced**—Specifies symmetrical hashing, which is derived from the combination of packet fields based on the criteria selected for the advanced-hash algorithm. For inline bypass applications, the most common choice of criteria for the advanced-hash algorithm is the combination of source IP and destination IP addresses. This produces a hash value that sends all traffic associated with the same session to the same inline tool in the inline tool group.
 - **a-srcip-b-dstip**—Specifies asymmetrical hashing, which is derived from the source IP address for side A of the network and the destination IP address for side B of the network. This produces a hash value that sends all traffic associated with the same source address residing on side A to the same inline tool in the inline tool group, regardless of destination or session.
 - **b-srcip-a-dstip**—Specifies asymmetrical hashing, which is derived from the destination IP address for side A of the network and the source IP address for side B of the network. This produces a hash value that sends all traffic associated with the same source address residing on side B to the same inline tool in the inline tool group, regardless of destination or session.
11. Click **Save**.

Configure Inline Tool Series

To configure an Inline Tool Series, do the following:

1. Select **Inline Bypass > Inline Serial Tools**.
2. Click **New**.
3. In the **Alias** field, enter a name to help identify the inline tool series.
4. For **Inline Tools**, select the inline tool ports for the inline tool series.
5. Select **Enabled** to enable this configuration.
6. Select the **Failover action**.

For details about the failover actions, refer to [Inline Tool Series Local Failover Action](#)

7. Select the **Per Direction Order**.

For details about per-direction order, refer to [Inline Tool Series Per-Direction Order](#).

Configure When GigaVUE-FM,GigaVUE HC Series® HC Series Modules are Operationally Up

Ensure that the GigaVUE-FM,GigaVUE HC Series® HC Series modules are in the operationally *up* state before configuring them. Configuration changes done when a module is operationally *down* are not supported.

Also, when an inline tool or inline tool group is in the operationally *down* state, do not modify the current failover action of that inline tool or inline tool group until the tool has recovered from the failover state.

Avoid Over subscription

In general, traffic received at inline network ports is delivered to the destination ports according to the inline maps and the out-of-band maps regardless of whether the destination ports have the capacity to absorb all the traffic or not.

NOTE: When an inline network is involved in an inline map or an out-of-band map to a destination port (tool port or inline tool port), when there is temporary oversubscription, some packets arriving at the inline network port will be dropped. This can happen when the traffic path is set to bypass or monitoring.

Ensure that destination ports of maps originating from inline network ports have enough capacity to absorb the amount of traffic coming to the inline network ports.

Inline Bypass Solution Examples

The following sections provide examples of inline bypass solutions. The solutions are presented in an order from simple to complex. Refer to the following:

- [Example 1: Unprotected Inline Bypass with an Inline Tool Group](#)
- [Example 2: Unprotected Inline Bypass with Default Heartbeat](#)
- [Example 3: Protected Inline Bypass Using Combo Modules](#)

Example 1: Unprotected Inline Bypass with an Inline Tool Group

Example 1 is a simple, unprotected inline bypass solution. In the example, aliases are used for inline network ports (iN1 and iN2), inline tool ports (iT1 and iT2), inline network (inNet), inline tool (inTool), and inline map (inMap).

On GigaVUE-HC3, an unprotected inline bypass solution can be configured on the bypass combo module with the inline networks and inline tools on ports 1/1/x1..x16 or on ports c1..c4, or on any other module on the GigaVUE-HC3 node.

On GigaVUE-HC1-Plus, an unprotected inline bypass solution can be configured with the inline networks and inline tools on ports 1/1/x1..x16 or on ports x17..x24, or on any other module on the GigaVUE-HC1-Plus node. Refer to [Figure 63 Logical Bypass Without Bypass Combo Module](#) which shows a GigaVUE-HC1-Plus.



Figure 63 Logical Bypass Without Bypass Combo Module

On GigaVUE-HC1-Plus, an unprotected inline bypass solution can be configured on the base module, with the inline networks and inline tools on ports 1/1/x1..x12 and 1/1/g1..g4, or on the bypass combo module on ports x1..x4.

Task	Description	UI Steps
1.	Configure inline network aliases, port type (inline-network), and administratively enable inline network ports.	1. Go to System > Ports > Ports > All Ports. 2. Click Quick Port Editor. 3. Use Quick search to find the ports to configure. In this example, the ports are 3/1/x1 and 3/1/x2 4. Set port 3/1/x1 to Type Inline-Network and select Enable. Enter iN1 for the port alias. 5. Set port 3/1/x2 to Type Inline-Network and select Enable. Enter iN2 for the port alias. 6. Make sure Enable is selected for Admin on the ports. 7. Click OK.
2.	Configure inline network.	1. Select Inline Bypass > Inline Networks. 2. Click New. 3. In the Alias field, type InNet. 4. For Port A, select iN1. 5. For Port B, select iN2. 6. Click Save.
3.	Configure inline tool ports, port type (inline-tool), and administratively enable inline tool ports.	1. Go to System > Ports > Ports > All Ports. 2. Click Quick Port Editor. 3. Use Quick search to find the ports to configure. In this example, the ports are 3/1/x3 and 3/1/x4 4. Set port 3/1/x4 to Type Inline-Tool and select Enable. Enter iT1 for the port alias. 5. Set port 3/1/x4 to Type Inline-Tool and select Enable. Enter iT2 for the port alias. 6. Make sure Enable is selected for Admin on the ports. 7. Click OK.

Task	Description	UI Steps
4.	Configure inline tool, and enable it. Also enable the default heartbeat profile.	1. Select Inline Bypass > Inline Tools. 2. Click New. 3. In the Alias field, type InTool. 4. For Port A, select iT1. 5. For Port B, select li2. 6. Under Configuration: a. Select Enabled b. Select Enabled Heartbeat and set Profile to default. 7. Click Save.
5.	Configure map passall, from inline network to inline tool.	1. Select Maps > Maps. 2. Click New. 3. In the Alias field, type InMap. 4. Select Inline for Type and Pass All for Subtype. 5. For Source, select InNet 6. For Destination, select InTool. 7. Click Save.
6.	Configure the path of the traffic to inline tool.	1. Select Inline ByPass > Inline Networks. 2. Select the Inline Network InNet and click Edit 3. Under Configuration, set the Traffic Path field to To Inline Tool. 4. Click Save.

Example 2: Unprotected Inline Bypass with Default Heartbeat

Example 2 adds the default heartbeat profile to the unprotected inline bypass solution in Example 1.

Task	Description	UI Steps
1.	Configure inline network aliases, port type (inline-network), and administratively enable inline network ports.	5. Go to System > Ports > Ports > All Ports. 6. Click Quick Port Editor. 7. Use Quick search to find the ports to configure. In this example, the ports are 3/1/x1 and 3/1/x2 8. Set port 3/1/x1 to Type Inline-Network and select Enable. Enter iN1 for the port alias. 9. Set port 3/1/x2 to Type Inline-Network and select Enable. Enter iN2 for the port alias. 10. Make sure Enable is selected for Admin on the ports. 11. Click OK.
2.	Configure inline network.	1. Select Inline Bypass > Inline Networks. 12. Click New. 13. In the Alias field, type InNet. 14. For Port A, select iN1. 15. For Port B, select iN2. 16. Click Save.
3.	Configure inline tool ports, port type (inline-tool), and administratively enable inline tool ports.	1. Go to System > Ports > Ports > All Ports. 17. Click Quick Port Editor. 18. Use Quick search to find the ports to configure. In this example, the ports are 3/1/x3 and 3/1/x4 19. Set port 3/1/x4 to Type Inline-Tool and select Enable. Enter iT1 for the port alias. 20. Set port 3/1/x4 to Type Inline-Tool and select Enable. Enter iT2 for the port alias. 21. Make sure Enable is selected for Admin on the ports. 22. Click OK.
4.	Configure default heartbeat profile.	In GigaVUE-FM,GigaVUE HC Series-HVUE, the default heartbeat profile is already configured. To view the profile, select Inline Bypass > Heartbeats.

Task	Description	UI Steps
5.	Configure inline tools, and enable it. Also enable the default heartbeat profile.	1. Select Inline Bypass > Inline Tools. 23. Click New. 24. In the Alias field, type InTool1. 25. For Port A, select iT1. 26. For Port B, select iT2. 27. Under Configuration: a. Select Enabled b. Select Enabled Heartbeat and set Profile to default. 28. Click Save.
6.	Configure map passall, from inline network to inline tool.	1. Select Maps > Maps. 29. Click New. 30. In the Alias field, type InMap. 31. Select Inline for Type and Pass All for Subtype. 32. For Source, select InNet 33. For Destination, select InTool. 34. Click Save.
7.	Configure the path of the traffic to inline tool.	1. Select Inline ByPass > Inline Networks. 35. Select the Inline Network InNet and click Edit 36. Under Configuration, set the Traffic Path field to To Inline Tool. 37. Click Save.

Example 3: Protected Inline Bypass Using Combo Modules

Example 3 is a protected inline bypass solution using bypass combo modules on GigaVUE-HC3. It also configures heartbeat and negative heartbeat profiles.

Protected inline networks are based on the pairs of ports associated with the physical protection switches located on the bypass combo modules. Unlike the unprotected examples, you do not need to configure inline network ports because they are created automatically. On GigaVUE-HC3, the port pairs are numbered for example: 2/2/x17 and 2/2/x18, 2/2/x19 and 2/2/x20, 2/2/x21 and 2/2/x22, 2/2/x23 and 2/2/x24.

You do not need to configure inline networks because they are also created automatically on bypass combo modules. The aliases of the default inline networks are: default_inline_net_2_2_1, default_inline_net_2_2_2, default_inline_net_2_2_3, default_inline_net_2_2_4.

On GigaVUE-HC3, protected inline bypass can be configured on the bypass combo module on ports c1..c4.

On GigaVUE-HC1, protected inline bypass can be configured on the bypass combo module. It can also be configured on the TAP-HC1-G10040 module placed in either bay 2 or bay 3, so the ports will be 1/2/g1..g8 or 1/3/g1..g8.

NOTE: The default value of the physical-bypass attribute of protected inline networks is set to enable, which means that the fibers attached to ports net-a and net-b of the inline network are optically coupled and the traffic is exchanged between end nodes without coming to the switching fabric. of the GigaVUE-FM,GigaVUE HC Series node. As shown in Example 4, after configuring the inline tool and the map passall, the physical-bypass attribute is set to disable in order to activate the Inline Bypass solution.

Task	Description	UI Steps
1.	Configure inline tool aliases, port type (inline-tool), and administratively enable inline network ports.	1. Go to System > Ports > Ports > All Ports . 38. Click Quick Port Editor. 39. Use Quick search to find the ports to configure. In this example, the ports are 2/2/x11 and 2/2/x12 40. Set port 2/2/x11 to Type Inline Tool and select Enable. Enter iT1 for the port alias. 41. Set port 2/2/x12 to Type Inline Tool and select Enable. Enter iT2 for the port alias. 42. Click OK.
2.	Configure a heartbeat profile.	1. Select Inline Bypass > Heartbeats. 43. Click New. 44. In the Alias field, type hb2. 45. For Type, select Regular. 46. Click Save.
3.	Configure negative heartbeat profile alias and PCAP file	1. Select Inline Bypass > Heartbeats. 47. Click New. 48. In the Alias field, type nhb1. 49. For Type, select Negative. 50. Click the Browse button for Custom Format and upload the pcap file; for example, hnb.pcap. 51. Click Save.
4.	Configure inline tools, and enable them. Also specify the heartbeat profile.	1. Select Inline Bypass > Inline Tools. 52. Click New. 53. In the Alias field, type InTool1. 54. For Port A, select iT1. 55. For Port B, select iT2. 56. Under Configuration:

Task	Description	UI Steps
		a. Select Enabled b. Select Enabled Regular Heartbeat and set Profile to hb2. c. Select Enabled Negative Heartbeat and set Negative Heartbeat Profile to nhb1. 57. Click Save. Configure the second inline tool. 1. Select Inline Bypass > Inline Tools. 58. Click New. 59. In the Alias field, type InTool2. 60. For Port A, select iT3. 61. For Port B, select iT4. 62. Under Configuration: a. Select Enabled b. Select Enabled Heartbeat and set Profile to hb_custom. 63. Click Save.
5.	Configure the inline tool group and enable it.	1. Select Inline Bypass > Inline Tool Group 64. Click New. 65. In the Alias field, type inToolGroup. 66. For Inline Tools, select InTool1 and InTool2. 67. Under Configuration, select Enabled. 68. Click Save.
6.	Configure map passall, from inline network to inline tool.	1. Select Maps > Maps. 69. Click New. 70. In the Alias field, type InMap. 71. Select Inline for Type and Pass All for Subtype. 72. For Source, select default_inline_net_2_2_1 73. For Destination, select InTool1 74. Click Save.
7.	Configure the path of the traffic to inline tool and disable the physical bypass	1. Select Inline ByPass > Inline Networks. 75. Select the Inline Network default_inline_net_2_2_1 and click Edit 76. Under Configuration, set the Traffic Path field to To Inline Tool. 77. Make sure Physical Bypass is not selected. 78. Click Save.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)