RSA® NETWITNESS®
Packets
Implementation Guide

Gigamon Out-of-Band and Inline SSL Solution

Jeffrey Carlson, RSA Partner Engineering

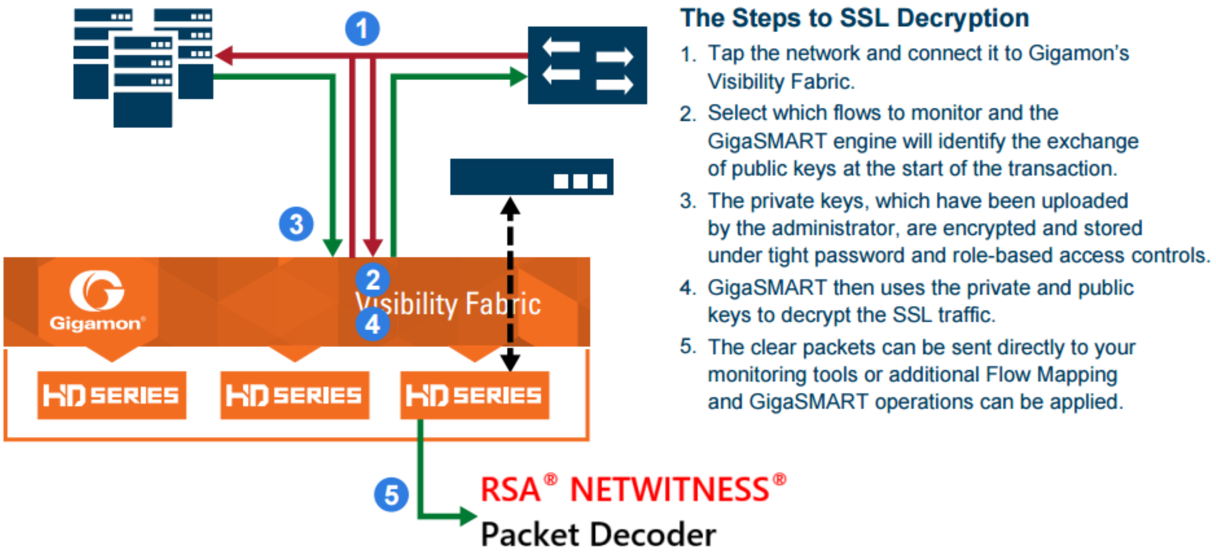
Last Modified: April 27th, 2017

RSA READY

Gigamon Out-of-Band SSL Solution Summary

SSL is a vital Internet technology upon which more and more applications rely. However, it severely limits visibility for both performance and security monitoring. The growing security threat posed by uninspected SSL sessions increases the urgency for inspecting SSL traffic. By decrypting SSL traffic for out-of-band monitoring Gigamon provides visibility where none existed. Rather than turning a blind eye to SSL traffic, the full capabilities of Flow Mapping and GigaSMART traffic intelligence can be applied.

Decrypting SSL is a tremendous processing burden for monitoring tools that do it themselves; this greatly inhibits tool performance and increases the cost of monitoring. By supplying clear, decrypted traffic to multiple tools, such as the RSA NetWitness Suite, Gigamon provides immediate value and return on investment in capital expenditure, licensing fees, and management costs.



The Steps to SSL Decryption

1. Tap the network and connect it to Gigamon's Visibility Fabric.
2. Select which flows to monitor and the GigaSMART engine will identify the exchange of public keys at the start of the transaction.
3. The private keys, which have been uploaded by the administrator, are encrypted and stored under tight password and role-based access controls.
4. GigaSMART then uses the private and public keys to decrypt the SSL traffic.
5. The clear packets can be sent directly to your monitoring tools or additional Flow Mapping and GigaSMART operations can be applied.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Gigamon GigaSMART with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Gigamon GigaSMART components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Gigamon GigaSMART is properly configured and secured before deploying to a production environment. For more information, please refer to the Gigamon GigaSMART documentation or website.

Gigamon GigaSMART Configuration

Given that Gigamon's Unified Visibility Fabric™ has access to bidirectional traffic, it has the ability to observe the exchange of public keys at the start of a transaction. Once an administrator loads the private keys, they are securely stored on the system. The power of the GigaSMART® traffic intelligence engine can then decrypt the traffic and forward it to tools for analysis. Each GigaSMART module contains high-performance compute engines that have hardware performance accelerators to handle SSL traffic.

Configuration Overview

Enabling SSL Decryption involves the following general steps:

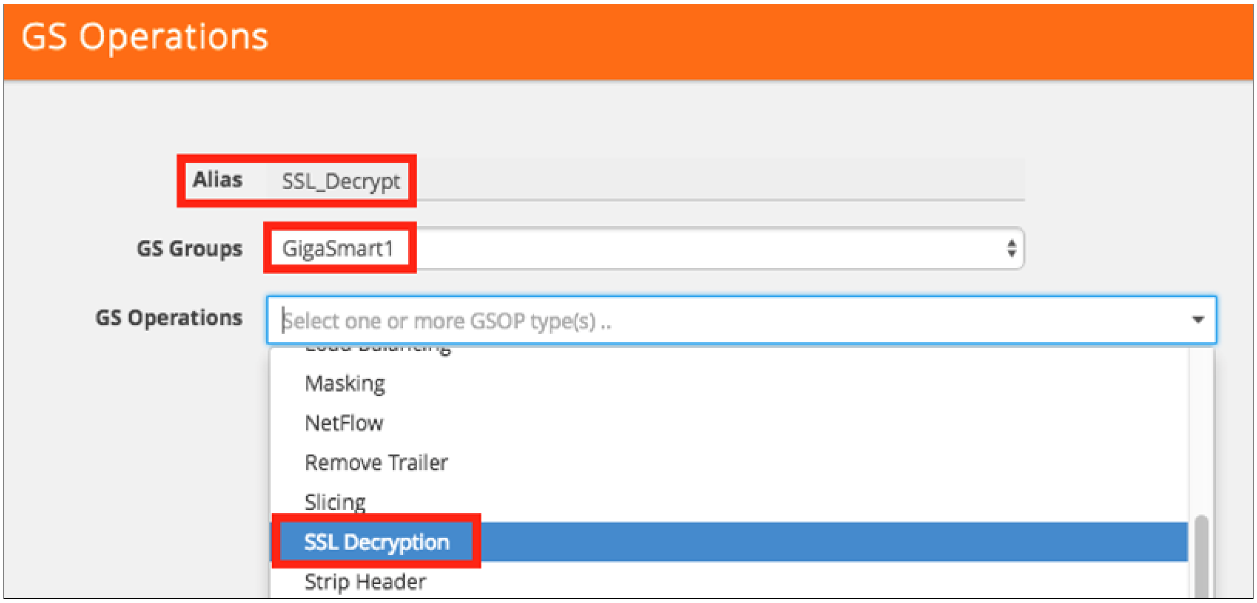
- Configure the GigaSMART Engine Group SSL parameters
- Create an SSL Keychain Password
- Add an SSL Private Key
- Create SSL Service
- Create Pass All Map for SSL
- Create SSL Decryption Map

For more information or details, consult the **GigaSMART SSL Decryption** section of the ***GigaVUE-OS H-VUE User's Guide***.

Configure GigaSMART Engine Group

To configure the GigaSMART Engine Group, do the following:

1. Select **GigaSMART** > **GigaSMART Operations** > **New**
2. On the GigaSMART Operation configuration page, do the following:
   - Enter an alias.
   - For GigaSMART Groups select GigaSmart1.
   - For GigaSMART Operations select **SSL Decryption**
   - Click **Save**.



GS Operations

Alias: SSL_Decrypt

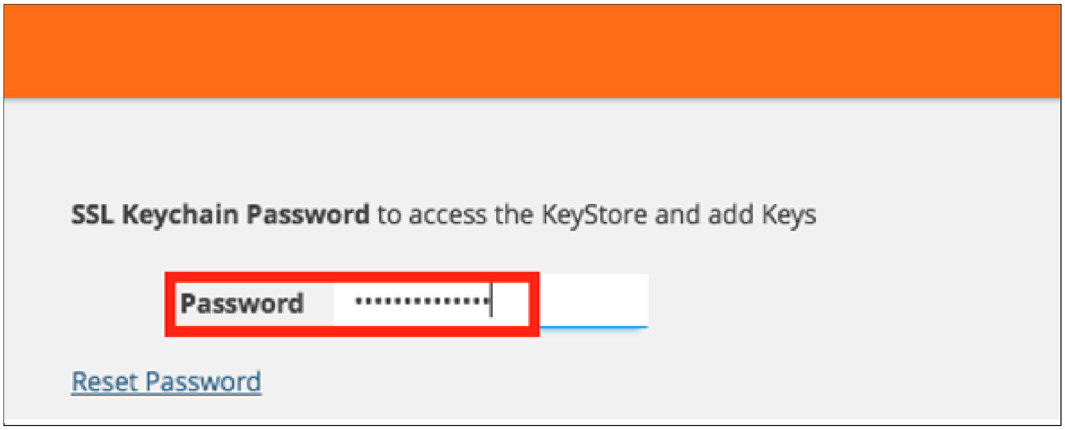
GS Groups: GigaSmart1

GS Operations: Select one or more GSOP type(s) ..

Creating Passwords

Before uploading keys or configuring SSL, you must create an SSL keychain password. The password is used to encrypt the private keys that you upload to the node. To create an SSL keychain password, use the following steps:

1. Select **GigaSMART** > **SSL** > **SSL Keys**.
2. Click **Password**.
3. Enter a password in the Password and Confirm Password fields.



SSL Keychain Password to access the KeyStore and add Keys

Password ••••••••••••••

You can only configure a strong password. A strong password has at least ten (10) characters and at least three (3) of the following:

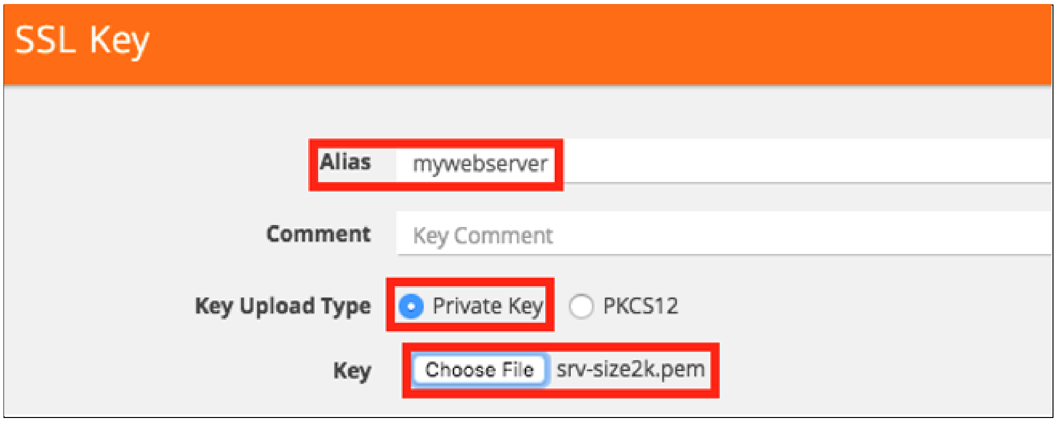
- uppercase letters
- lowercase letters
- numbers
- special characters

4. Click **Submit**.

Uploading SSL Private Keys

SSL Private Keys must be uploaded to the GigaVUE H Series node using a unique alias. To upload an SSL private key, do the following:

1. Select **GigaSMART > SSL Decryption > SSL Keys**.
2. Click **Install**.
3. Enter an alias for the SSL key in the **Alias** field.
4. Select **Private Key** for the upload type.
5. Browse to the desired certificate file.



SSL Key

Alias mywebserver

Comment Key Comment

Key Upload Type ● Private Key ○ PKCS12

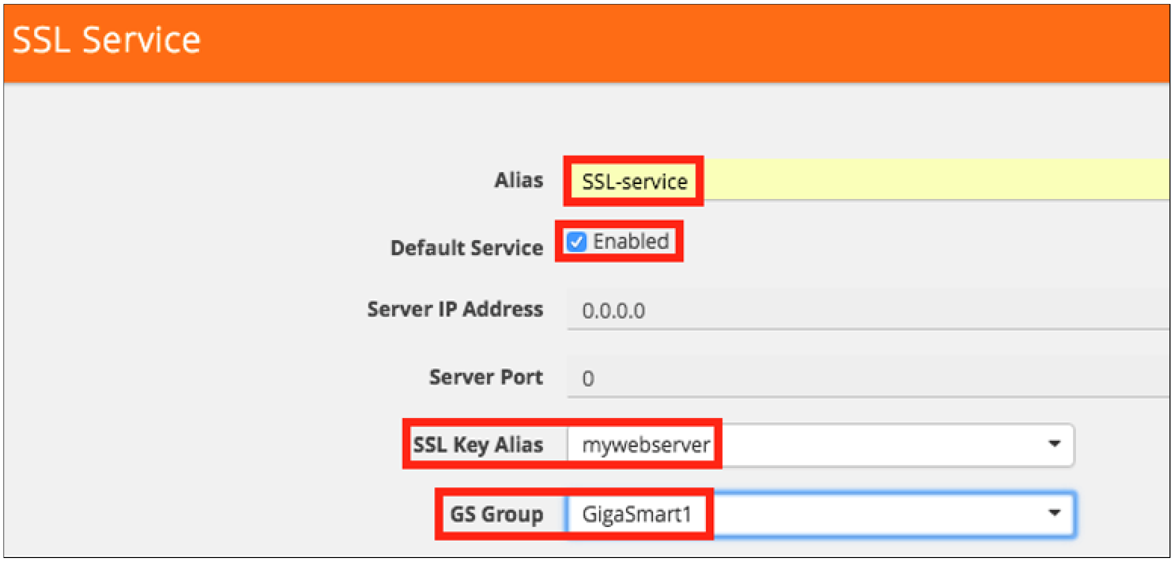
Key srv-size2k.pem

6. Click **Save.**

Creating an SSL Service

To create a service, do the following:

1. Select **GigaSMART > SSL Decryption > SSL Services**.
2. Click **New**.
3. On the SSL Service configuration page, do the following:
   - Enter an alias.
   - Select **Default Service**.
   - Select the alias of SSL Key previously uploaded.
   - Select the GigaSMART Group with SSL decryption enabled to associate with this SSL service.



SSL Service

Alias: SSL-service

Default Service: ☑ Enabled

Server IP Address: 0.0.0.0

Server Port: 0

SSL Key Alias: mywebserver

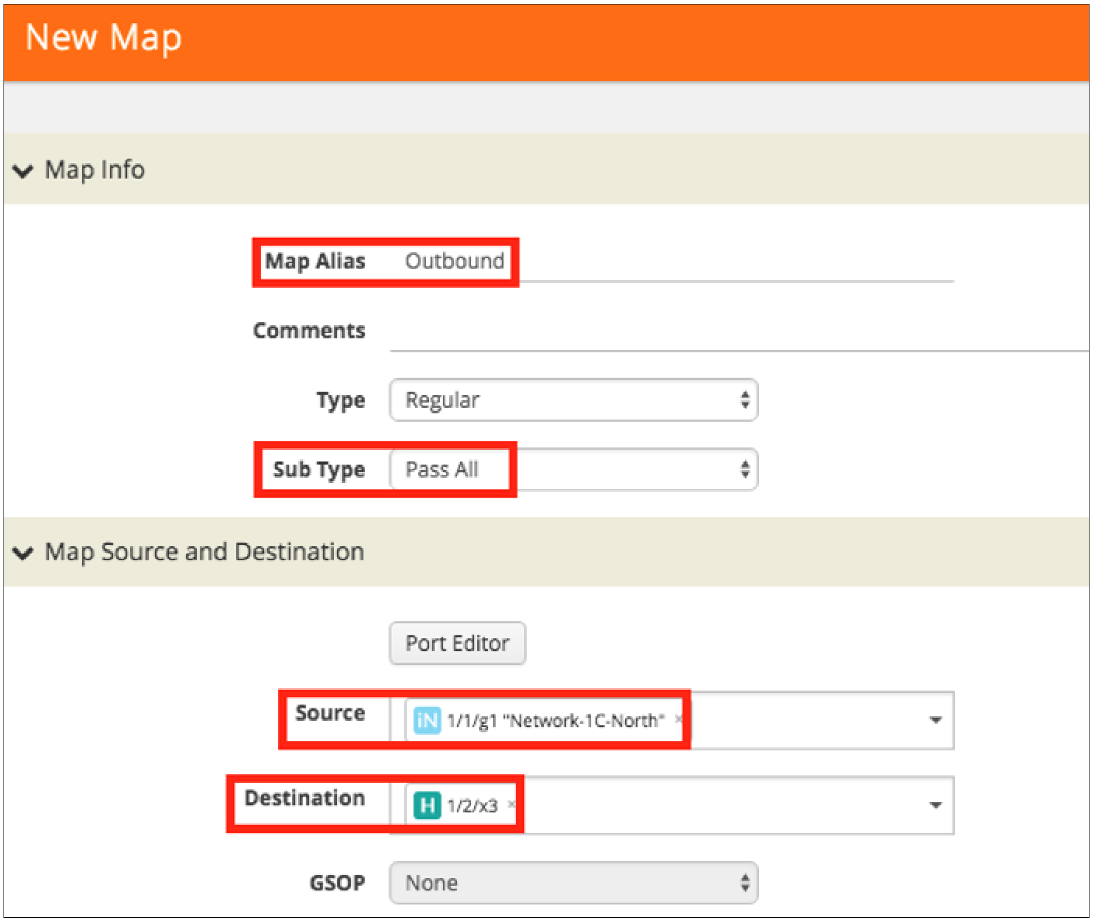
GS Group: GigaSmart1

4. Click **Save**.

Create Pass All Map for SSL

To create the Map, do the following:

1. Select **Maps > New**.
2. On the New Map configuration page, do the following:
   - Enter an alias.
   - Set the Sub Type to **Pass All**.
   - Set the Source to one of the ports in your Inline Network.
   - Set the Destination to a Hybrid or Tool Port. Use the Port Editor if you don’t have these ports enabled.
   - Click **Save**.



New Map

Map Info

Map Alias: Outbound

Comments:

Type: Regular

Sub Type: Pass All

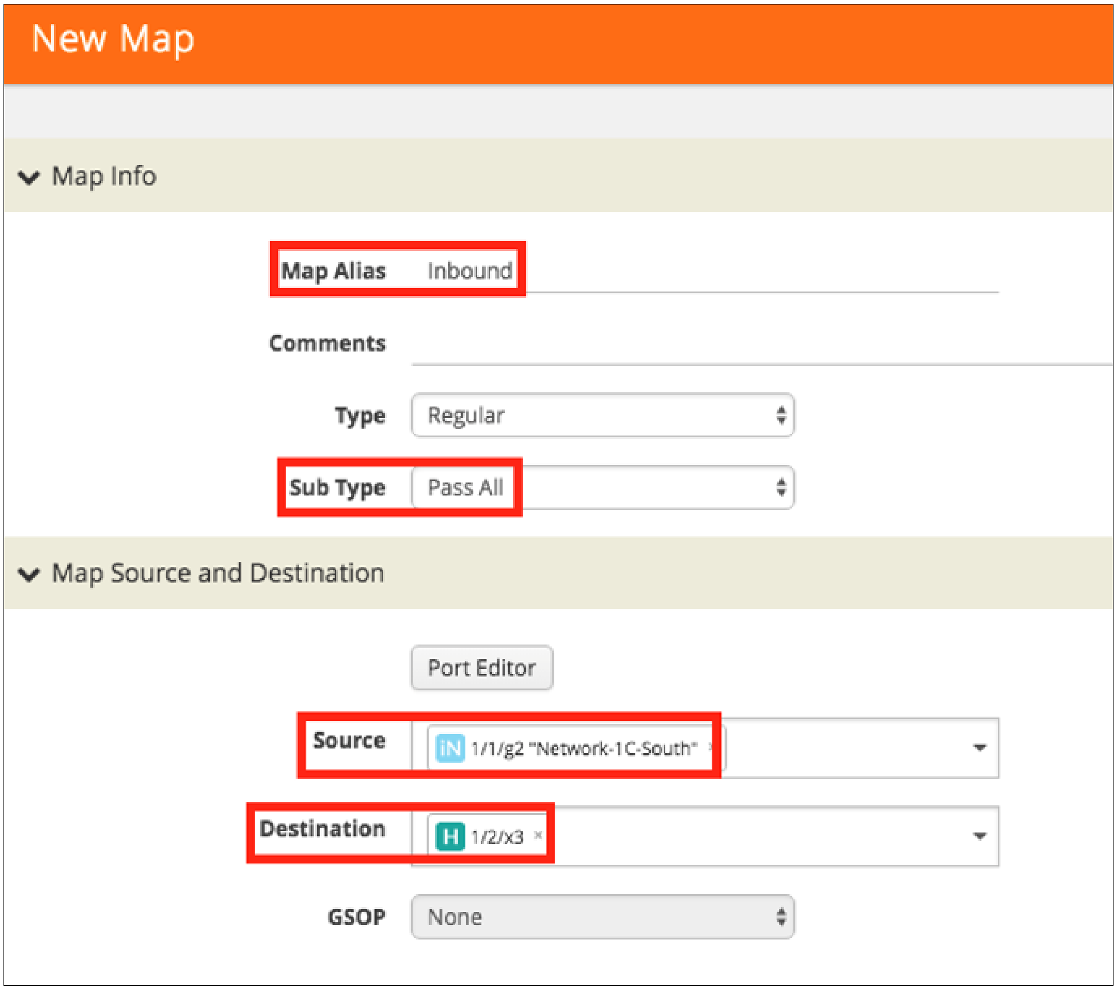
Map Source and Destination

Source: iN 1/1/g1 "Network-1C-North"

Destination: H 1/2/x3

GSOP: None

3. Click **New**.
4. On the New Map configuration page, do the following:
   - Enter an alias.
   - Set the Sub Type to **Pass All**.
   - Set the Source to the other port in your Inline Network.
   - Set the Destination to the same Hybrid or Tool Port as the previous step.
   - Click **Save**.



New Map

Map Info

Map Alias: Inbound

Comments:

Type: Regular

Sub Type: Pass All

Map Source and Destination

Source: iN 1/1/g2 "Network-1C-South"

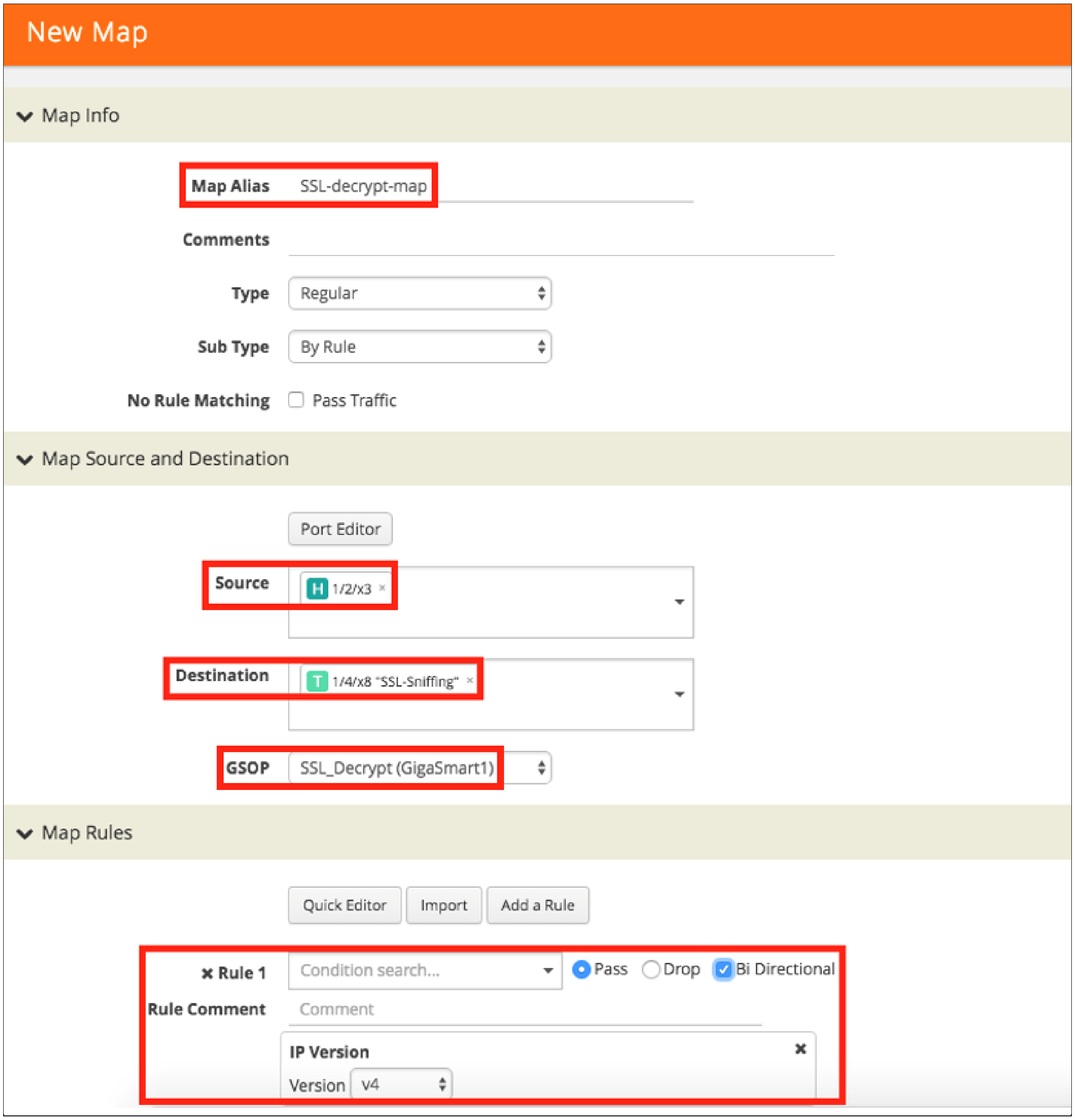
Destination: H 1/2/x3

GSOP: None

Create SSL Decryption Map

To create the Map, do the following:

1. Select **Maps > New**.
2. On the New Map configuration page, do the following:
    - Enter an alias.
    - Set the Source to the Hybrid or Tool Port used in the previous Map.
    - Set the Destination to a Tool port where the Decrypted traffic will be sent. Use the Port Editor if you don't have a Tool port enabled.
    - Set the GigaSMART Operations Group configured in the previous steps.
    - Under Map Rules click **Add a Rule > IP Version 4 > Bi Directional > Save**



New Map

Map Info

Map Alias SSL-decrypt-map

Comments

Type Regular

Sub Type By Rule

No Rule Matching □ Pass Traffic

Map Source and Destination

Port Editor

Source H 1/2/x3

Destination T 1/4/x8 "SSL-Sniffing"

GSOP SSL_Decrypt (GigaSmart1)

Map Rules

Quick Editor | Import | Add a Rule

Rule 1 Condition search... ● Pass ○ Drop ☑ Bi Directional

Rule Comment Comment

IP Version

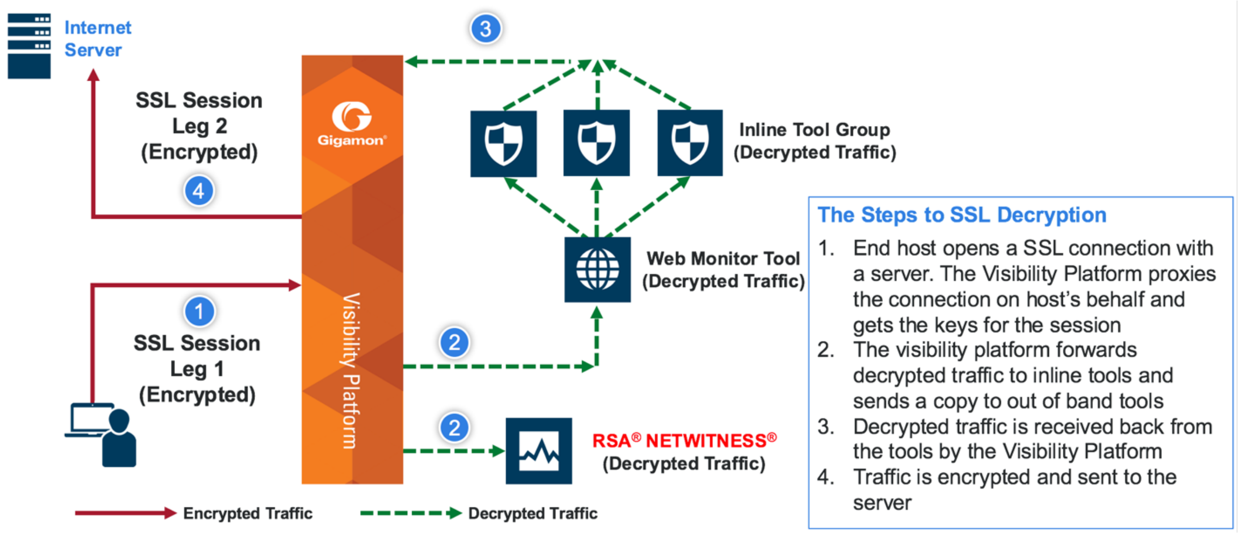
Version v4

Once the configuration has been completed, the decrypted packets can be captured by an RSA NetWitness Packet Decoder for further analysis and inspection.

Gigamon Inline SSL Solution Summary

SSL is a vital Internet technology upon which more and more applications rely. Gartner predicts that more than 80% of enterprise traffic will be encrypted through 2019[1]. However, it severely limits visibility for both performance and security monitoring. The growing security threat posed by uninspected SSL sessions increases the urgency for inspecting SSL traffic. Rather than turn a blind eye to SSL traffic, we can apply the full capabilities of Flow Mapping and Gigamon's inline SSL decryption solution to address this challenge.

Decrypting SSL inline for PFS ciphers like Diffie-Hellman is a tremendous processing burden for monitoring tools that do it themselves; this greatly inhibits tool performance and increases the cost of monitoring. By supplying clear, decrypted traffic to inline tools and out-of-band tools, such as the RSA NetWitness Suite, Gigamon provides immediate value and return on investment in capital expenditure, licensing fees, and management costs.


Internet Server
3
SSL Session Leg 2 (Encrypted)
4
Gigamon
Inline Tool Group (Decrypted Traffic)
Web Monitor Tool (Decrypted Traffic)
1
SSL Session Leg 1 (Encrypted)
Visibility Platform
2
2
RSA® NETWITNESS® (Decrypted Traffic)
Encrypted Traffic
Decrypted Traffic

The Steps to SSL Decryption

1. End host opens a SSL connection with a server. The Visibility Platform proxies the connection on host's behalf and gets the keys for the session
2. The visibility platform forwards decrypted traffic to inline tools and sends a copy to out of band tools
3. Decrypted traffic is received back from the tools by the Visibility Platform
4. Traffic is encrypted and sent to the server

[1] Source: Gartner "Predicts 2017: Network and Gateway Security", December 13 2016.

Partner Product Configuration

Before You Begin

This document is not intended to suggest optimum installations or configurations. This section provides instructions for configuring Gigamon Inline SSL solution with RSA NetWitness.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components. All Gigamon inline SSL decryption solution components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Gigamon inline SSL decryption solution is properly configured and secured before deploying to a production environment. For more information, please refer to the Gigamon inline SSL decryption solution documentation or website.

Gigamon Inline SSL Decryption Configuration

Gigamon's Visibility Platform is uniquely positioned with access to bidirectional traffic. It has the ability to proxy the SSL connection to the server on an end host's behalf and generate the session keys for traffic decryption. Once the keys are generated, they are used to decrypt traffic. The decrypted traffic is sent to inline tools, with a copy forwarded to out-of-band tools. The decrypted traffic that is received back from the inline tools is re-encrypted by the visibility platform and sent to the server. Each GigaSMART module contains high-performance compute engines that have hardware performance accelerators to handle SSL traffic.

Configuration Overview

Enabling SSL Decryption involves the following general steps:

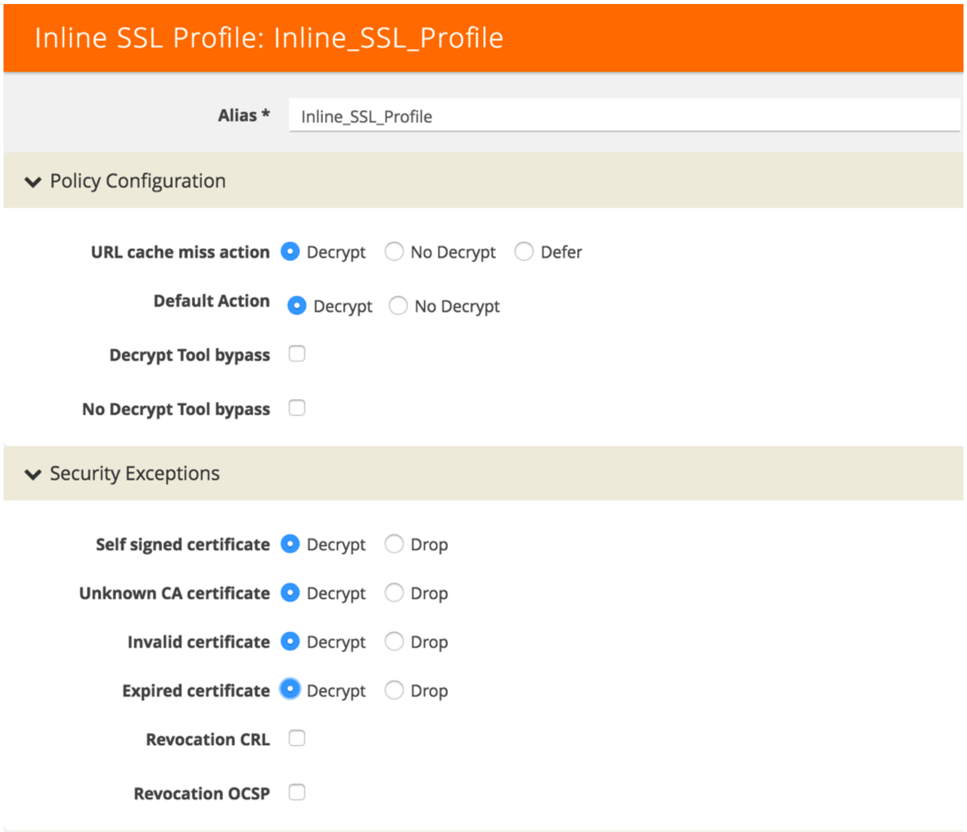
- Configure the Inline SSL Profile
- Configure GigaSMART Engine Group and GigaSMART Operations
- Creating Key Store Password and Generating a Signing CA
- Attaching Key Pair to the Signing CA
- Configuring the Inline Tool
- Creating Maps for Inline SSL

For more information or details, consult the **GigaSMART Inline SSL Decryption** section of the ***GigaVUE-OS H-VUE User's Guide***.

Configure Inline SSL Profile

To configure the Inline SSL Profile, do the following:

3. Select **GigaSMART** > **Inline SSL** > **New**
4. On the Inline SSL Profile configuration page, do the following:
    - Enter an alias.
    - Under **Policy Configuration** and **Security Exceptions** set everything to **Decrypt** and hit **OK**.



Inline SSL Profile: Inline_SSL_Profile

Alias * Inline_SSL_Profile

Policy Configuration

URL cache miss action ● Decrypt ○ No Decrypt ○ Defer

Default Action ● Decrypt ○ No Decrypt

Decrypt Tool bypass □

No Decrypt Tool bypass □

Security Exceptions

Self signed certificate ● Decrypt ○ Drop

Unknown CA certificate ● Decrypt ○ Drop

Invalid certificate ● Decrypt ○ Drop

Expired certificate ● Decrypt ○ Drop

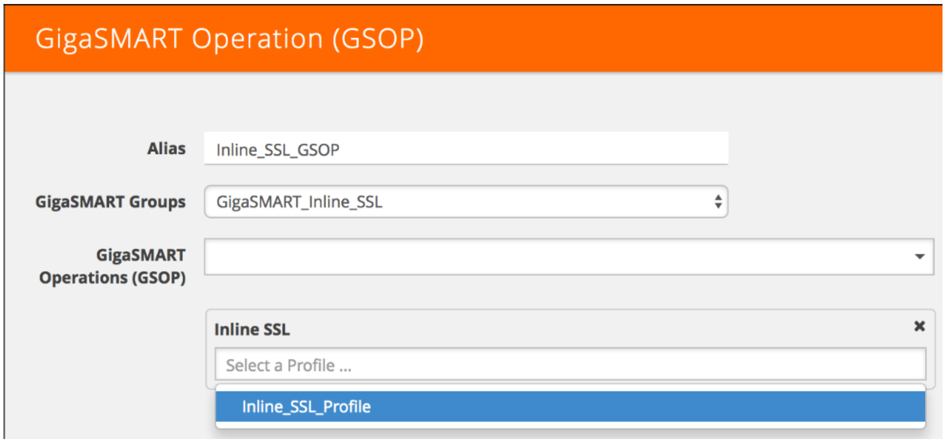
Revocation CRL □

Revocation OCSP □

Configure GigaSMART Engine Group and GigaSMART Operations

To configure the GigaSMART Engine Group, do the following:

5. Select **GigaSMART** > **GigaSMART Operations** > **New**
6. On the GigaSMART Operation configuration page, do the following:
    - Enter an alias.
    - For GigaSMART Groups select **GigaSMART_Inline_SSL**
    - For GigaSMART Operations select **Inline SSL**
    - Click **Save**.



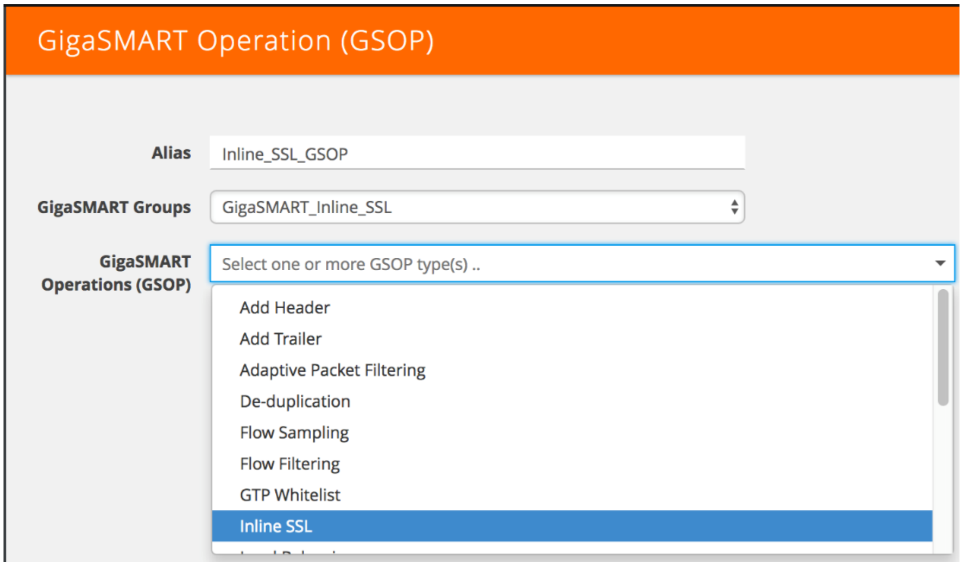
GigaSMART Operation (GSOP)

Alias: Inline_SSL_GSOP

GigaSMART Groups: GigaSMART_Inline_SSL

GigaSMART Operations (GSOP):

Inline SSL: Select a Profile ...



GigaSMART Operation (GSOP)

Alias: Inline_SSL_GSOP

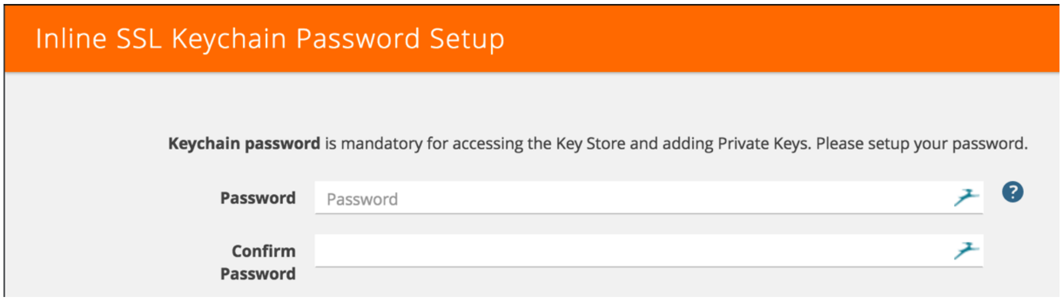
GigaSMART Groups: GigaSMART_Inline_SSL

GigaSMART Operations (GSOP): Select one or more GSOP type(s) ..

Creating Key Store Password and Generating a Signing CA

Before configuring SSL, you must create an SSL Keychain password. The password is used to encrypt the private keys that you upload to the node. To create an SSL keychain password, use the following steps:

5. Select **GigaSMART** > **Inline SSL** > **Key Store**
6. Click **Keychain Password**
7. Enter a password in the **Password** and **Confirm Password** fields.



Inline SSL Keychain Password Setup

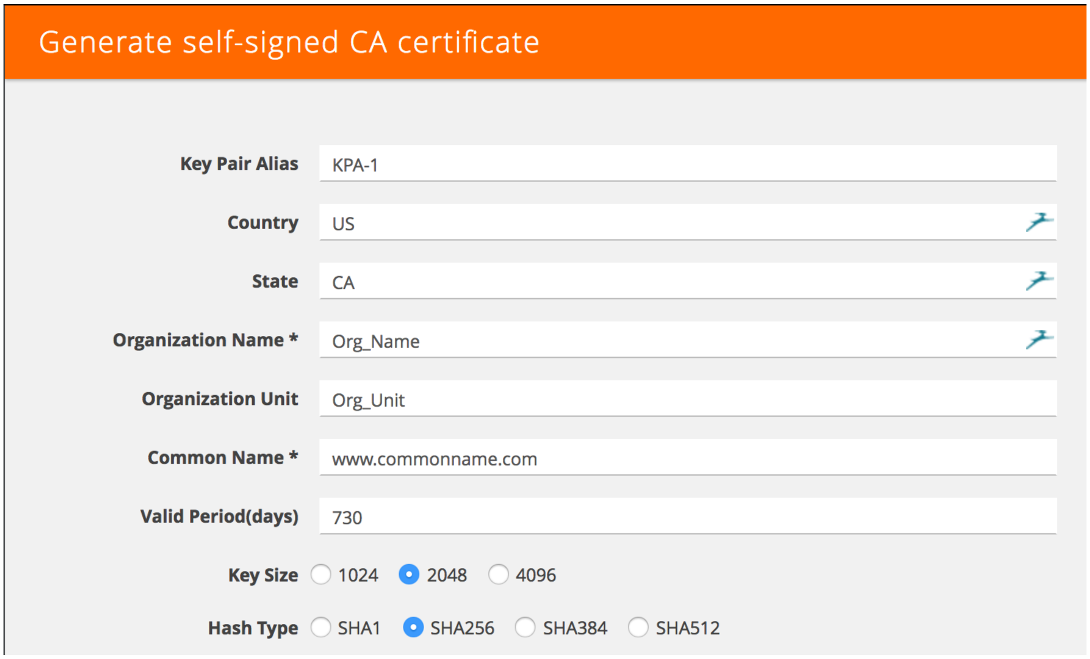
Keychain password is mandatory for accessing the Key Store and adding Private Keys. Please setup your password.

Password	Password
Confirm Password	

You can only configure a strong password. A strong password has at least ten (10) characters and at least three (3) of the following:

- uppercase letters
- lowercase letters
- numbers
- special characters

8. Click **Submit**.
9. Click **Actions > Generate Certificate.**
10. Enter relevant details in the various fields like **Key Pair Alias, Country** etc. and hit OK



Generate self-signed CA certificate

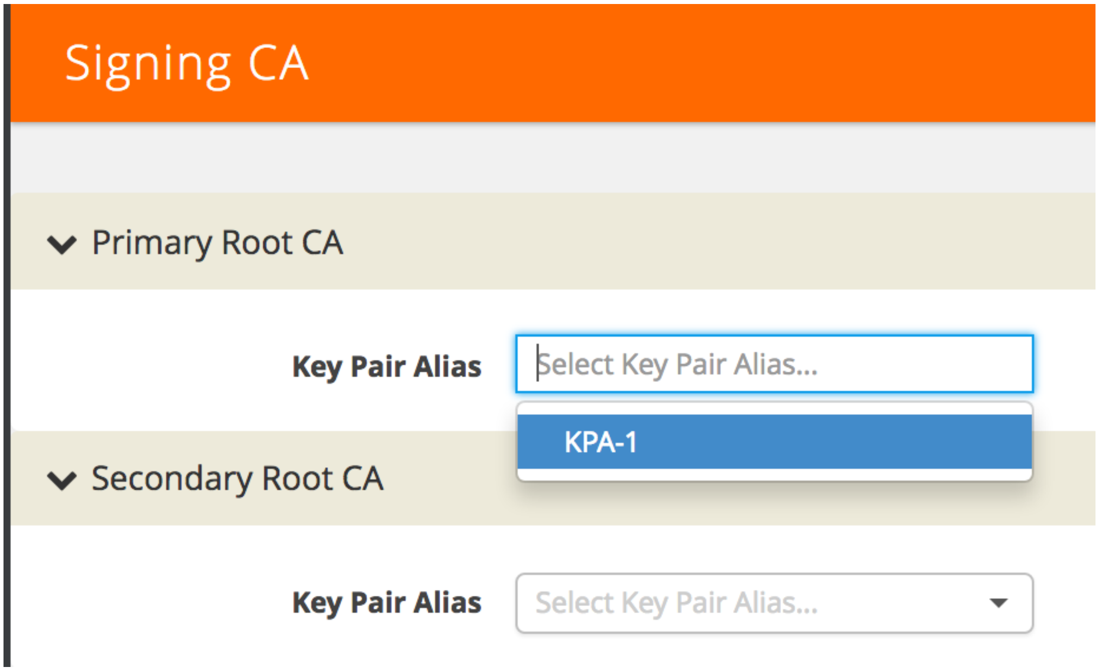
Key Pair Alias	KPA-1
Country	US
State	CA
Organization Name *	Org_Name
Organization Unit	Org_Unit
Common Name *	www.commonname.com
Valid Period(days)	730
Key Size	○ 1024 ● 2048 ○ 4096
Hash Type	○ SHA1 ● SHA256 ○ SHA384 ○ SHA512

Attaching Key Pair to the Signing CA

The Key Pair generated in the previous step needs to be attached to the Signing CA.

1. Click **Inline SSL**
2. Click **Signing CA > Add**

3. In **Primary Root CA** under **Key Pair Alias** select the key pair generated in the last step and click OK



Signing CA

Primary Root CA

Key Pair Alias: Select Key Pair Alias...

KPA-1

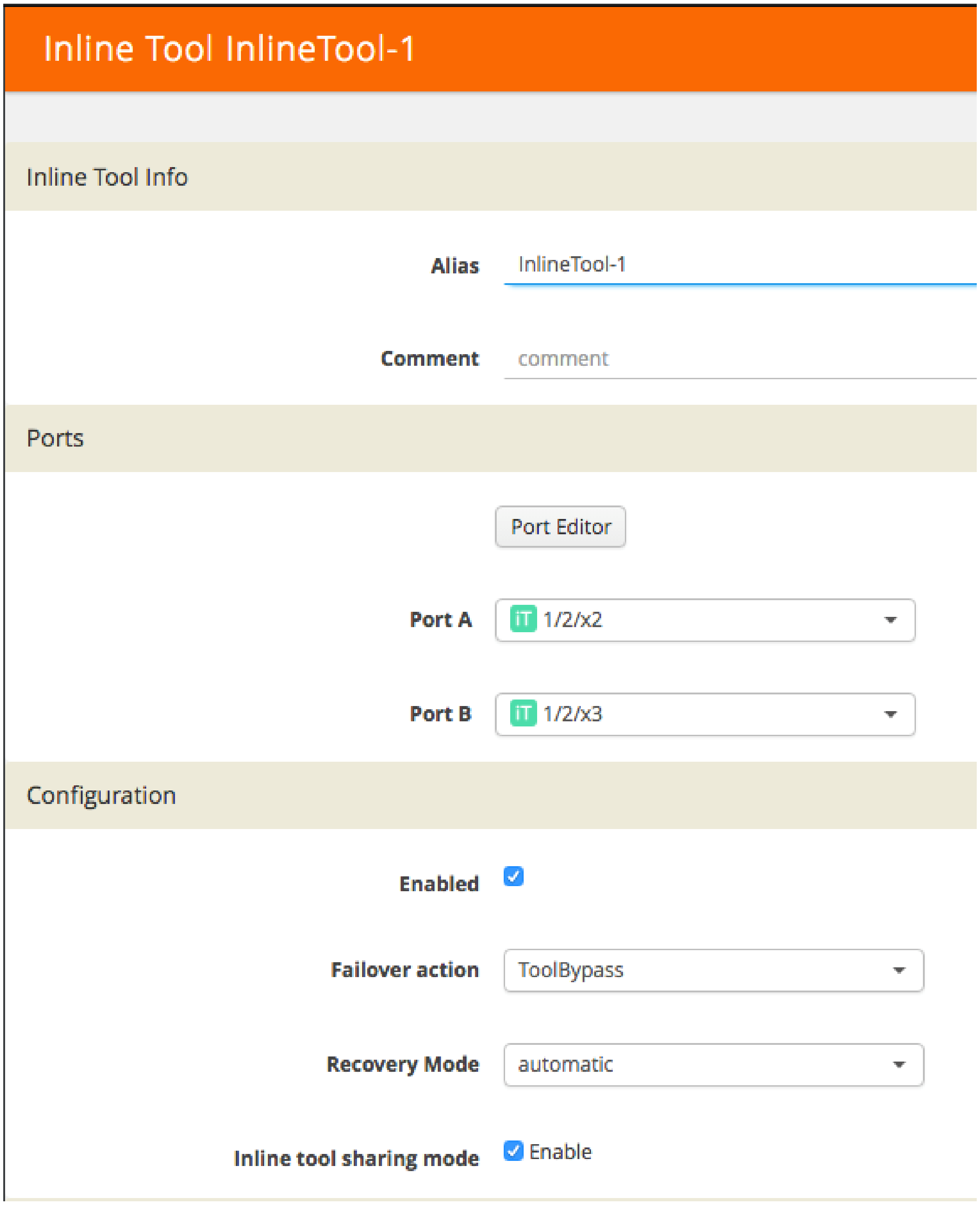
Secondary Root CA

Key Pair Alias: Select Key Pair Alias...

Configuring the Inline Tool

To create Inline Tool, do the following:

5. Navigate to **Inline Bypass** > **Inline Tools**
6. Click **New** and enter the information like **Alias, Ports A and B**
7. Click **Enabled** and **Inline tool sharing mode** and then **OK**



Inline Tool InlineTool-1

Inline Tool Info

Alias: InlineTool-1

Comment: comment

Ports

Port A: IT 1/2/x2

Port B: IT 1/2/x3

Configuration

Enabled: ☑

Failover action: ToolBypass

Recovery Mode: automatic

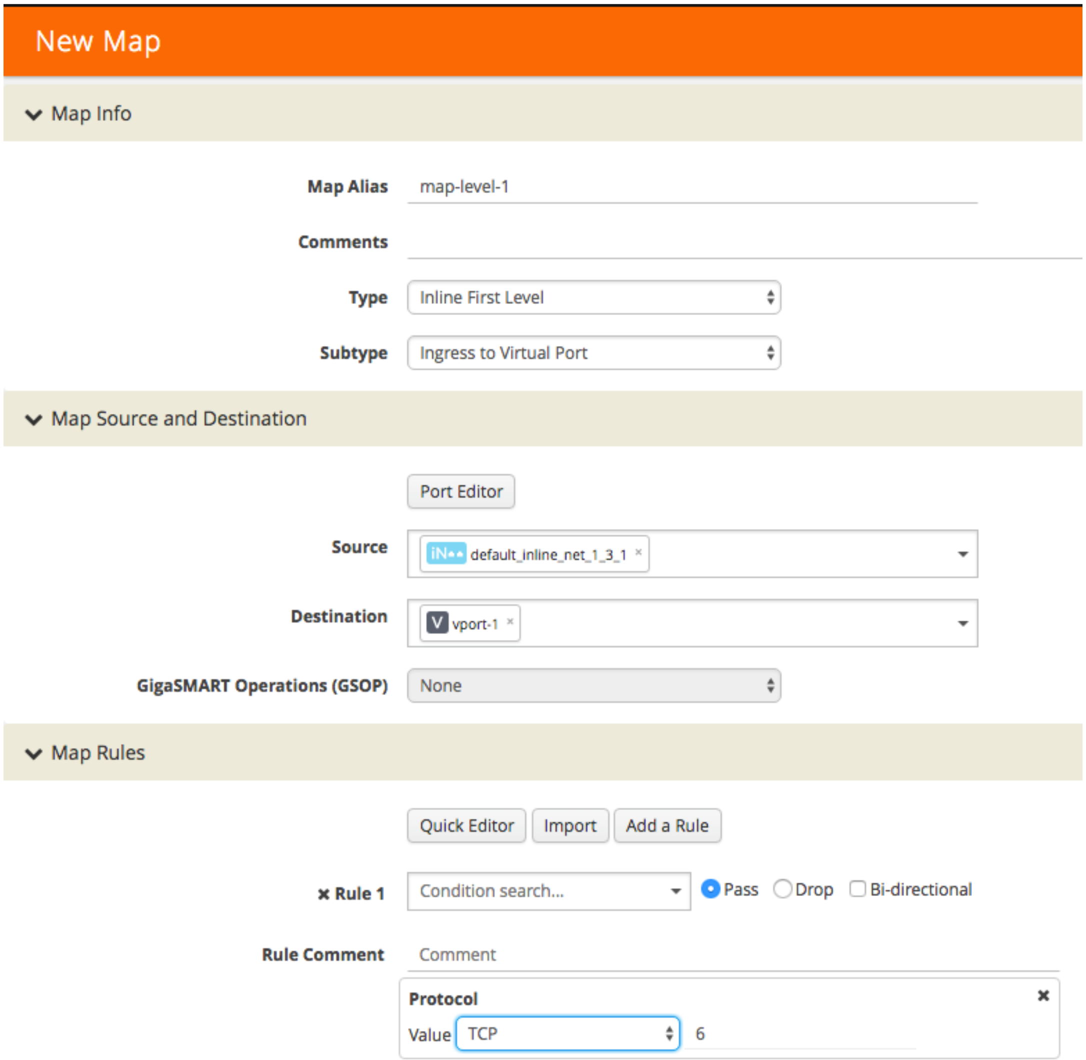
Inline tool sharing mode: ☑ Enable

Creating Maps for Inline SSL

To create Maps, do the following. Since inline SSL is a GigaSMART operation it uses virtual port for traffic.

8. First create a virtual port by navigating to **GigaSMART** > **Virtual Ports**
9. Enter an **Alias and select a GigaSMART Group** then click **OK**
10. Navigate to **Maps** and select **New**. In the **New** Map configuration page, do the following:
    - Enter an alias

- Set the Type to **Inline First Level**
- Set the Subtype to **Ingress to Virtual Port**
- Set the **Source** to one of the ports in your Inline Network
- Set the **Destination** to virtual port created in steps 1 and 2
- Since SSL is intercepted for TCP, it is recommended to add TCP to the Rule. Click on **Add a Rule** and select **TCP** under **Protocol**
- Click **Save**.



New Map

Map Info

Map Alias: map-level-1
Comments:
Type: Inline First Level
Subtype: Ingress to Virtual Port

Map Source and Destination

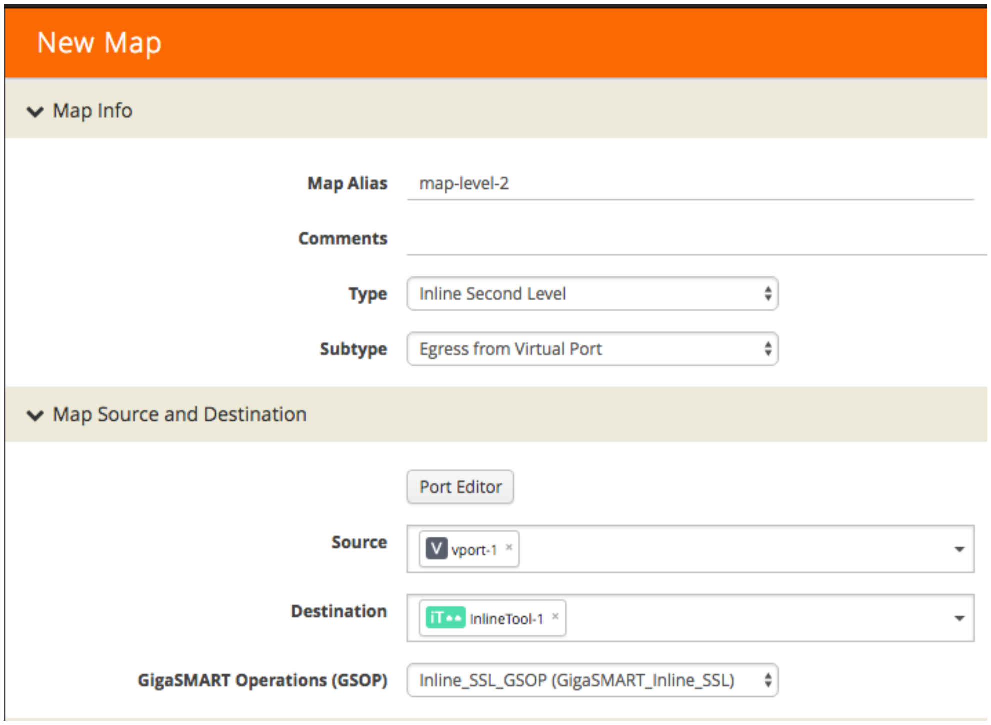
Source: default_inline_net_1_3_1
Destination: vport-1
GigaSMART Operations (GSOP): None

Map Rules

Rule 1: Condition search... ● Pass ○ Drop □ Bi-directional
Rule Comment: Comment
Protocol
Value: TCP 6

11. Now to create the second level map, click **New**.
12. On the New Map configuration page, do the following:
    - Enter an **alias**
    - Set the Type to **Inline Second Level**
    - Set the Subtype to **Egress from Virtual Port**

- Set the Source to the virtual port configured in step 3
- Set the Destination to the inline tool added previously
- Set the GigaSMART Operations (GSOP) to the GSOP created earlier
- Click **Save**.



New Map

Map Info

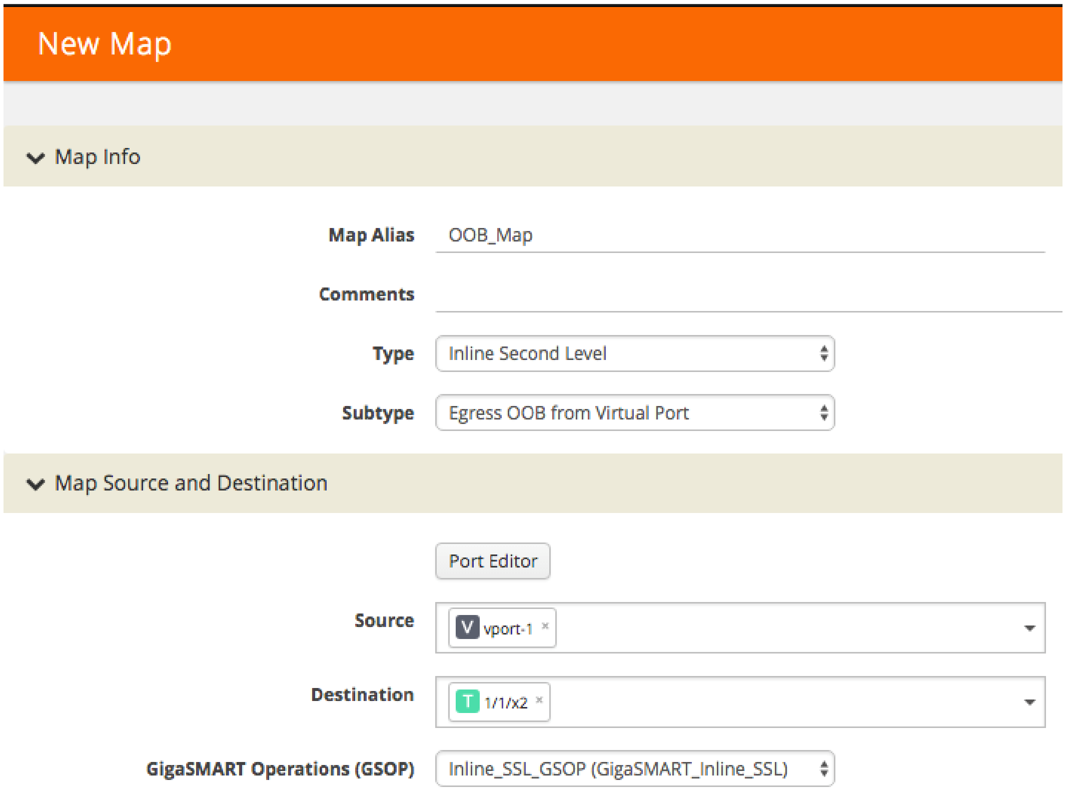
Map Alias: map-level-2
Comments:
Type: Inline Second Level
Subtype: Egress from Virtual Port

Map Source and Destination

Source: vport-1
Destination: InlineTool-1
GigaSMART Operations (GSOP): Inline_SSL_GSOP (GigaSMART_Inline_SSL)

13. Now to send decrypted traffic to the Out Of Band tool, another second level map is required. Under **Maps**, click **New**.
14. On the New Map configuration page, do the following:
    - Enter an **alias**
    - Set the Type to **Inline Second Level**
    - Set the Subtype to **Egress OOB from Virtual Port**
    - Set the Source to the virtual port configured in step 3
    - Set the Destination to the OOB tool port
    - Set the GigaSMART Operations (GSOP) to the GSOP created earlier

    Click **Save**.



New Map

Map Info

Map Alias: OOB_Map

Comments:

Type: Inline Second Level

Subtype: Egress OOB from Virtual Port

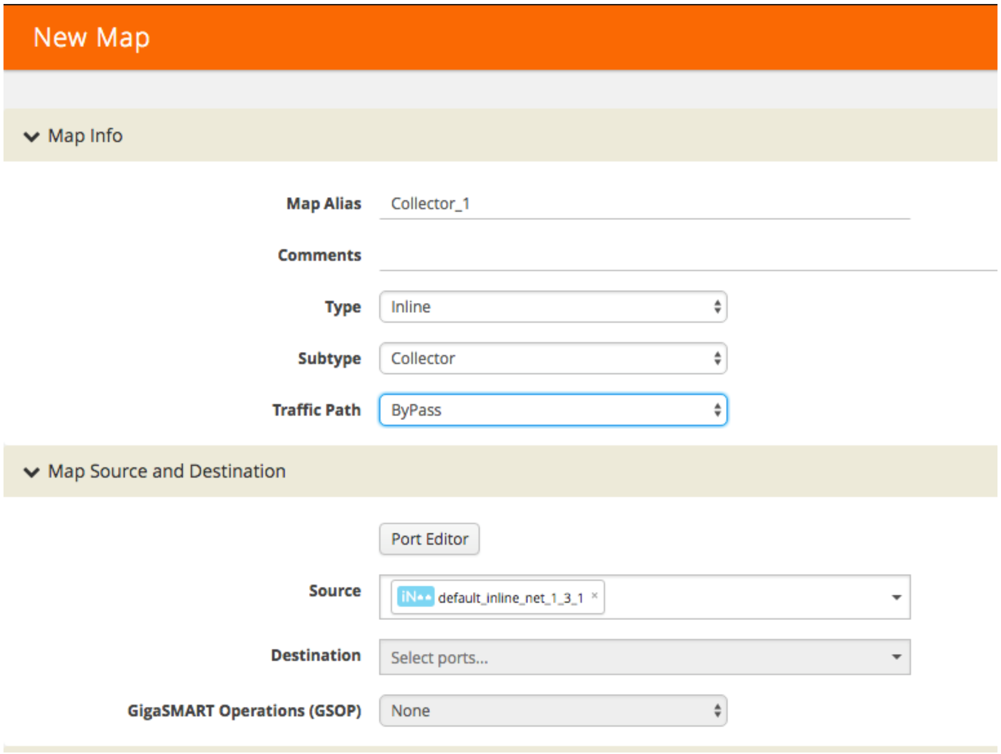
Map Source and Destination

Source: vport-1

Destination: 1/1/x2

GigaSMART Operations (GSOP): Inline_SSL_GSOP (GigaSMART_Inline_SSL)

15. The last map is a collector which is needed for all other traffic. Select **Maps** and Click **New**
16. On the New Map configuration page, do the following:
    - Enter an **alias**
    - Set the Type to **Inline**
    - Set the Subtype to **Collector**
    - Set the Traffic Path to **Collector**
    - Set the Source to the inline network
    - Click **OK**



New Map

Map Info

Map Alias	Collector_1
Comments	
Type	Inline
Subtype	Collector
Traffic Path	ByPass

Map Source and Destination

Source	iN default_inline_net_1_3_1 ×
Destination	Select ports...
GigaSMART Operations (GSOP)	None

Certification Checklist for RSA NetWitness

Date Tested: April 4th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.2	Virtual Appliance
GigaVUE-OS	5.0.1	GigaVUE-OS

Security Analytics Test Case	Result
Outbound SSL Decryption	
HTTPS	
Google Search	✓
Bing Search	✓
Facebook	✓
YouTube	✓
Twitter	✓
LinkedIn	✓
Reddit	✓
WEBMAIL	
GMail	✓
Yahoo	✓
Live	✓
AOL	✓
Inbound SSL Decryption	
HTTPS	
Web Server	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function