Gigamon®

Deployment Guide: A Multi-Product Security Architecture Example

COPYRIGHT

Copyright © 2017 Gigamon. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without Gigamon's written permission.

TRADEMARK ATTRIBUTIONS

Copyright © 2017 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal- trademarks. All other trademarks are the trademarks of their respective owners.

Table of Contents

Introduction

Today's enterprises have many choices to make when it comes to securing their IT infrastructure. Hundreds of vendors are offering a wide variety of security solutions – each with their own strengths (and weaknesses). Do you deploy a suite of functionality from one of the large vendors, select the best-of-breed for each tool type you require, or design a mix of the two? Most enterprises will start with a Next Generation Firewall (NGFW) but what should come next: a Security Information and Event Manager (SIEM), a secure email gateway, or Network Access Control (NAC)? The answer can be different for each enterprise based on risk assessment, budget, business profile, technologies deployed, and the opinions of architects and trusted advisors.

With this deployment guide, we describe how a leading set of security tools can be effectively deployed using the Gigamon Visibility Platform. It is not designed to be the prescribed InfoSec architecture for your business. It is just an architectural example to help you understand some of the options available to you and to demonstrate the flexibility and benefits such an architectural approach can provide.

While each of the vendor products included are leaders for the functionality we have described, they are not the only choice open to you. Several of the products have over-lapping functionality – for example, most of the vendors provide threat intelligence feeds and you probably wouldn't choose to subscribe to all the available services. Some of this overlap is desirable – different technological approaches may be suited to discovering various types of threats, i.e. zero-day – while single choices for other functionality may be desirable. We recommend consulting security experts within your organization or a consultant at your chosen VAR when designing the best solution for you.

In our example architecture, we have described how to deploy the following Technology Partner devices:

- Advanced Malware Detection/Sandbox: FireEye NX
- Next Generation Firewall with Application Visibility and Simple Category Blocking: Palo Alto Networks PA-3020 Series
- Intrusion Prevention System (IPS): Cisco FirePOWER
- Security Information and Event Manager (SIEM): Splunk Enterprise
- Packet Capture Device: FireEye PX

The approach we have described can be deployed all at once, or over time – it's up to you to balance the budget, business disruption and risk in deciding how to define your project. By utilizing Gigamon's Visibility Platform as the underlying method for obtaining access to any data traversing the managed infrastructure, you will build an effective and resilient foundation that is easily extensible to support current and future security requirements.

Overview

Gigamon, along with its ecosystem partners, solves customer problems with best of breed monitoring solutions for network security, troubleshooting, application monitoring, forensic analysis, and more. Technology Partners attach their solutions to the Gigamon Visibility Platform to get unobstructed, on demand access to any or all segments of the physical and virtual network.

The Gigamon Visibility Platform enables a modern network infrastructure that delivers pervasive visibility into all the data in motion across your entire network – whether physical, virtual or cloud. This visibility solution allows enterprises, governments, and service providers to effectively manage, secure, and understand what's happening across their increasingly complex networks.

For Security Operations (SecOps) teams, Gigamon helps you see more so you can secure more. Our visibility platform provides capabilities that enable and enhance your security tools by optimizing nework data and delivering the appropriate data to the proper security tools.

This deployment guide describes an example of a joint solution with FireEye NX, Cisco FirePOWER NGIPS, Palo Alto Networks NGFW, and Splunk Enterprise all connected to the Gigamon Visibility Platform.

As organization's scaling requirements change with the addition or upgrade of network links, Gigamon provides a flexible and efficient way to deploy inline and out-of-band tools without affecting traffic continuity or monitoring operations. The Gigamon platform provides all the necessary traffic handling capabilities to ensure that only packet data relevant to the function of each attached device gets sent to that device. It also helps avoid devices becoming overloaded with traffic that cannot be processed because it is irrelevant to the function being performed or because the device cannot process that volume of data.

Gigamon provides inline tool groups for partner appliances to deliver Security Service Assurance (SSA) for inline advanced malware protection. Putting FireEye, Cisco and Palo Alto Network's security devices in the inline tool group helps ensure that they remain available even in the case of appliance maintenance or failure. Also, Gigamon's GigaVUE HC Series Inline Bypass Modules provide physical bypass protection to provide continued network availability in the event of a power outage on the GigaVUE-HC2 nodes.

The solution described in this guide was tested with Gigamon GigaVUE-HC2, Palo Alto 3020 NGFWs, Cisco NGIPS, and FireEye NX 2400 Series advanced malware protection appliances in inline mode. The FireEye PX series and Splunk Enterprise are connected in out-of-band mode.

Deployment Prerequisites

The joint Gigamon solution consisting of Palo Alto NGFWs, Cisco NGIPSs, FireEye NX 2400s, FireEye PX series appliances, and Splunk Enterprise comprises of the following:

- GigaVUE-FM version 3.5
- GigaVUE-HC2 chassis with GigaVUE-OS 4.8 and GigaVUE HC Series GigaBPS module
- Two Palo Alto 3020 NGFWs running the following:
  - Software version: 7.1 or newer
- Two Cisco NGIPS running the following:
  - Software version: 6.0
- Two FireEye NX2400 appliances running the following:
  - Software version: 7.7.3
  - Content version: 531.148
  - Guest image information: WinXP SP3, Win7X64 SP1, Win7 SP1 – 15.1218
- Standalone FireEye PX series
- Standalone Splunk Enterprise server
  - Software version: 6.5.0

Architecture Overview

This section discusses the joint solution using a Gigamon GigaVUE-HC2 with bypass module, two Palo Alto 3020 NGFWs, two Cisco NGIPSs, two FireEye NX 2400 appliances in inline mode along with an optional standalone FireEye PX series appliance and Splunk Enterprise in out-of-band mode. The reference architecture in Figure 1 shows each component's position in the overall network infrastructure, where all network components and inline security tools are connected directly to the GigaVUE-HC2.

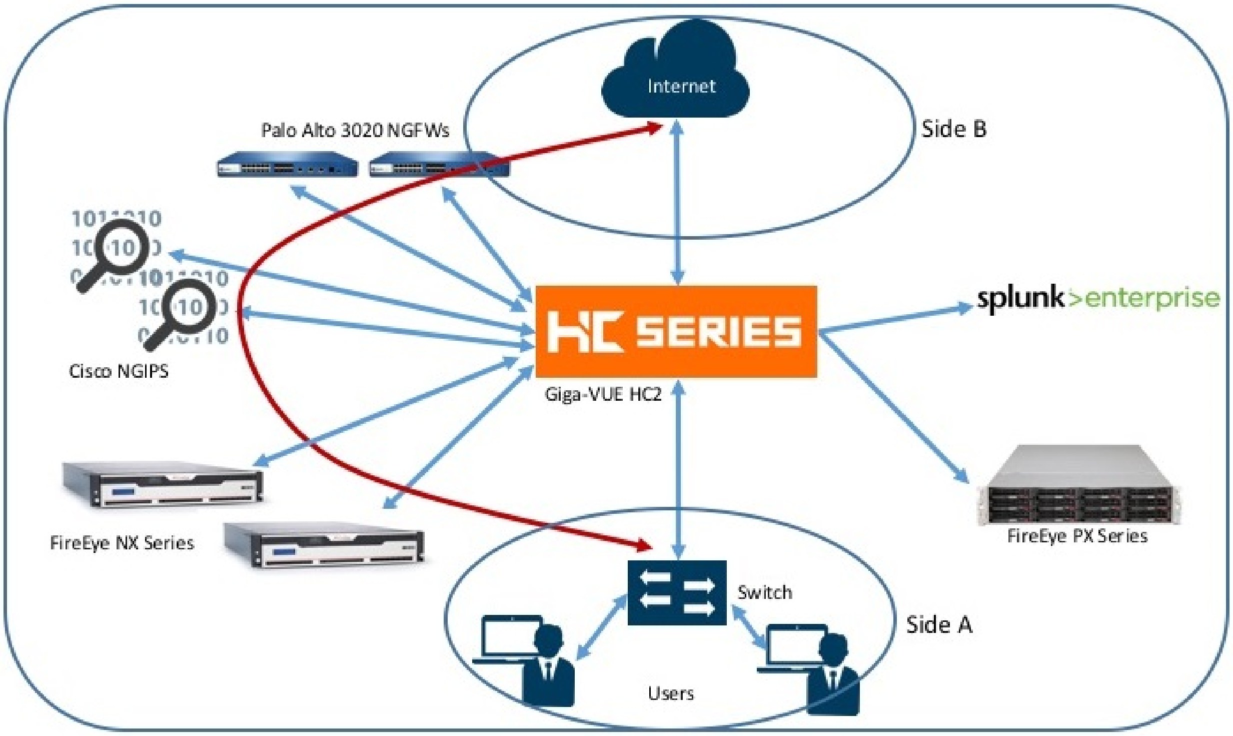


Figure 1: Gigamon Inline Bypass Joint Solution

For configuration purposes, the side where clients reside is assigned as side A. The side connected to the internet is assigned as side B.

NOTE: It is essential that the inline network and inline tool device bridge links are connected to GigaVUE-HC2 correctly relative to side A and side B so that traffic is distributed correctly to the devices in the inline tool group.

Two of each inline device type is chosen to demonstrate the additional resilience and scale that can be achieved this way. Gigamon's GigaSTREAM traffic balancing solution means that traffic can be shared across the available devices. Additional capacity could be added by deploying additional devices as traffic levels grow.

Network Topology

A detailed view of the network setup is shown in Figure 2**Error! Reference source not found.**. There are two links connected to the GigaVUE-HC2 inline bypass module which are internal and external sides of the network. Each inline device has a pair of links connected to GigaVUE-HC2. The Splunk Enterprise and FireEye PX appliances are connected with single links only.

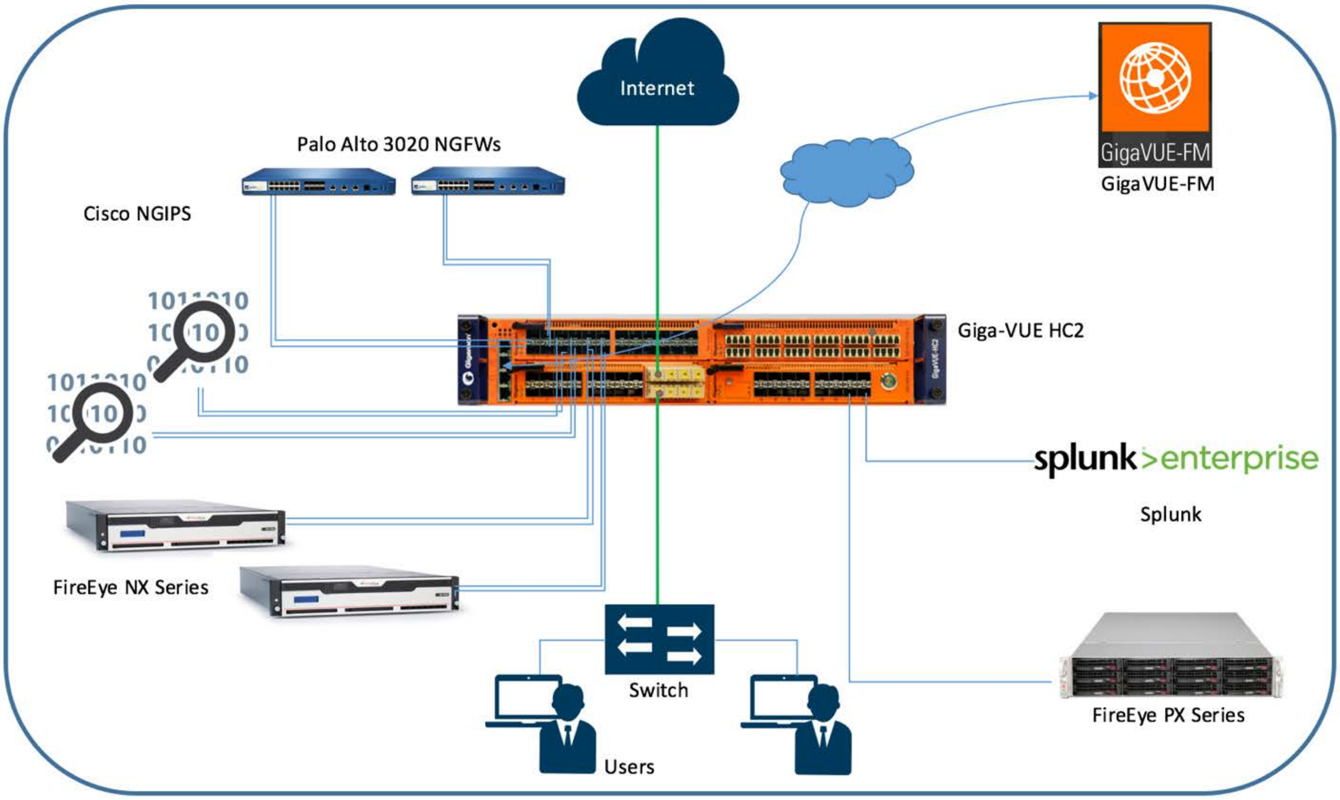


Figure 2: Complete Network Topology

Configuration

This section describes the configuration procedures for the GigaVUE-HC2, Palo Alto PA-3020, FireEye NX 2400 and Cisco FirePOWER through the respective management platforms. The procedures are organized as follows:

- Configuring FireEye NX 2400 for Inline Block Operation Mode
- Configuring Palo Alto PA 3020 for Virtual Wire Mode
- Configuring Cisco FirePOWER NGIPSv
- Configuring Splunk Enterprise
- Configuring GigaVUE-HC2

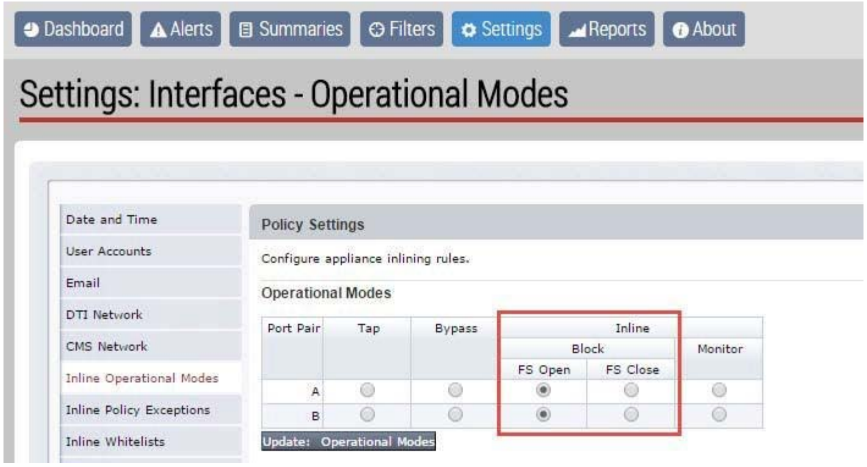
Configuring FireEye NX 2400 for Inline Block Operation Mode

The FireEye GUI procedures focus on FireEye inline block operational mode. The configuration procedures in the later section will configure the GigaVUE-HC2 to send live traffic to the FireEye inline tool group, which will allow the use of FireEye's on-system deployment testing tools. Per FireEye's best practices guidelines, GigaVUE-HC2 will be configured to distribute the traffic to the two FireEye appliances in the inline tool group, assuring all traffic for any given client (by IP address) goes to the same member of the FireEye inline tool group. This ensures complete session information is sent to a single device which, in turn, delivers best possible performance from your solution.

NOTE: This section assumes the FireEye appliances are directly connected to the GigaVUE-HC2 as shown in Figure 2. All GigaVUE-HC2 ports that FireEye appliances are connected to should be configured as port type Inline Tool. Furthermore, all GigaVUE-HC2 inline bypass ports that the network devices are connected to should be configured as Inline Network type ports. For specific instructions on how to complete these tasks, refer to the Help Topics in GigaVUE-FM.

To individually configure FireEye NX 2400 to block traffic so it detects malicious traffic, perform the following steps for each FireEye appliance:

1. On the FireEye GUI, select **Settings** > **Interfaces - Operational Modes**.
2. In the Policy Settings page, select the **Inline** > **Block** > **FS Open** radio button for both Port Pair A and Port Pair B as shown in Figure 3.



Settings: Interfaces - Operational Modes

Policy Settings

Configure appliance inlining rules.

Operational Modes

Port Pair	Tap	Bypass	Inline		Monitor
			Block		
			FS Open	FS Close	
A	○	○	●	○	○
B	○	○	●	○	○

Figure 3: Inline Block Operational Mode on FireEye Appliance

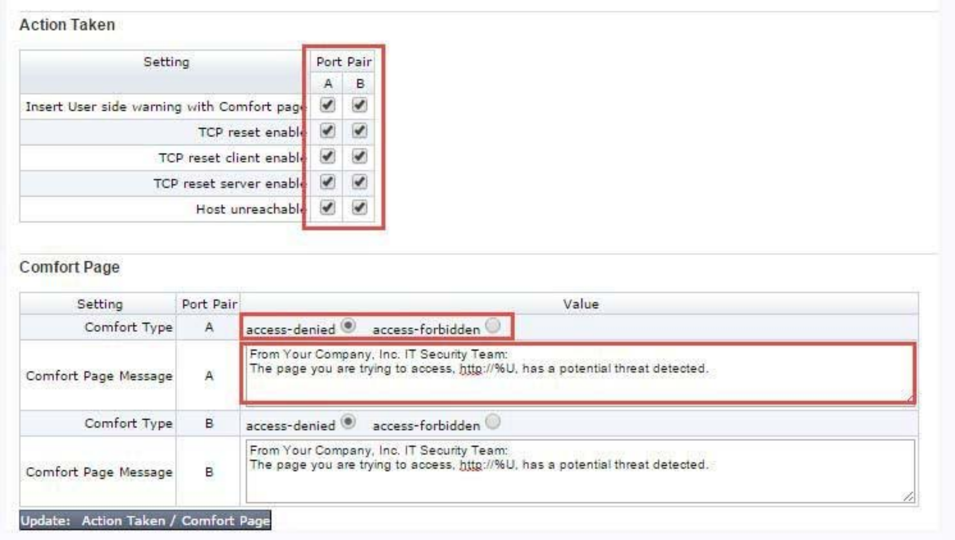
3. Click **Update: Operational Modes**.

Configuring FireEye Actions Taken: Comfort Page, TCP Resets:

FireEye NX has several options for actions to be taken when malicious content is detected. The following procedure walks you through the steps for sending a customized comfort page to the client and TCP resets to client and server. These steps are optional.

To set the Actions Taken and Comfort Page, perform the following steps:

1. In the **Policy Settings** > **Actions Taken** section, select all check boxes for Comfort page and TCP resets for both Port Pair A and Port Pair B as shown in Figure 4.



Action Taken

Setting	Port Pair	
	A	B
Insert User side warning with Comfort page	☑	☑
TCP reset enable	☑	☑
TCP reset client enable	☑	☑
TCP reset server enable	☑	☑
Host unreachable	☑	☑

Comfort Page

Setting	Port Pair	Value
Comfort Type	A	access-denied ● access-forbidden ○
Comfort Page Message	A	From Your Company, Inc. IT Security Team: The page you are trying to access, http://%U, has a potential threat detected.
Comfort Type	B	access-denied ● access-forbidden ○
Comfort Page Message	B	From Your Company, Inc. IT Security Team: The page you are trying to access, http://%U, has a potential threat detected.

Figure 4: FireEye Action Taken/Comfort Page Customization

2. In the **Comfort Page** section, leave the radio button set to **access-denied** (HTTP response code 401), unless you have a preference for **access-forbidden** (HTTP response code 403).

3. In the **Comfort Page Message** box, type a customized message for Port Pair A and Port Pair B.

4. Click **Update: Action Taken / Comfort Page**.

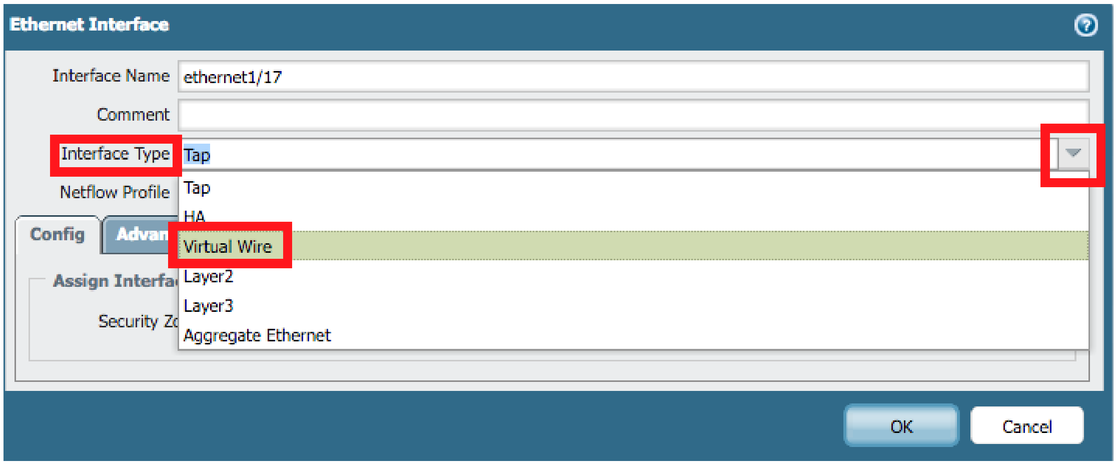
Configuring Palo Alto PA 3020 for Virtual Wire Mode

To configure the Palo Alto 3020 NGFW for Virtual Wire mode, perform the following steps for each Palo Alto appliance. You can skip these steps if the Virtual Wires you wish to use are already configured.

1. In the Palo Alto management GUI, select the **Network** tab and do the following:

   a. Click on the first interface you want to configure as part of the pair.

   b. Click the **Interface Type** drop-down list and select **Virtual Wire** as the interface type as shown in Figure 5.



Ethernet Interface

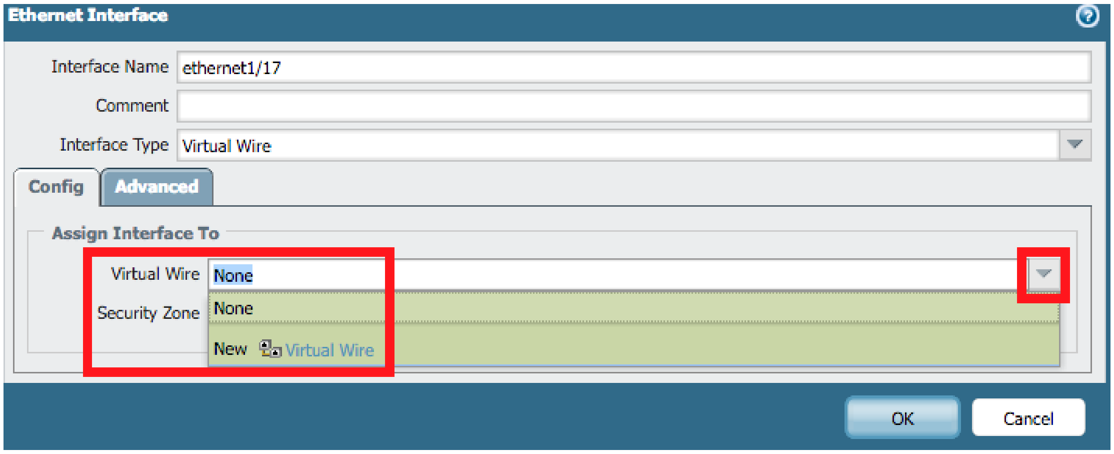
Interface Name: ethernet1/17

Comment:

Interface Type: Tap

Figure 5: FireEye Ethernet Interface

2. On the **Config** tab, click the **Virtual Wire** drop-down list and select **New > Virtual Wire** as shown in Figure 6. The Virtual Wire dialog box is displayed.



Ethernet Interface

Interface Name: ethernet1/17

Comment:

Interface Type: Virtual Wire

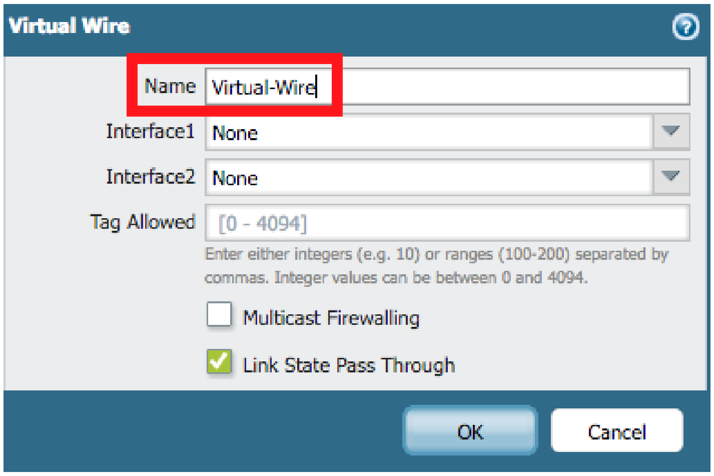
Assign Interface To

Virtual Wire: None

Security Zone:

Figure 6: FireEye Virtual Wire Configuration

3. In the **Virtual Wire dialog box**, enter a name for the Virtual Wire and click **OK**. In this example, the name entered is Virtual-Wire as shown in Figure 7.



Virtual Wire

Name	Virtual-Wire
Interface1	None
Interface2	None
Tag Allowed	[0 - 4094]

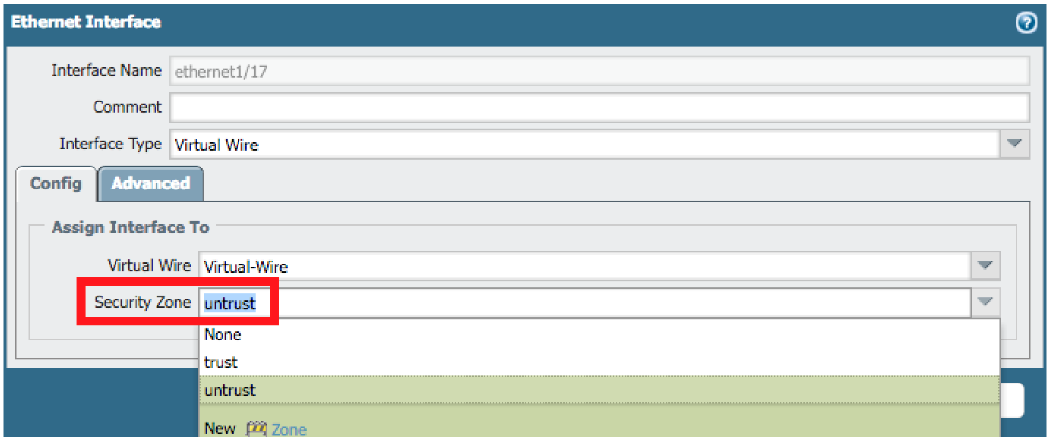
Enter either integers (e.g. 10) or ranges (100-200) separated by commas. Integer values can be between 0 and 4094.

☐ Multicast Firewalling

☑ Link State Pass Through

Figure 7: FireEye Virtual Wire

4. In the **Security Zone** drop-down list, select **untrust** and click **OK** as shown in Figure 8.



Ethernet Interface

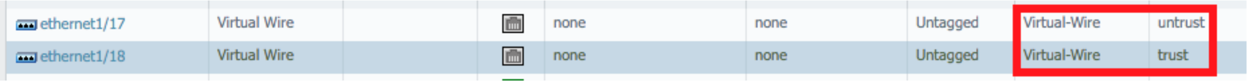
Interface Name	ethernet1/17
Comment	
Interface Type	Virtual Wire

Assign Interface To

Virtual Wire	Virtual-Wire
Security Zone	untrust

Figure 8: FireEye Security Zone

5. Repeat steps 2 to 4 for configuring the next interface (ethernet1/18 in this example) but select **trust** as the Security Zone in step 4 as shown in Figure 9.



ethernet1/17	Virtual Wire			none	none	Untagged	Virtual-Wire	untrust
ethernet1/18	Virtual Wire			none	none	Untagged	Virtual-Wire	trust

Figure 9: FireEye Interface set to trust

6. Click **Commit** (and optionally **Save**) to apply the changes.

7. Repeat steps 1 to 6 to configure the next Palo Alto 3020 NGFW.

Configuring Cisco FirePOWER NGIPSv

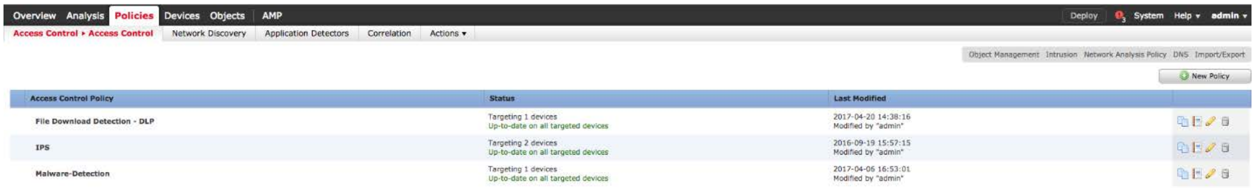
This section explains the steps to configure various elements of Cisco FirePOWER inline sets and access control policies.

1. Creating the default access control policies for NGIPSv sensors: Access control is a hierarchical policy-based feature that allows you to specify, inspect, and log (non-fast-pathed) network traffic. Especially useful in multi-domain deployments, you can nest access control policies, where each policy inherits the rules and settings from an ancestor (or *base*) policy. You can enforce this inheritance or allow lower-level policies to override their ancestors. Each managed device can be targeted by one access control policy.

   In the Cisco FirePOWER Management Center, perform the following:

   a. Select **Policies** > **Access Control** > **Access Control**.

   b. Click **New Policy**, and then create a default policy from any source zone to any destination zone keeping all the default parameters intact as shown in Figure 10.

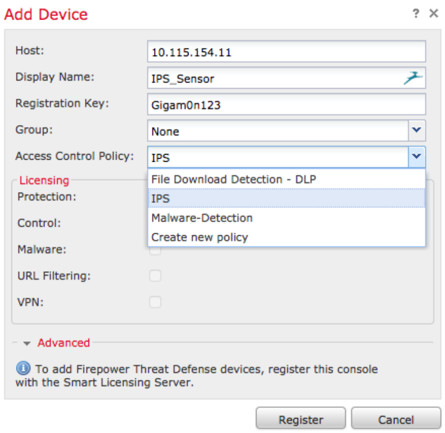


Access Control Policy	Status	Last Modified
File Download Detection - DLP	Targeting 1 devices Up-to-date on all targeted devices	2017-04-20 14:38:16 Modified by "admin"
IPS	Targeting 2 devices Up-to-date on all targeted devices	2016-09-19 15:57:15 Modified by "admin"
Malware-Detection	Targeting 1 devices Up-to-date on all targeted devices	2017-04-06 16:53:01 Modified by "admin"

Figure 10: Cisco FirePOWER Management Center Policies Page

2. Registering the device: For a sensor to be managed by Cisco FirePOWER Management Center, you must register the device. In the Cisco FirePOWER Management Center, perform the following:

   a. Select **Devices** > **Device Management** > **Add Device**. Refer to Figure 11.



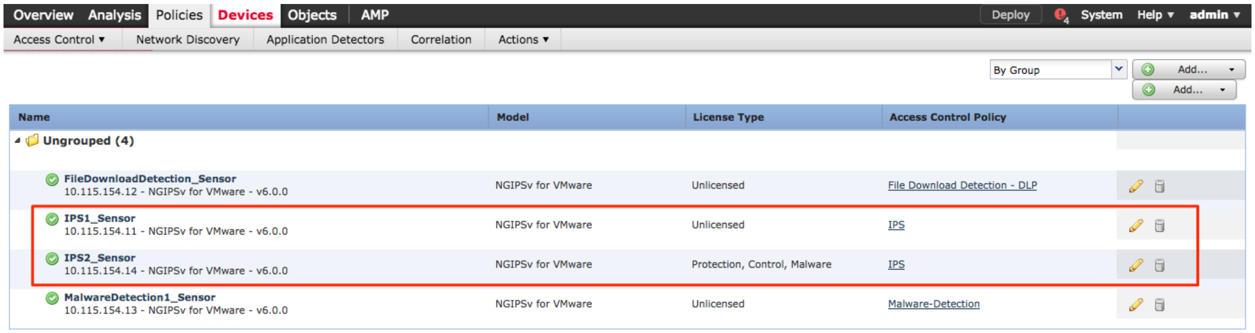
Add Device

Host:	10.115.154.11
Display Name:	IPS_Sensor
Registration Key:	Gigam0n123
Group:	None
Access Control Policy:	IPS

To add Firepower Threat Defense devices, register this console with the Smart Licensing Server.

Figure 11: Adding Device on Cisco FirePOWER Management Center

b. Fill out the information as shown in Figure 11, and then click **Register**. The Device Management page is displayed with the device information as shown in Figure 12.



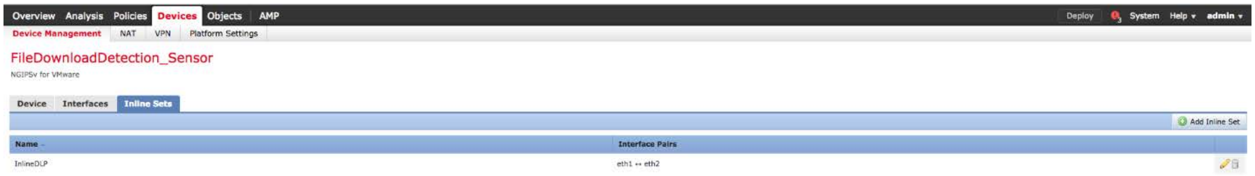
Name	Model	License Type	Access Control Policy
Ungrouped (4)			
FileDownloadDetection_Sensor 10.115.154.12 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Unlicensed	File Download Detection - DLP
IPS1_Sensor 10.115.154.11 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Unlicensed	IPS
IPS2_Sensor 10.115.154.14 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Protection, Control, Malware	IPS
MalwareDetection1_Sensor 10.115.154.13 - NGIPSv for VMware - v6.0.0	NGIPSv for VMware	Unlicensed	Malware-Detection

Figure 12: Cisco FirePOWER Management Center Device Management Page

3. Configuring Inline Set: Before you can use inline interfaces in an inline deployment, you must configure inline sets and assign inline interface pairs to them. An inline set is a grouping of one or more inline interface pairs on a device; an inline interface pair can belong to only one inline set at a time. This is a way to bridge together the incoming and outgoing interface for the traffic. In the Cisco FirePOWER Management Center, perform the following:

   a. Select **Devices** > **Device Management** > **Inline Sets**.

   b. Click **Add Inline Set**.



FileDownloadDetection_Sensor

NGIPSv for VMware

Name	Interface Pairs
InlineDLP	eth1 ↔ eth2

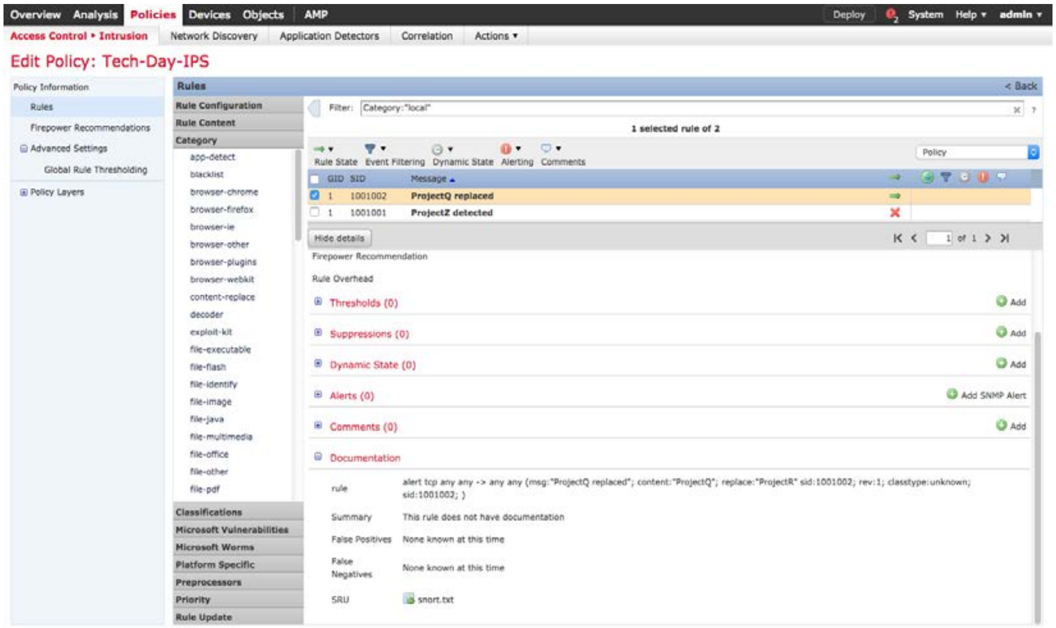
Figure 13: Inline Set on Cisco FirePOWER Management Center

4. Creating the Intrusion Sensor Policies: To add Intrusion policy through Cisco FirePOWER Management Center, select **Policies > Access Control > Intrusion.**

   The first example below adds a rule to replace and allow a string with “ProjectQ” text string with “ProjectR” in a traffic flow. The second example detects and blocks a flow when “ProjectZ” text string is detected. Refer to Figure 14, Figure 15, and Figure 16. These policies are created with the following rules:

   a. alert tcp any any → any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR"; sid: 1001001; rev:1;)

   b. alert tcp any any → any any (msg:"ProjectZ detected"; content:"ProjectZ"; sid: 1001002; rev:1;)



Filter: Category:"local"

1 selected rule of 2

	GID	SID	Message ▴	
☐				
☑	1	1001002	ProjectQ replaced	➡
☐	1	1001001	ProjectZ detected	✗

Firepower Recommendation

Rule Overhead

⊞ Thresholds (0)

⊞ Suppressions (0)

⊞ Dynamic State (0)

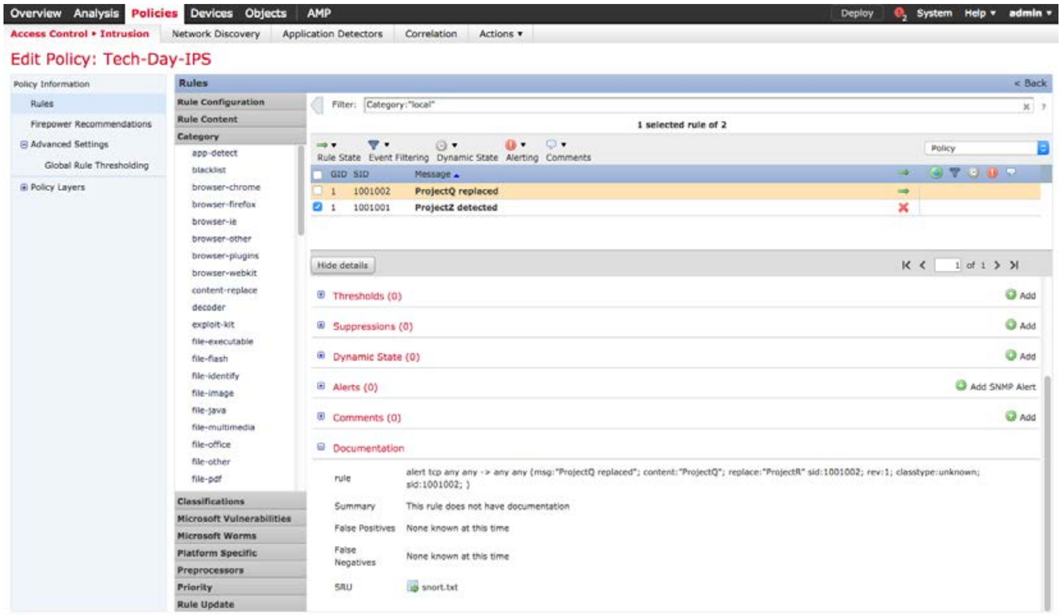
⊞ Alerts (0)

⊞ Comments (0)

⊟ Documentation

rule	alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR" sid:1001002; rev:1; classtype:unknown; sid:1001002;)
Summary	This rule does not have documentation
False Positives	None known at this time
False Negatives	None known at this time
SRU	snort.txt

Figure 14: Intrusion Detection Policy on Cisco FirePOWER Management Center



Filter: Category:"local"

1 selected rule of 2

	GID	SID	Message
□	1	1001002	ProjectQ replaced
☑	1	1001001	ProjectZ detected

⊞ Thresholds (0)

⊞ Suppressions (0)

⊞ Dynamic State (0)

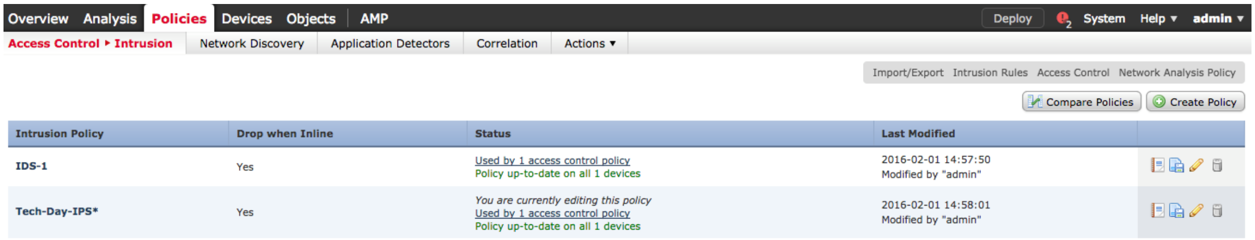
⊞ Alerts (0)

⊞ Comments (0)

⊟ Documentation

rule	alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR" sid:1001002; rev:1; classtype:unknown; sid:1001002;)
Summary	This rule does not have documentation
False Positives	None known at this time
False Negatives	None known at this time
SRU	snort.txt

Figure 15: Intrusion Detection Policy on Cisco FirePOWER Management Center



Intrusion Policy	Drop when Inline	Status	Last Modified
IDS-1	Yes	Used by 1 access control policy Policy up-to-date on all 1 devices	2016-02-01 14:57:50 Modified by "admin"
Tech-Day-IPS*	Yes	*You are currently editing this policy* Used by 1 access control policy Policy up-to-date on all 1 devices	2016-02-01 14:58:01 Modified by "admin"

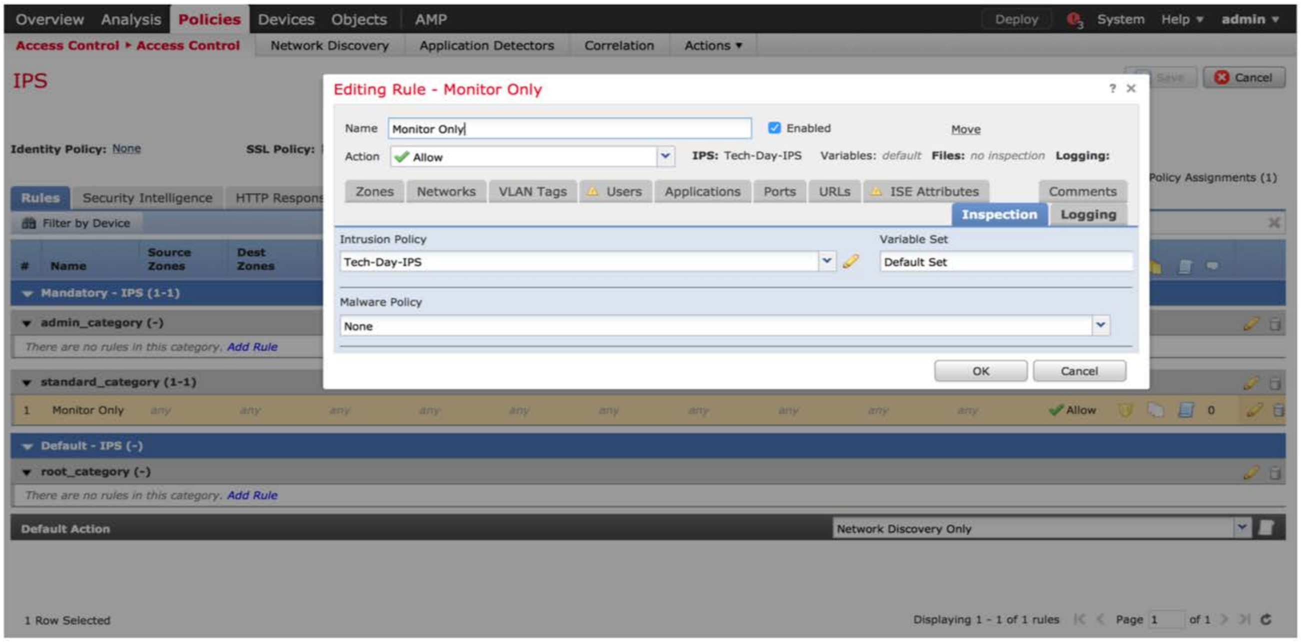
Figure 16: Intrusion Policies on Cisco FirePOWER Management Center

5. Assigning the IPS Access Control Policy: Apply the device level policy to the global access policy and assign the policy to target sensors. This section describes how to apply the device level policy to the global access policy, and then assign it to the target sensors.

   To assign IPS sensor level policy to global access control policy through Cisco FirePOWER Management Center, perform the following:

   a. Select **Policies** > **Access Control** > **Access Control** > **IPS**.

b. Click **Edit**. The Editing Rule – Monitor Only dialog box is displayed.



Editing Rule - Monitor Only

Name: Monitor Only

☑ Enabled

Action: Allow

IPS: Tech-Day-IPS Variables: *default* Files: *no inspection* Logging:

Intrusion Policy: Tech-Day-IPS

Variable Set: Default Set

Malware Policy: None

1 Monitor Only any any any any any any any any any any Allow 0

Default Action: Network Discovery Only

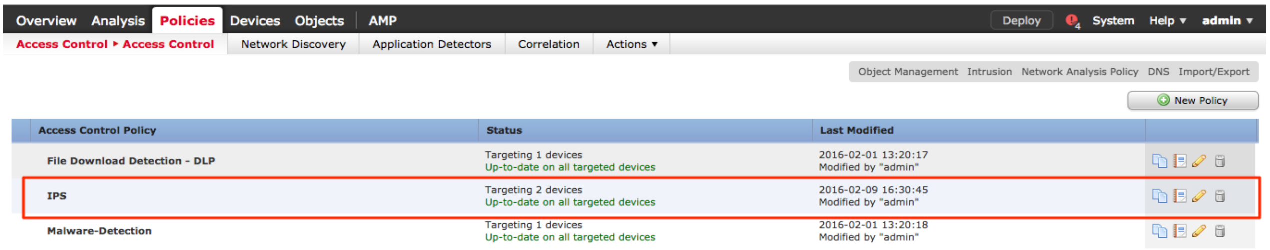
Figure 17: Intrusion Policy and Rules on the Cisco FirePOWER Management Center

c. Click the **Inspection** tab.

d. Select the **Intrusion Policy** of interest. In Figure 17, the Intrusion Policy selected is **Tech-Day-IPS**. Click **OK**.

e. Assign the policy to the targeted devices using the **Policy Assignments** link in the right hand corner.

The completed Access control policy page lists the Intrusion policy as shown in Figure 18:



Access Control Policy	Status	Last Modified
File Download Detection - DLP	Targeting 1 devices Up-to-date on all targeted devices	2016-02-01 13:20:17 Modified by "admin"
IPS	Targeting 2 devices Up-to-date on all targeted devices	2016-02-09 16:30:45 Modified by "admin"
Malware-Detection	Targeting 1 devices Up-to-date on all targeted devices	2016-02-01 13:20:18 Modified by "admin"

Figure 18: Access Control Policies on the Cisco FirePOWER Management Center

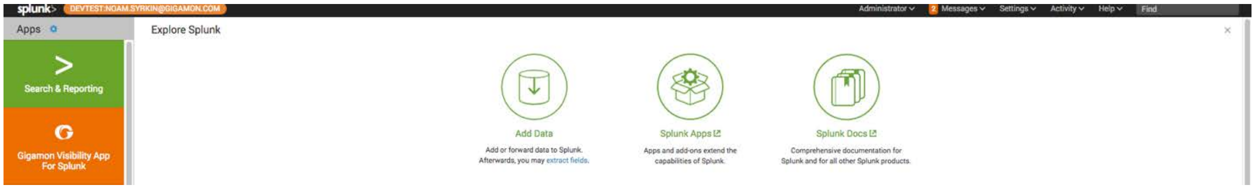
Configuring Splunk Enterprise

This section explains the steps to configure Splunk Enterprise to receive IPFIX metadata from Gigamon. Such metadata enables a number of advanced security use cases to be performed. For more information, refer to https://www.gigamon.com/resources/white-paper/harnessing-power-metadata-security-4068.

Perform the following steps to configure Splunk Enterprise:

1. Configure the Splunk Add-on for IPFIX by navigating to the following link: https://www.gigamon.com/sites/default/files/resources/deployment-guide/dg-gigamon-with-splunk-4053.pdf

2. On the Splunk Enterprise dashboard, navigate to **Explore Splunk**.



Add or forward data to Splunk. Afterwards, you may extract fields.

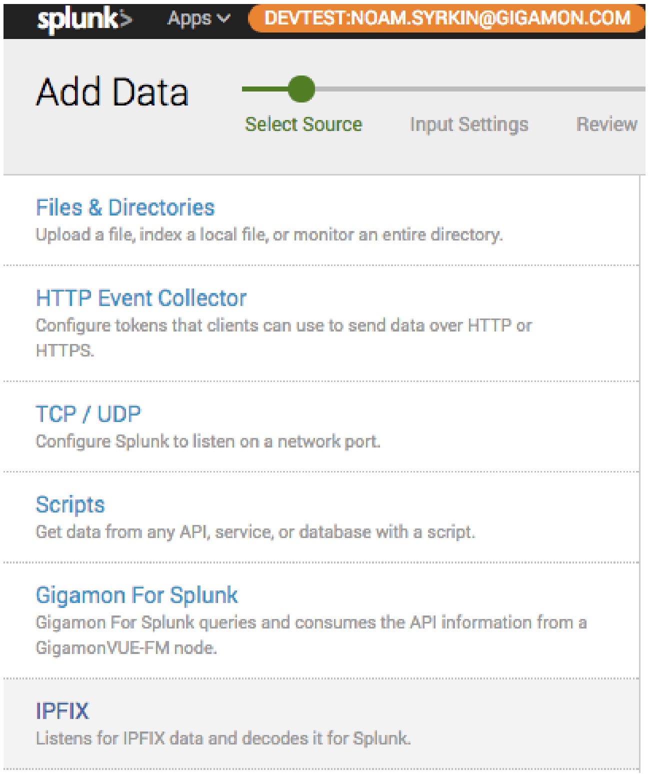
Apps and add-ons extend the capabilities of Splunk.

Comprehensive documentation for Splunk and for all other Splunk products.

Figure 19: Splunk Enterprise Dashboard with Options

3. Select **Add Data** as shown in Figure 19.

4. Select **monitor**. On the next screen, select **IPFIX** as shown in Figure 20.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

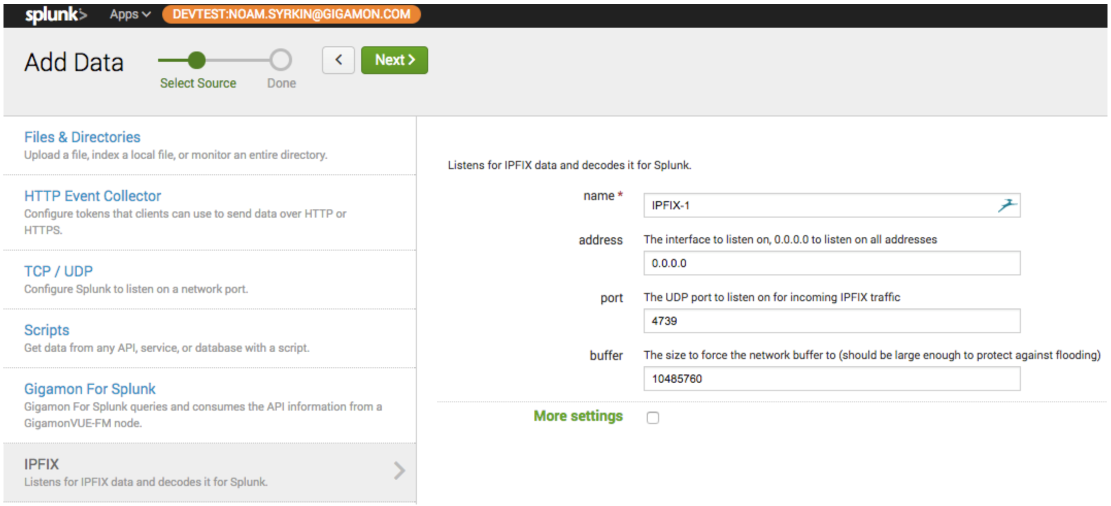
Scripts
Get data from any API, service, or database with a script.

Gigamon For Splunk
Gigamon For Splunk queries and consumes the API information from a GigamonVUE-FM node.

IPFIX
Listens for IPFIX data and decodes it for Splunk.

Figure 20: IPFIX Option for Adding Data in Splunk Enterprise

5. Enter the appropriate information as shown in Figure 21 and click **Next**.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Gigamon For Splunk
Gigamon For Splunk queries and consumes the API information from a GigamonVUE-FM node.

IPFIX
Listens for IPFIX data and decodes it for Splunk.

Listens for IPFIX data and decodes it for Splunk.

name * IPFIX-1

address The interface to listen on, 0.0.0.0 to listen on all addresses
0.0.0.0

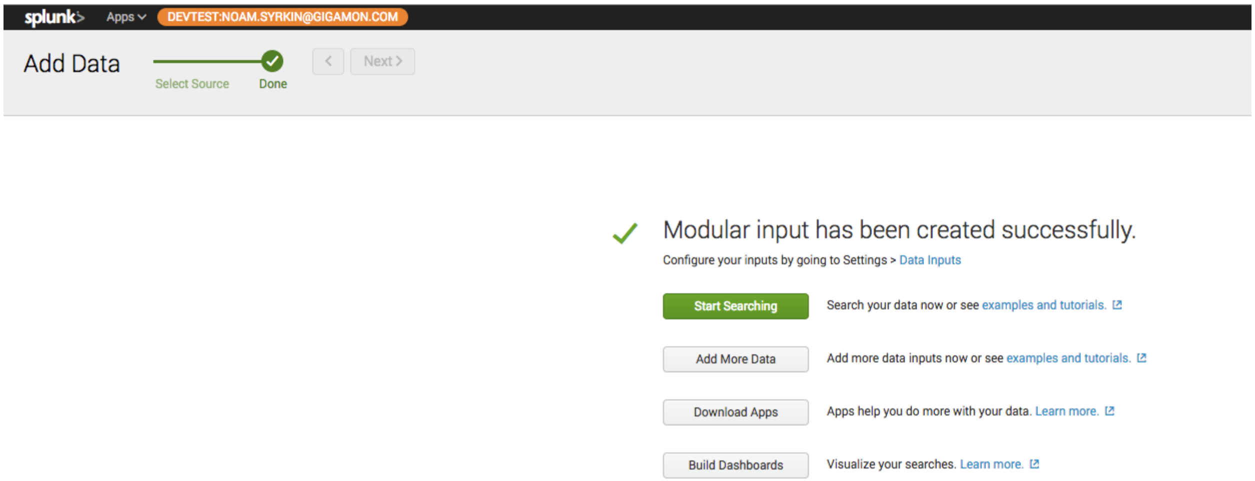
port The UDP port to listen on for incoming IPFIX traffic
4739

buffer The size to force the network buffer to (should be large enough to protect against flooding)
10485760

More settings □

Figure 21: IPFIX Fields

6. After the configuration is complete, a message is displayed as shown in Figure 22.



✓ Modular input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Start Searching	Search your data now or see examples and tutorials.
Add More Data	Add more data inputs now or see examples and tutorials.
Download Apps	Apps help you do more with your data. Learn more.
Build Dashboards	Visualize your searches. Learn more.

Figure 22: IPFIX Configuration

Configuring GigaVUE-HC2

This section covers how to configure GigaVUE-HC2 for all inline network and inline tool elements that you will use to create traffic flow maps. This configuration consists of the following procedures:

- Configuring the Inline Network
- Configuring the Inline Tools
- Configuring the Inline Tool Groups
- Configuring the Inline Serial Tools
- Configuring the Inline Traffic Flow Maps

Configuring the Inline Network

This section walks you through the steps needed to configure inline network bypass pairs. As the organization's architecture grows, additional inline network pairs can be added to the inline network group.

The steps described in this section assume that you are logged in to GigaVUE-FM, selected Physical Nodes in the left pane and then selected the GigaVUE-HC2 on the Physical Nodes page.

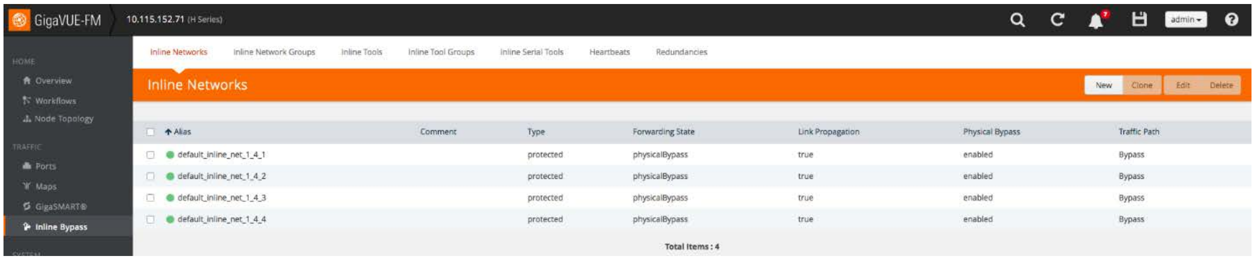
NOTE: This section assumes all the ports that the network devices are connected to are set as Inline Network port types. For specific instructions on completing these tasks, refer to *Gigamon-OS H-VUE User's Guide*.

Configure the Inline Network Bypass Pair

To configure the inline network bypass pair, perform the following:

1. Log into **GigaVUE-FM**. In the left navigation pane, select **Physical Nodes**.
2. Double-click the GigaVUE-HC2 from the list of physical nodes GigaVUE-FM is managing.
3. Select **Inline Bypass** > **Inline Networks**.

NOTE: If there is a bypass combo module in the GigaVUE-HC2, there will be four preconfigured Inline Network port pairs as shown in Figure 23. If you are using BPS ports, the step will be similar to those covered but limited. Notably, you will not be able to change the alias. Also, port A and port B will be preselected. If your network is 1G or 10G fiber, use one of the preconfigured inline bypass pairs listed in Figure 23.



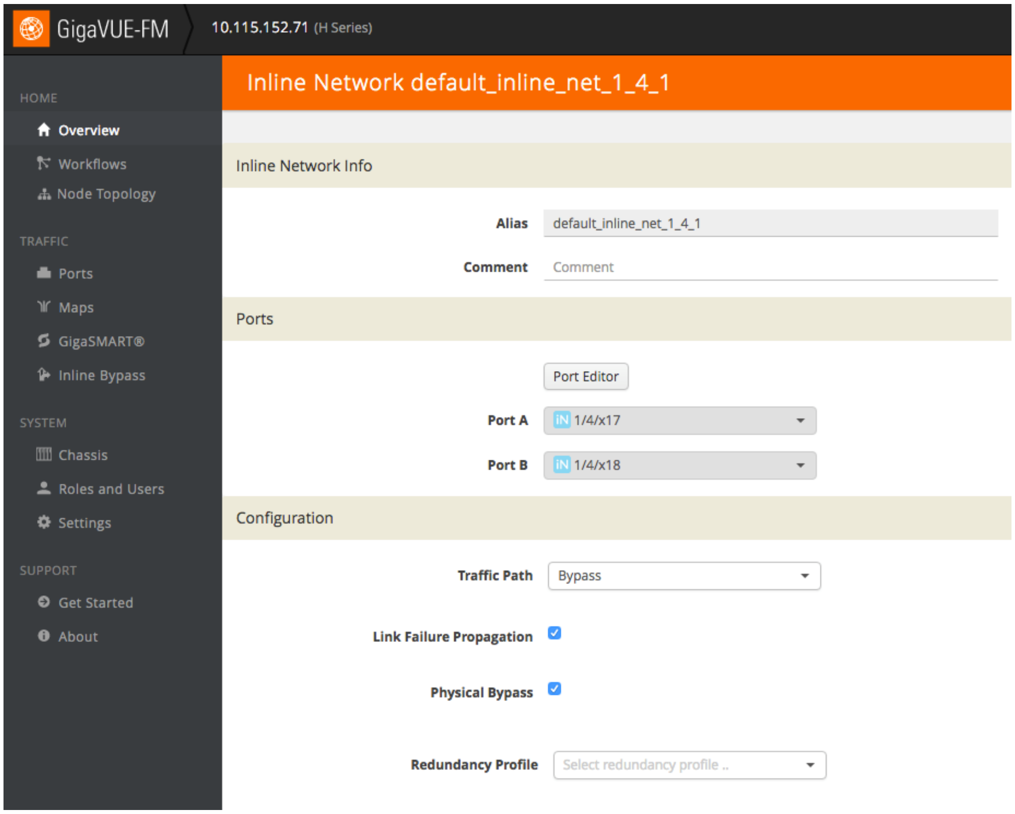
Inline Networks

Alias	Comment	Type	Forwarding State	Link Propagation	Physical Bypass	Traffic Path
default_inline_net_1_4_1		protected	physicalBypass	true	enabled	Bypass
default_inline_net_1_4_2		protected	physicalBypass	true	enabled	Bypass
default_inline_net_1_4_3		protected	physicalBypass	true	enabled	Bypass
default_inline_net_1_4_4		protected	physicalBypass	true	enabled	Bypass

Total Items : 4

Figure 23: Inline Networks view

4. Select an existing **Inline Network** and click **Edit**. The Inline Network configuration page is displayed as shown in Figure 24.



Inline Network default_inline_net_1_4_1

Inline Network Info

Alias: default_inline_net_1_4_1

Comment: Comment

Ports

Port A: IN 1/4/x17

Port B: IN 1/4/x18

Configuration

Traffic Path: Bypass

Link Failure Propagation ☑

Physical Bypass ☑

Redundancy Profile: Select redundancy profile ..

Figure 24: Inline Network Pair Configuration

5. On the Inline Network page, perform the following:

   a. In the **Alias** field, type an alias that will help you remember which network link this Inline Network bypass pair represents.

   b. Note down the port for **Port A** and **Port B**.

   Important: It is essential that the side A and side B of the GigaVUE-HC2 match the side A and side B of the Inline Tools. Otherwise, the traffic distribution for the Inline Tool Group will not work correctly.

c. Retain the **Traffic Path** and the **Link Failure Propagation** options set to the default values.

d. Select **Physical Bypass**. This minimizes packet loss during traffic map changes.

e. Click **Save**.

NOTE: Traffic Path is set to **Bypass** to prevent packet loss until the inline tool groups and maps have been set up. After the inline tool groups and maps are configured, the traffic path can be set to inline tool as described in the subsequent section.

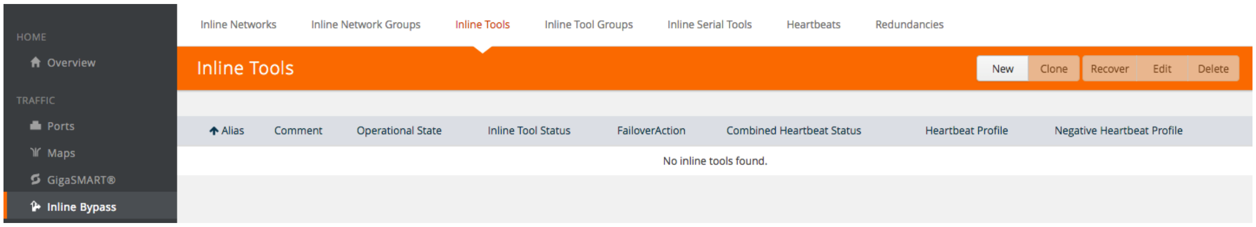
Configuring the Inline Tools

This section discusses the configuration steps to add various inline tools.

Adding FireEye NX2400

This section walks you through the steps necessary to define the inline tool port pairs and the inline tool group that will be used in the traffic flow map.

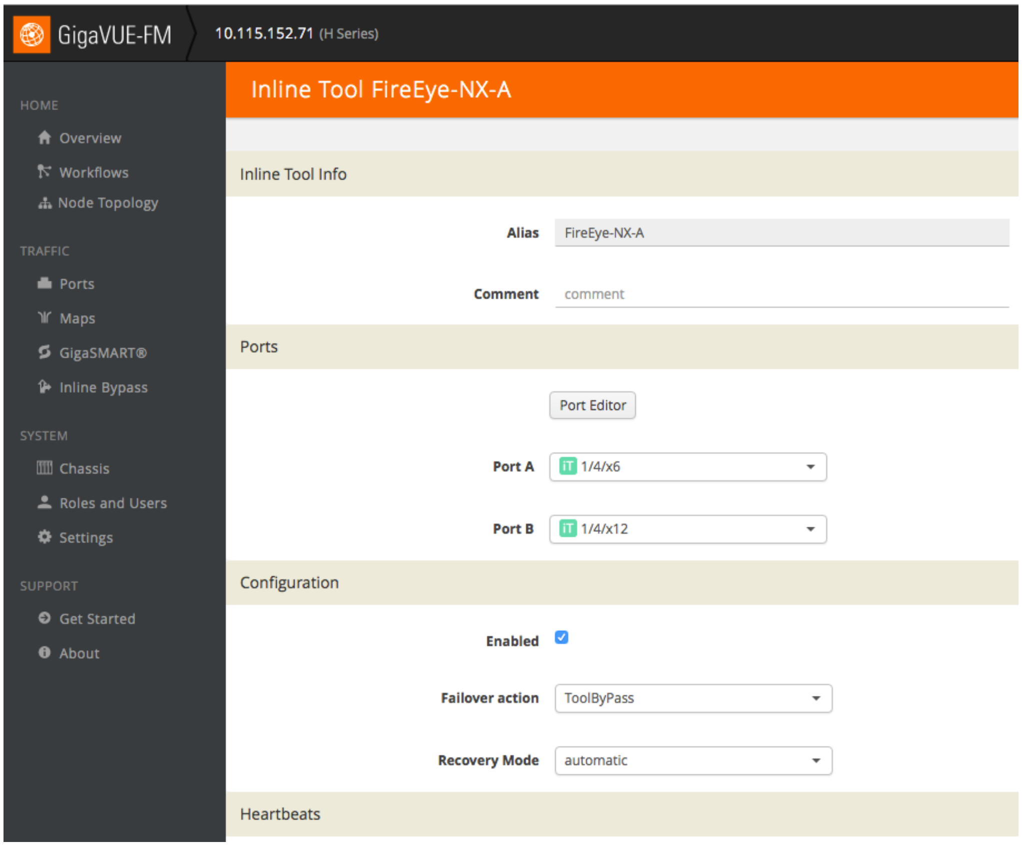
1. On GigaVUE-FM, select **Inline Bypass** > **Inline Tools**.



No inline tools found.

Figure 2625: Navigating to the Inline Tools page

2. Click **New** to open the configuration page for inline tools as shown in Figure 26.



Inline Tool FireEye-NX-A

Inline Tool Info

Alias: FireEye-NX-A

Comment: comment

Ports

Port A: IT 1/4/x6

Port B: IT 1/4/x12

Configuration

Enabled: ☑

Failover action: ToolByPass

Recovery Mode: automatic

Heartbeats

Figure 26: Inline Tool Pair Configuration3.

3. In the **Alias** field, type an alias that will help you remember which inline tool this inline tool pair represents. For example, **FireEye-NX-A .**

4. In the Ports section, specify the ports as follows:

- For **Port A**, specify the port that corresponds to side A in the network diagram (refer to Figure 2).

- For **Port B**, specify the port that corresponds to side B in the network diagram (refer to Figure 2).

  Important: It is essential that the Port A and Port B match the side A and side B respectively.

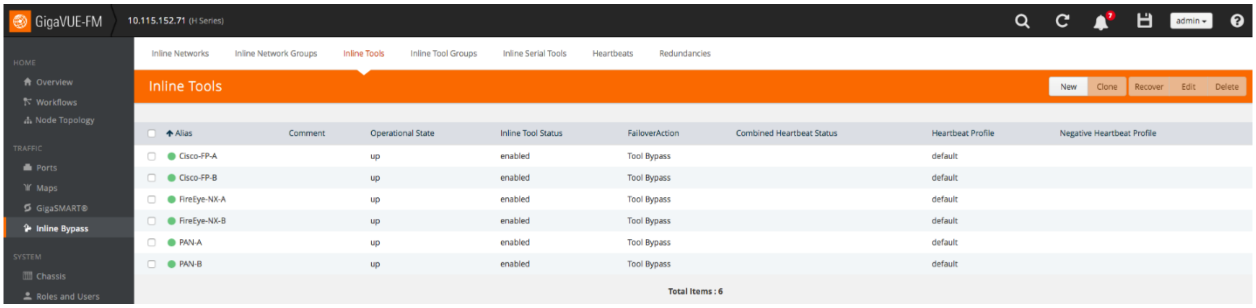
5. Retain the default settings for the remaining configuration options.

6. Click **Save.**

   NOTE: The failure action for this inline tool is **ToolBypass**. This means that GigaVUE-HC2 will not send traffic to this inline tool if it is considered to be in a failure mode. There are other options for inline tool failure that are fully described in the online help. The other options have very different effects on the overall traffic flow. Since the heartbeat feature is not enabled to reduce overall complexity, the failover action will only take place if one of the tool port links fail.

Adding Palo Alto PA 3020s and Cisco NGIPSv

Repeat steps 1 to 6 as decribed in the Adding FireEye NX2400 section for configuring ports where the Palo Alto PA-3020s and Cisco FirePOWER devices are connected. After the configuration, the Inline Tools page is displayed as shown in Figure 27.



Alias	Comment	Operational State	Inline Tool Status	FailoverAction	Combined Heartbeat Status	Heartbeat Profile	Negative Heartbeat Profile
Cisco-FP-A		up	enabled	Tool Bypass		default	
Cisco-FP-B		up	enabled	Tool Bypass		default	
FireEye-NX-A		up	enabled	Tool Bypass		default	
FireEye-NX-B		up	enabled	Tool Bypass		default	
PAN-A		up	enabled	Tool Bypass		default	
PAN-B		up	enabled	Tool Bypass		default	

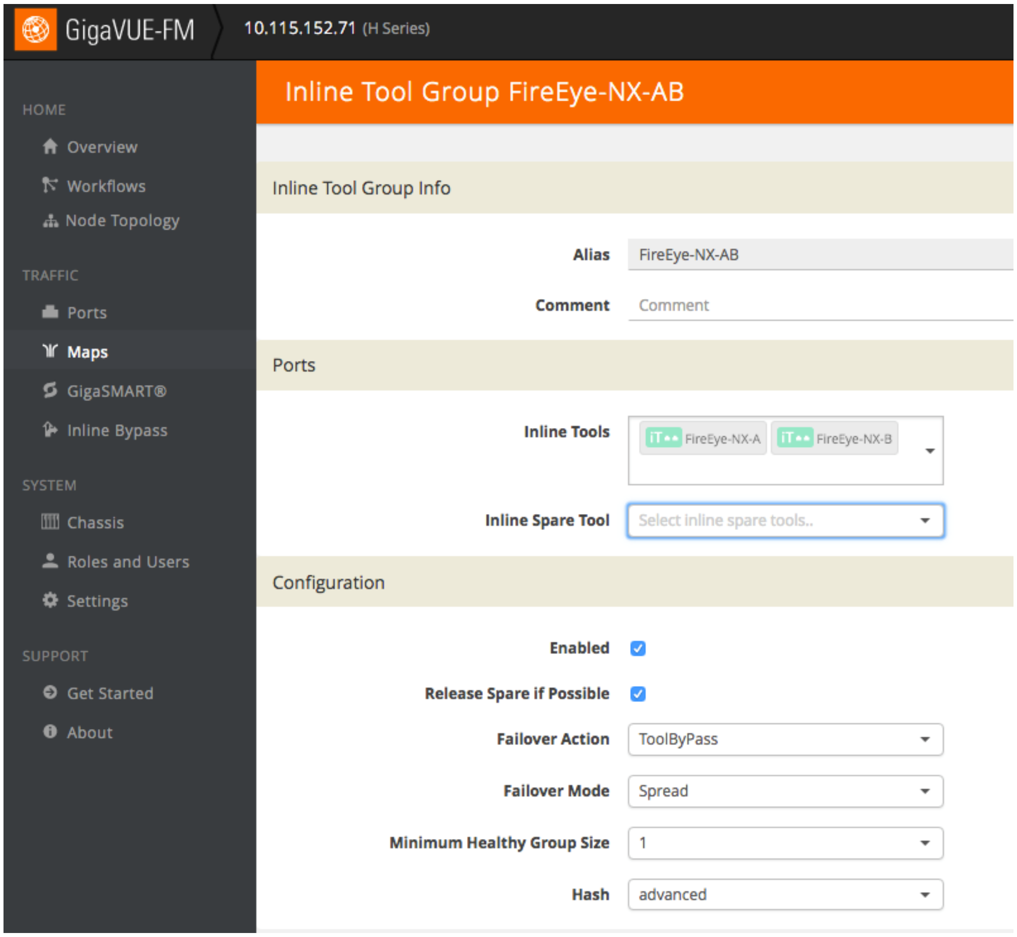
Total Items : 6

Figure 27: Inline Tools Complete Configuration

Configuring the Inline Tool Groups

To configure the inline tool group, perform the following:

1. In GigaVUE-FM, select **Inline Bypass** > **Inline Tool Groups**.
2. Click **New** to open the Inline Tool Groups configuration page as shown in Figure 28.



Inline Tool Group FireEye-NX-AB

Inline Tool Group Info

Alias: FireEye-NX-AB

Comment: Comment

Ports

Inline Tools: FireEye-NX-A, FireEye-NX-B

Inline Spare Tool: Select inline spare tools..

Configuration

Enabled: ☑

Release Spare if Possible: ☑

Failover Action: ToolByPass

Failover Mode: Spread

Minimum Healthy Group Size: 1

Hash: advanced

Figure 28: Inline Tool Group Configuration

3. In the **Alias** field, type an alias that describes the inline tool groups.

4. In the Ports section, click the **Inline tools** field and select all the inline tools for this group from the list of available inline tools.

   There is an option to select an **Inline spare tool**. When this option is configured, it becomes the primary failure action for this inline tool group.

5. In the Configuration section, perform the following:

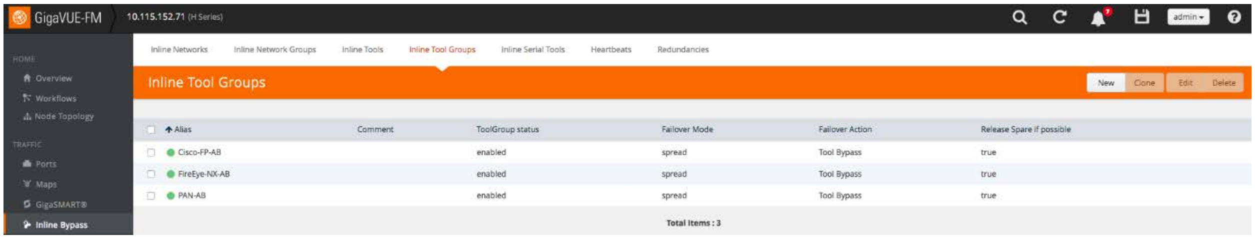
   a. Select **Enabled** to enable the inline tool group.

   b. Select **Release Spare If Possible** if applicable. 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 should be included in the active set of inline tools or if it becomes the new spare inline tool.

   c. Keep the defaults for **Failover action** to when the inline tool group fails. The traffic that normally was directed to the inline tool group is redirected to the bypass path, **Failover Mode**, and **Minimum Healthy Group Size**.

d. From the **Hash** drop-down list**, select advanced**.

6. Repeat steps 1 to 5 for configuring Palo Alto 3020s and Cisco NGIPSv. The Inline Tool Groups configuration page is displayed as shown in Figure 29.



Alias	Comment	ToolGroup status	Failover Mode	Failover Action	Release Spare if possible
Cisco-FP-AB		enabled	spread	Tool Bypass	true
FireEye-NX-AB		enabled	spread	Tool Bypass	true
PAN-AB		enabled	spread	Tool Bypass	true

Total Items : 3

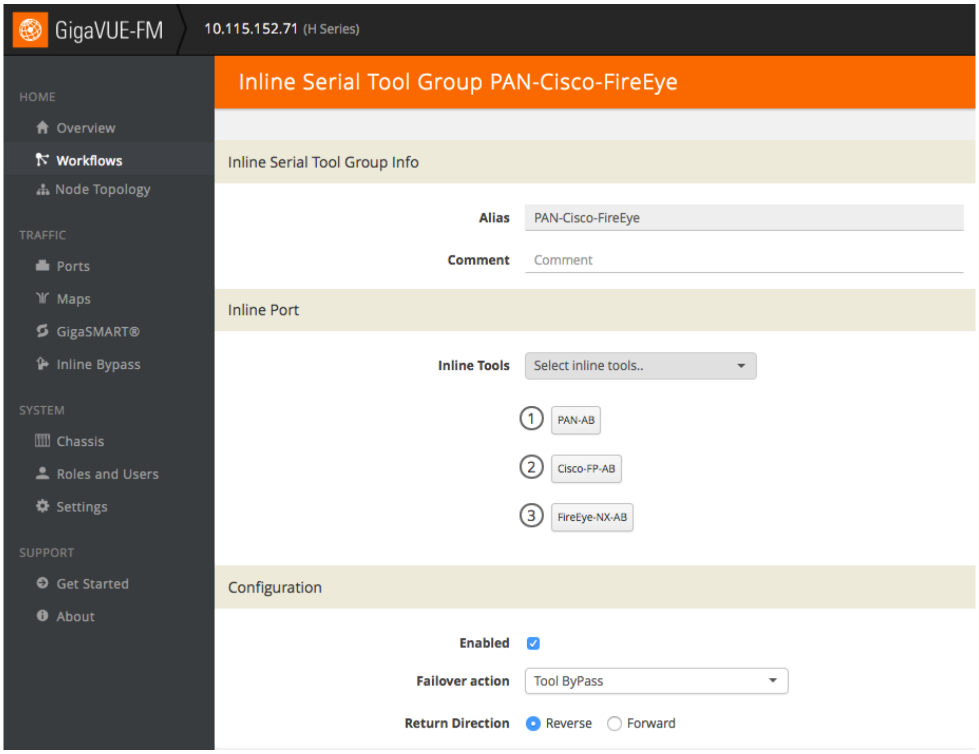
Figure 29: Inline Tool Groups Complete Configuration

Configuring the Inline Serial Tools

This section provides steps to configure tools in a serial manner.

1. In GigaVUE-FM, select **Inline Bypass** > **Inline Serial Tools**.

2. Click **New** to open the **Inline Serial Tool Group** configuration page as shown in Figure 30.



Inline Serial Tool Group PAN-Cisco-FireEye

Inline Serial Tool Group Info

Alias: PAN-Cisco-FireEye

Comment: Comment

Inline Port

Inline Tools: Select inline tools..

1. PAN-AB
2. Cisco-FP-AB
3. FireEye-NX-AB

Configuration

Enabled: ☑

Failover action: Tool ByPass

Return Direction: ● Reverse ○ Forward

Figure 30: Inline Serial Tool Group Complete Configuration

3. In the **Alias** field, type an alias that describes the inline serial tool group.

4. In the **Inline Tools** drop-down list, select the tools in the order in which the traffic needs to traverse. In the example in Figure 30, the traffic first goes through Palo Alto Networks (Inline Tool Group), then to Cisco FirePOWER (Inline Tool Group), and finally to FireEYE-NX (Inline Tool Group), before being sent out to the network.

Configuring the Inline Traffic Flow Maps

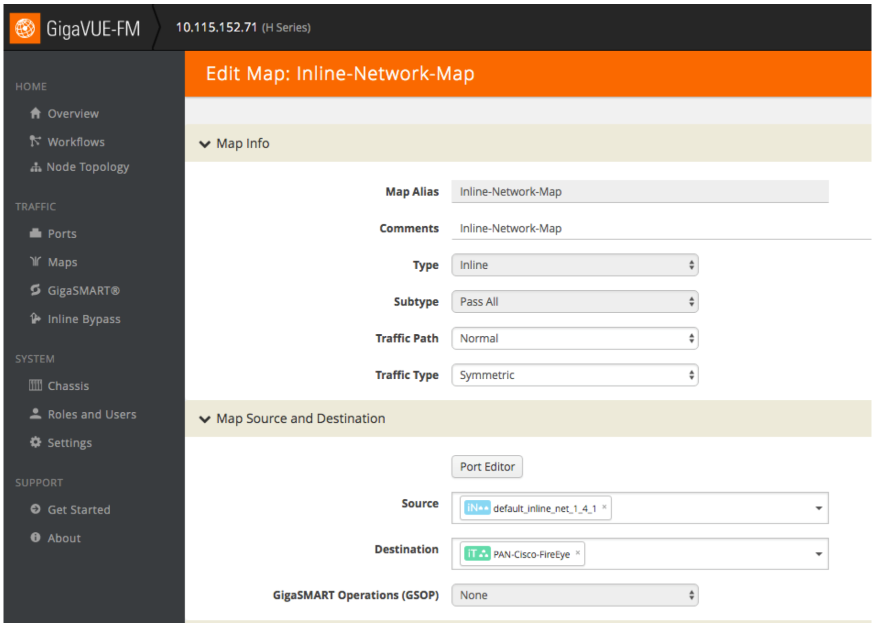
This section describes the steps for configuring traffic to flow from the inline network links to the inline tool group allowing you to test the deployment functionality of the inline tools within the group. This will be done in two steps as follows:

- Configuring the Traffic Flow Map with an Inline Bypass Rule
- Changing the Inline Network Traffic Path to Inline Tool

Configuring the Traffic Flow Map with an Inline Bypass Rule

This section covers how to configure the traffic flow map between the inline network group and the inline tool group.

1. In **GigaVUE-FM**, go to the **Maps** page.
2. Click **New**. The New Map page is displayed as shown in Figure 31.



Edit Map: Inline-Network-Map

Map Info

Map Alias: Inline-Network-Map
Comments: Inline-Network-Map
Type: Inline
Subtype: Pass All
Traffic Path: Normal
Traffic Type: Symmetric

Map Source and Destination

Source: iN default_inline_net_1_4_1
Destination: iT PAN-Cisco-FireEye
GigaSMART Operations (GSOP): None

Figure 31: Rule for Inline Network to Tool Flow Map

3. In the Map Info section, perform the following configuration:

    a. In the **Map Alias** field, enter a map alias that represents the network source and tool destination.

    b. From the **Type** drop-down list, select **Inline**.

    c. From the **Sub Type** drop-down list, select **Pass All**.

    d. From the **Traffic Path** drop-down list, select **Normal**.

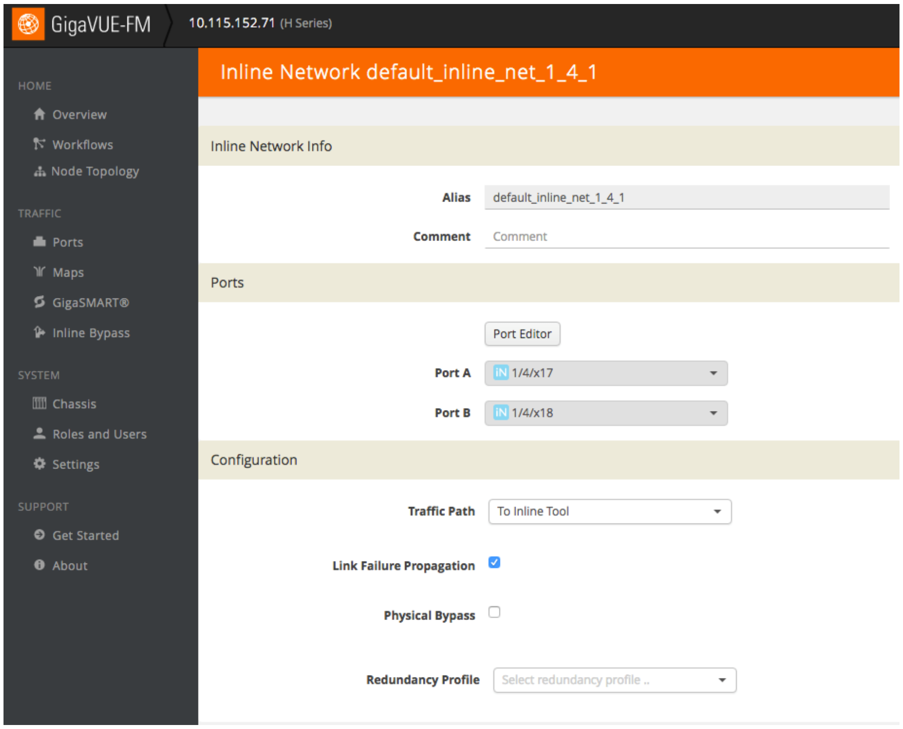
4. In Map Source and Destination, set the Source and Destination as follows:
    a. Set **Source** to the first inline network.
    b. Set **Destination** to inline tool group configured previously.
5. Click **Save.**

Changing the Inline Network Traffic Path to Inline Tool

After configuring the maps, you need to change the traffic path for the inline networks from Bypass to Inline Tool. However, before setting the traffic path to inline tools, make sure that the inline tool ports are up. To check the status of the ports, go to **Inline Bypass > Inline Tools.**

To change the traffic path from bypass to inline tool, perform the following:

1. In GigaVUE-FM, select **Inline Bypass** > **Inline Networks**.
2. Select one of the inline networks that you defined previously and then click **Edit**.
3. In the Configuration section, make the following changes as shown in Figure 32:
    a. From the **Traffic Path** drop-down list, select **To Inline Tool**.
    b. Uncheck **Physical Bypass**.



10.115.152.71 (H Series)

Inline Network default_inline_net_1_4_1

Inline Network Info

Alias: default_inline_net_1_4_1

Comment: Comment

Ports

Port Editor

Port A: IN 1/4/x17

Port B: IN 1/4/x18

Configuration

Traffic Path: To Inline Tool

Link Failure Propagation ☑

Physical Bypass ☐

Redundancy Profile: Select redundancy profile ..

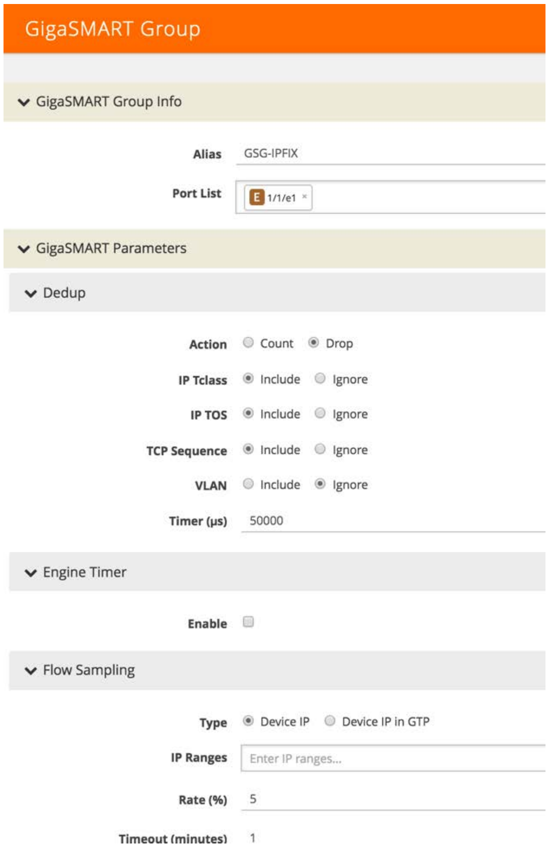
Figure 32: Inline Network Traffic Path Changed to Inline Tool, Physical Bypass Unchecked

4. Click **Save**.

Configuring IPFIX to Send metadata to Splunk Enterprise

This section demonstrates how to configure Gigamon GigaVUE-HC2 to send IPFIX metadata to Splunk Enterprise. Perform the following steps:

1. Create a GigaSMART group and assign parameters.. Commonly, de-duplication is used in conjunction with NetFlow. In the example shown in Figure 33, GigaSMART group for NetFlow and De-duplication is created.



GigaSMART Group

GigaSMART Group Info

Alias: GSG-IPFIX

Port List: E 1/1/e1 ×

GigaSMART Parameters

Dedup

Action: ○ Count ● Drop

IP Tclass: ● Include ○ Ignore

IP TOS: ● Include ○ Ignore

TCP Sequence: ● Include ○ Ignore

VLAN: ○ Include ● Ignore

Timer (µs): 50000

Engine Timer

Enable: □

Flow Sampling

Type: ● Device IP ○ Device IP in GTP

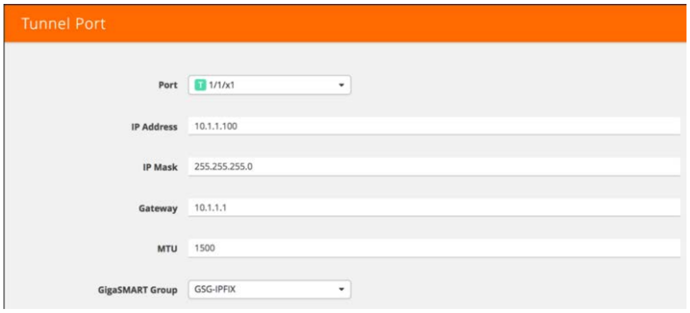
IP Ranges: Enter IP ranges...

Rate (%): 5

Timeout (minutes): 1

Figure 33: Creating a GigaSMART Group

2. Create a tunnel port on GigaVUE-HC2 as shown in Figure 34. The tunnel port is used to carry metadata out from the device to the network.



Tunnel Port

Port: T 1/1/x1

IP Address: 10.1.1.100

IP Mask: 255.255.255.0

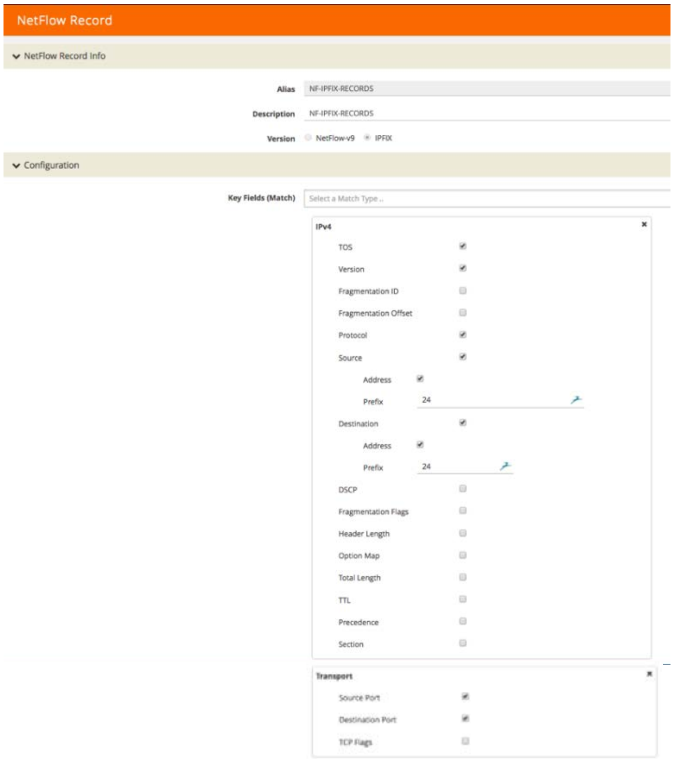
Gateway: 10.1.1.1

MTU: 1500

GigaSMART Group: GSG-IPFIX

Figure 34: Creating a Tunnel Port

3. Select **NetFlow / IPFIX Generation** > **Records and** click **New**. Configure the Netflow Record as shown in Figure 35 and Figure 36 where some match and collect fields are selected.



NetFlow Record

NetFlow Record Info

Alias: NF-IPFIX-RECORDS

Description: NF-IPFIX-RECORDS

Version: ○ NetFlow-v9 ● IPFIX

Configuration

Key Fields (Match): Select a Match Type ..

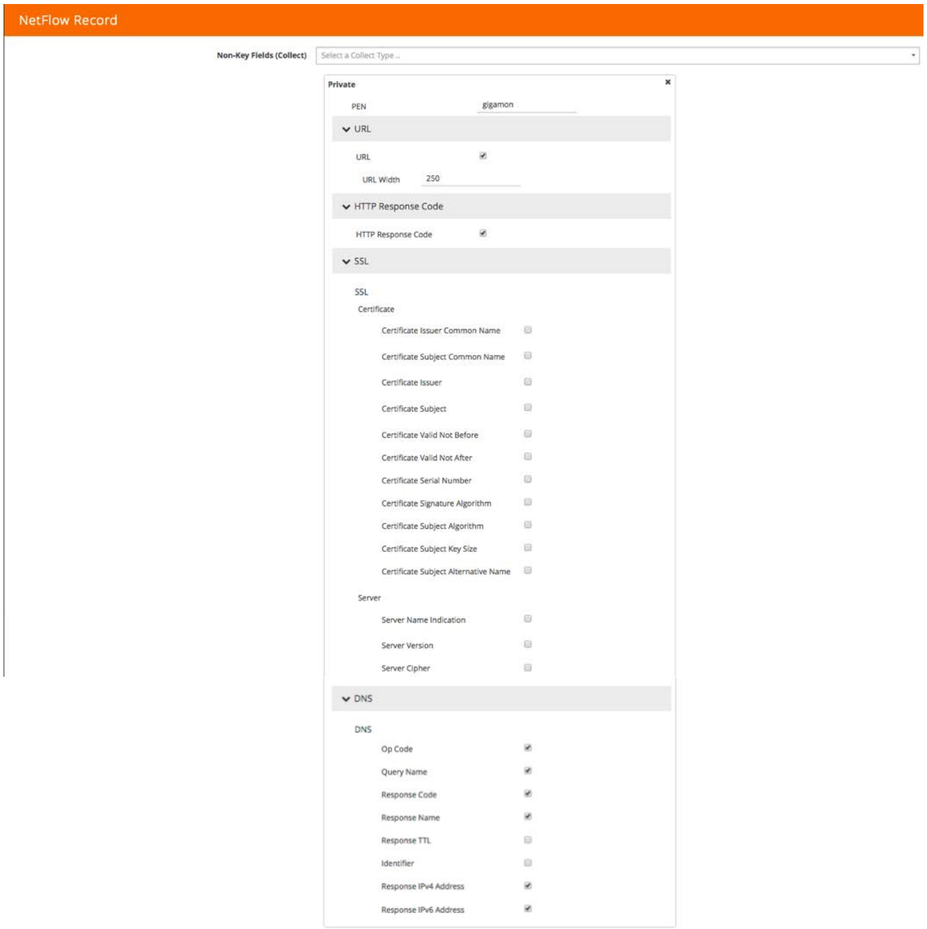
IPv4

- TOS ☑
- Version ☑
- Fragmentation ID □
- Fragmentation Offset □
- Protocol ☑
- Source ☑
  - Address ☑
  - Prefix 24
- Destination ☑
  - Address ☑
  - Prefix 24
- DSCP □
- Fragmentation Flags □
- Header Length □
- Option Map □
- Total Length □
- TTL □
- Precedence □
- Section □

Transport

- Source Port ☑
- Destination Port ☑
- TCP Flags □

Figure 35: Match fields used in NetFlow Record



NetFlow Record

Non-Key Fields (Collect) Select a Collect Type ..

Private

PEN: gigamon

URL

- URL ☑
- URL Width: 250

HTTP Response Code

- HTTP Response Code ☑

SSL

SSL

Certificate

- Certificate Issuer Common Name ☐
- Certificate Subject Common Name ☐
- Certificate Issuer ☐
- Certificate Subject ☐
- Certificate Valid Not Before ☐
- Certificate Valid Not After ☐
- Certificate Serial Number ☐
- Certificate Signature Algorithm ☐
- Certificate Subject Algorithm ☐
- Certificate Subject Key Size ☐
- Certificate Subject Alternative Name ☐

Server

- Server Name Indication ☐
- Server Version ☐
- Server Cipher ☐

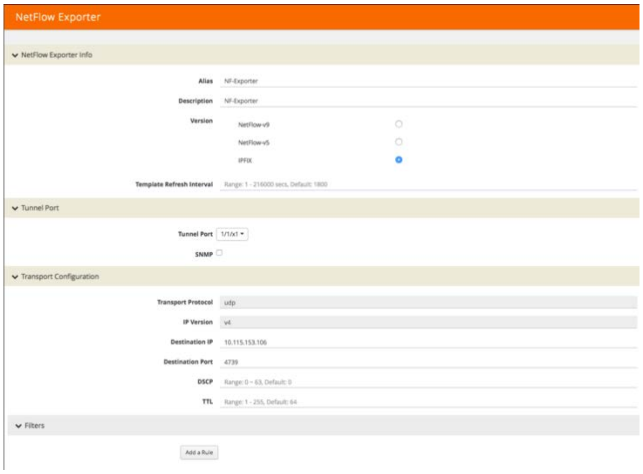
DNS

DNS

- Op Code ☑
- Query Name ☑
- Response Code ☑
- Response Name ☑
- Response TTL ☐
- Identifier ☐
- Response IPv4 Address ☑
- Response IPv6 Address ☑

Figure 36: Collect fields used in NetFlow Record

4. Select **Exporter** and click **New**. Configure the Netflow Exporter as shown in Figure 37. Remember to use the same destination port as configured in Splunk Enterprise in the section Configuring Splunk Enterprise.



NetFlow Exporter

NetFlow Exporter Info

Alias: NF-Exporter

Description: NF-Exporter

Version: NetFlow-v9 ○ NetFlow-v5 ○ IPFIX ●

Template Refresh Interval: Range: 1 - 216000 secs, Default: 1800

Tunnel Port

Tunnel Port: 1/1/x1

SNMP: □

Transport Configuration

Transport Protocol: udp

IP Version: v4

Destination IP: 10.115.153.106

Destination Port: 4739

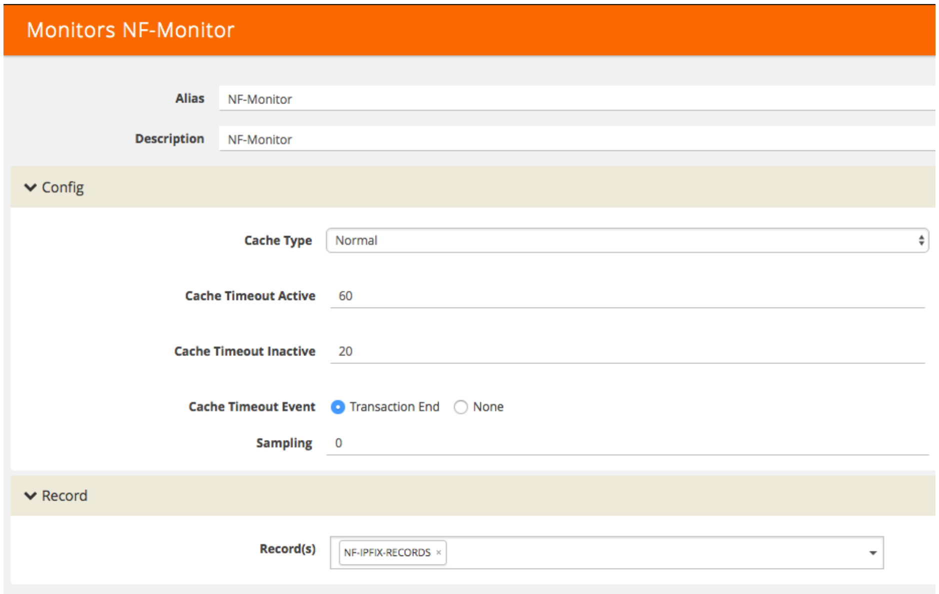
DSCP: Range: 0 ~ 63, Default: 0

TTL: Range: 1 - 255, Default: 64

Filters

Figure 37: NetFlow Exporter Configuration

5. Select **Monitors** and click **New**. Configure the Monitors as shown in Figure 38.



Monitors NF-Monitor

Alias: NF-Monitor

Description: NF-Monitor

Config

Cache Type: Normal

Cache Timeout Active: 60

Cache Timeout Inactive: 20

Cache Timeout Event: ● Transaction End ○ None

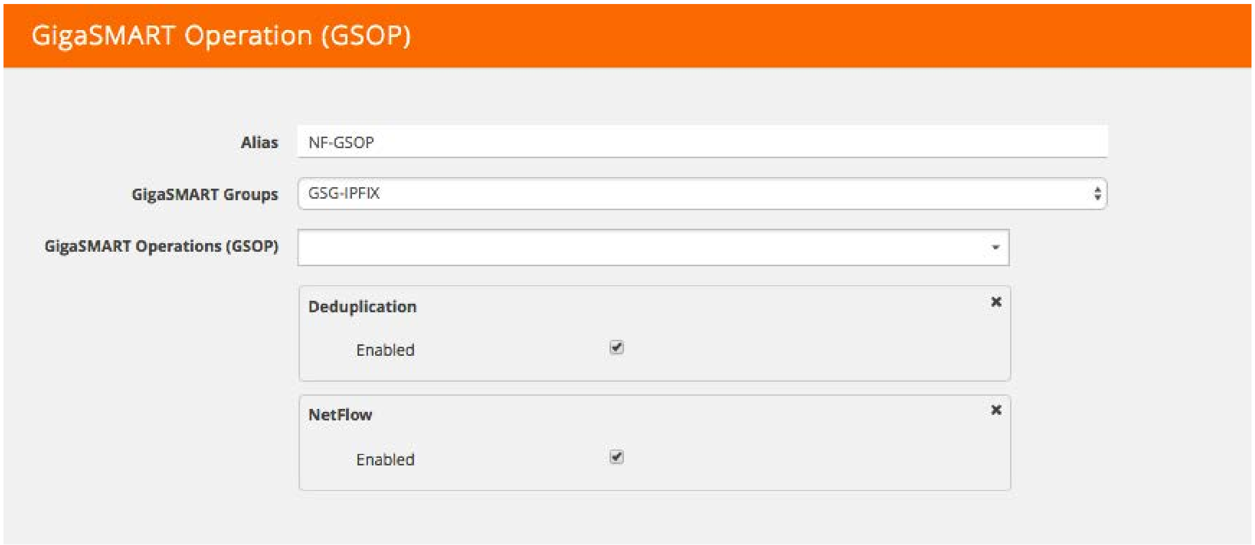
Sampling: 0

Record

Record(s): NF-IPFIX-RECORDS ×

Figure 38: NetFlow Monitor Configuration

6. Select **GigaSMART > GigaSMART Operations (GSOP)** and click **New** to create a new GSOP. Create a new GSOP as shown in Figure 39.



GigaSMART Operation (GSOP)

Alias: NF-GSOP

GigaSMART Groups: GSG-IPFIX

GigaSMART Operations (GSOP):

Deduplication

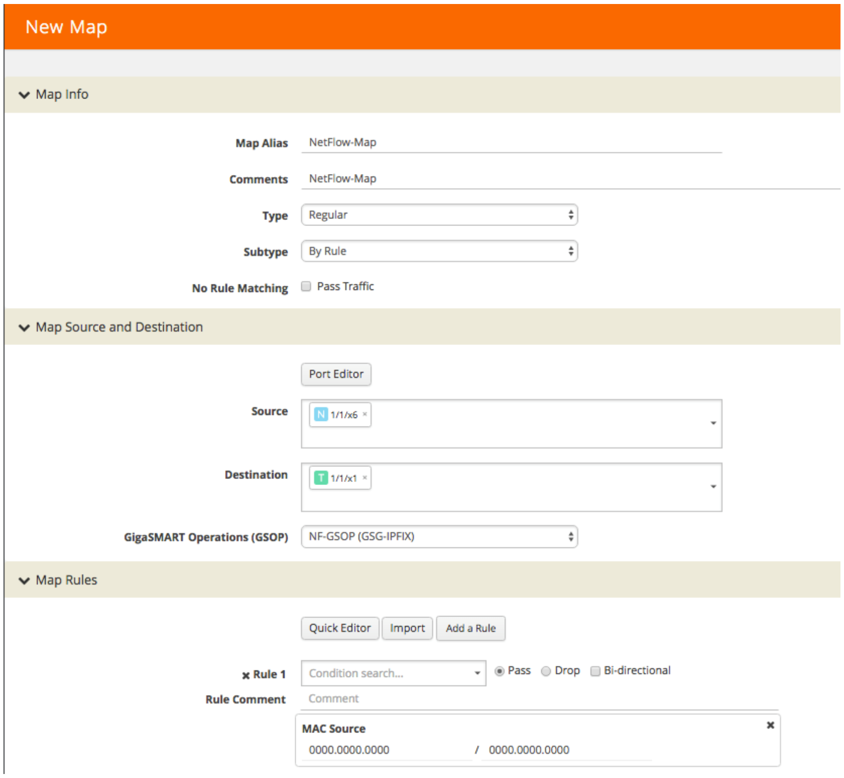
Enabled ☑

NetFlow

Enabled ☑

Figure 39: GSOP Configuration for NetFlow

7. Add a map to allow traffic to pass from the network port to the tool port. Use the GSOP created in the step 6. Add a new map as shown in Figure 40.



New Map

Map Info

Map Alias: NetFlow-Map

Comments: NetFlow-Map

Type: Regular

Subtype: By Rule

No Rule Matching: □ Pass Traffic

Map Source and Destination

Source: N 1/1/x6

Destination: T 1/1/x1

GigaSMART Operations (GSOP): NF-GSOP (GSG-IPFIX)

Map Rules

Rule 1: Condition search... ● Pass ○ Drop □ Bi-directional

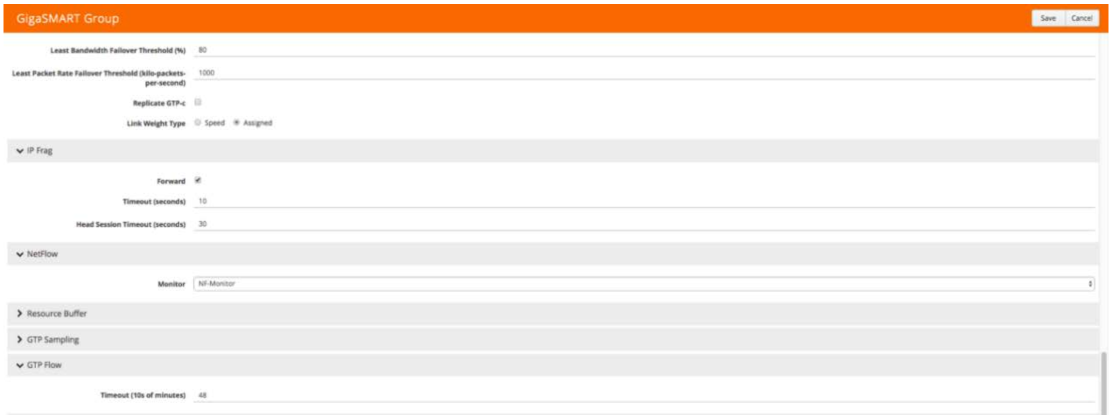
Rule Comment: Comment

MAC Source

0000.0000.0000 / 0000.0000.0000

Figure 40: Map for NetFlow

8. Select **GigaSMART > GigaSMART Groups.** Select the GigaSMART Group configured previously and click on **Edit**. Scroll down to the bottom of the page and click **NetFlow**. From the **Monitor** drop-down list, select the monitor created in the step 5. Configure the GigaSMART groups as shown in Figure 41.



Least Bandwidth Failover Threshold (%) 80

Least Packet Rate Failover Threshold (kilo-packets-per-second) 1000

Replicate GTP-c □

Link Weight Type ○ Speed ● Assigned

Forward ☑

Timeout (seconds) 10

Head Session Timeout (seconds) 30

Monitor NF-Monitor

Timeout (10s of minutes) 48

Figure 41: GigaSMART Group Configuration

Other Gigamon Features

Gigamon's Visibility Platform offers a variety of additional services that combine with services described already in the previous sections.

One can use inline flow mapping to provide the tools with the exact traffic they need, eliminating oversubscription and tool overload. Moreover, GigaSMART® technology extends the intelligence and value of the Gigamon Security Delivery Platform by enhancing the monitoring of your network infrastructure and improving security tool performance.

A range of applications are available to optimize the traffic sent from your network to the tools you rely upon to monitor, manage, and secure the network. GigaSMART's advanced processing engine can be accessed anywhere within the Gigamon Visibility Platform without port- or card-based restrictions. GigaSMART engines can be combined to manage higher traffic loads and optimized for specific applications. GigaSMART applications can be combined or service chained so the traffic is optimized and delivered based on multiple functions running concurrently, such as decrypting SSL/TLS traffic after packet duplicates have been removed, or stripping VLAN headers before load balancing the traffic and sending it out to the appropriate tools.

Some GigaSMART applications of interest include:

- **SSL/TLS Decryption**: Provides automatic visibility into SSL/TLS traffic regardless of the port or application while sending it to multiple inline or out-of-band tools simultaneously. For more information, refer to the SSL/TLS decryption page (https://www.gigamon.com/products/technology/ssl-tls-decryption).

- **Application Session Filtering (ASF)**: Forwards complete application sessions traffic to security appliances increasing their efficacy and performance, classifies flows of interest using signatures to filter applications such as video streaming, email, web 2.0, and other business applications, and provides complete visibility into traffic flows by forwarding all packets from session initiation to termination to security and monitoring tools. For more information, see the feature brief (https://www.gigamon.com/sites/default/files/resources/feature-brief/fb-application-session-filtering-3169.pdf).

- **Packet Deduplication**: Relieves tool processing resources when packets are gathered from multiple collection points along a path or inter-VLAN communications by only forwarding a packet once.

- **FlowVUE®** : Performs flow-aware sampling of active connections to selectively reduce traffic bound to monitoring and analytic tools. For more information, see the feature brief (https://www.gigamon.com/sites/default/files/resources/feature-brief/fb-flowvue-active-subscriber-aware-flow-sampling-3096.pdf)

- **Header Stripping**: Eliminates the need for monitoring tools to decipher protocols, normalize the data provided to the tools, and allow easy filtering, aggregation, and load balancing of packets with headers removed.

- **Packet Slicing**: Reduces the packet size to increase the processing and monitoring throughput, allowing tools to process fewer bits while maintaining the vital, relevant portions of each packet thus significantly increasing the capacity of forensic recording tools.

For more information on GigaSMART applications, see the GigaSMART data sheet at - https://www.gigamon.com/sites/default/files/resources/datasheet/ds-gigasmart-4003.pdf.

Summary

The changing threat landscape and evolving network infrastructure are forcing organizations to fundamentally rethink their approach to security in order to keep advanced threats at bay. Security teams are turning to multi-tiered deployments, leveraging the latest threat intelligence tools to protect their network. However, these tools are only as effective as the information they see. The ability to filter through the deluge of Big Data from across the network and scrutinize it in real time is vital to identifying and mitigating advanced threats.

Gigamon's Visibility Platform offers a comprehensive and sophisticated security services delivery platform. It provides scalability while improving resiliency, simplifying management, and enabling the deployment of best-of-breed security solutions. Gigamon works with security tools to increase their field of vision, improve their performance, support resiliency, reduce troubleshooting times, and accelerate return on investment. The Gigamon Visibility Platform provides the platform for end-to-end visibility coupled with traffic intelligence that is needed to efficiently manage risks and mitigate threats in today's ever-evolving network environments.

See Inside Your Network™

4128-01 04/17