Cisco FirePOWER with Gigamon Inline Deployment Guide

Contents

1 Overview

Gigamon's GigaSECURE Security Delivery Platform and Cisco FirePOWER offer a combined solution that meets today's active inline security needs. This solution can scale as the protected network infrastructure grows with the addition of network links. With Gigamon's bypass functionality in place, quick addition and removal of inline security devices for maintenance, software/firmware upgrades, or simply to move the device to another area of the network is seamless, eliminating the need to schedule downtime during off-peak hours. The inline tool group with Cisco FirePOWER ensures that the inline security *service* remains available regardless of appliance maintenance or failure. Additionally, Gigamon's bypass protection capability provides continuous network availability in the event of failure of any GigaSECURE nodes used for bypass protection.

The Cisco FirePOWER System is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. The use cases in this guide were validated with virtual FirePOWER sensors (also called NGIPSv) and virtual FirePOWER Management Center deployed on an ESXi host using the VMware vSphere Hypervisor. The Cisco virtual FirePOWER appliance was validated in conjunction with a GigaVUE-HC2 node. The GigaVUE-HC2 is a 4-slot visibility appliance that is part of the GigaSECURE Security Delivery Platform. The steps outlined in this guide are also applicable for inline deployment of a physical FirePOWER appliance with a Gigamon GigaVUE-HC2.

The solution described in this guide is based on a standard active inline network and tool deployment where virtual NGIPSv sensors configured to act as Intrusion Prevention System (IPS), File Download Detection, and Malware appliances are directly cabled in series to one GigaVUE-HC2 chassis. Upon full deployment, the GigaVUE-HC2 sends only the traffic of interest to these inline tool groups for traffic analysis, file and malware inspection.

This chapter covers the following:

- Use Cases
- Deployment Prerequisites
- Architecture Overview
- Access Credentials

Use Cases

This section describes the following use cases:

- Load balancing (parallel mode)
- Serial Mode

Use Case 1: Load Balancing (Parallel) mode

There are multiple network links of varied speeds and media in an infrastructure that need to be protected by Cisco security solutions. When the aggregate traffic exceeds the capacity of any single Cisco sensor, multiple sensors must be deployed with the ability to distribute traffic among the group of sensors. The Gigamon GigaSECURE Security Delivery Platform provides the ability to select traffic of interest, while bypassing the rest, then distributing the selected traffic of interest amongst two or more sensors.

This distribution ensures all packets in a given TCP/UDP session go to the same group member. It also ensures that if any member of the group goes offline for any reason, the traffic will be distributed amongst the remaining members, thereby ensuring availability of the security functions provided by Cisco FirePOWER.

Gigamon also gives the ability to test the configuration in an out-of-band mode called “bypass with monitoring” to allow complete confidence before going “live”. Switching from out-of-band to in-band is done by changing a setting in the inline network link, eliminating the need for physical change control procedures.

Use Case 2: Serial Mode

This use case is similar to the above except there are several different types of Cisco inline security tools that network traffic will pass through sequentially. Traffic can be filtered in the Gigamon GigaVUE-HC2 for each inline tool so only relevant traffic will flow through that tool.

The above two use cases are validated together by configuring IPS and DLP sensors in series going to two Malware sensors in parallel for load balancing. Refer Figure 1-1. However, if only serial or parallel mode is desired for other specific use cases then the relevant subset from this user guide can be leveraged.

Deployment Prerequisites

The Gigamon and Cisco FirePOWER combined solution consists of the following:

- GigaVUE-HC2 chassis running GigaVUE-OS 4.5 with:
  - 1 TAP-HC0-G100C0 Copper bypass module
  - 1 TAP-HC0-D25AC0 Fiber bypass module
- GigaVUE-FM version 3.2 Fabric Manager
- Cisco Virtual FirePOWER Management Center appliance version 6.0.0 (Snort version 2.9.8 GRE)
- Cisco Virtual Next-Generation IPS (NGIPSv) for VMWare version 6.0.0
- Two Windows virtual machines used to simulate as server and a client. The server VM runs Webserver uploaded with files types such as .exe, pdf, RIFF and malware files. When the user from a client VM attempts to access these files, the FirePOWER appliance inspects the files and depending on the configured policy in FirePOWER, the content would be blocked or allowed and the action logged.

Note: The GigaVUE-HC2 offers inline bypass modules for both 1Gb Copper and 10Gb Fiber interfaces. Both types of modules have the same bypass functionality. The 10Gb Fiber bypass module additionally offers tool ports on the same module. For this deployment guide the Copper interface module was used on the GigaVUE-HC2 as the Cisco NGIPSv was set up with 1Gb copper interfaces. In this deployment guide, only the tool ports on the GigaVUE-HC2 Fiber bypass module are used.

This guide assumes that all appliances (both physical and virtual) are fully licensed for the features used, management network interfaces have been configured, and an account with sufficient admin privileges is used.

This document is intended to provide the information of integrated solution for evaluation purpose and should be modified appropriately for production deployments.

Architecture Overview

This section presents the combined solution using a GigaVUE-HC2 inline bypass node with Cisco FirePOWER System. The reference architecture in Figure 1-1 shows the position of each component in the overall infrastructure, where all network components and inline security tools are connected directly to the GigaVUE-HC2. The proposed monitoring configuration uses eight ports on module 1 for inline tools, and four ports on module 3 as protected inline bypass ports. Figure 1-2 shows the logical layout of the setup where traffic flow traverses the IPS, DLP, and Malware engines in the Cisco FirePOWER suite sequentially. The two malware engines are connected in parallel for load-balancing purposes. Figure 1-3 shows the traffic flow diagram. All inline bypass links are inherently bidirectional. The traffic flow diagram below shows only one direction of traffic flow to simplify the illustration. Ports 1,6,7,12 represent inline network ports while ports 2,3,4,5 represent inline tool serial and ports 8,9,10 and 11 represent inline tool group ports.

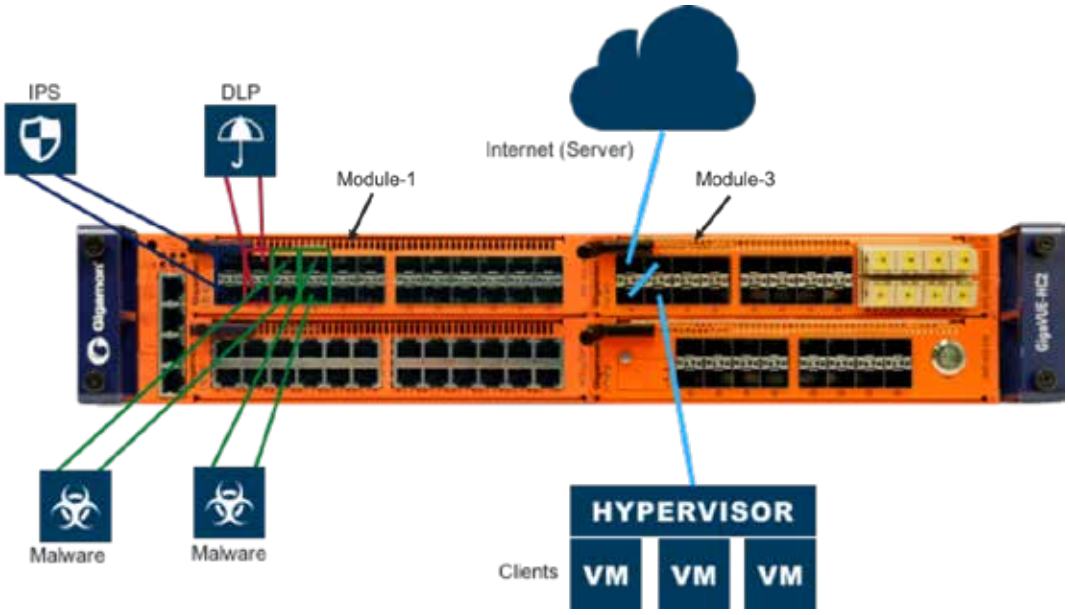


Figure 1-1: Gigamon Inline Bypass with Cisco FirePOWER System

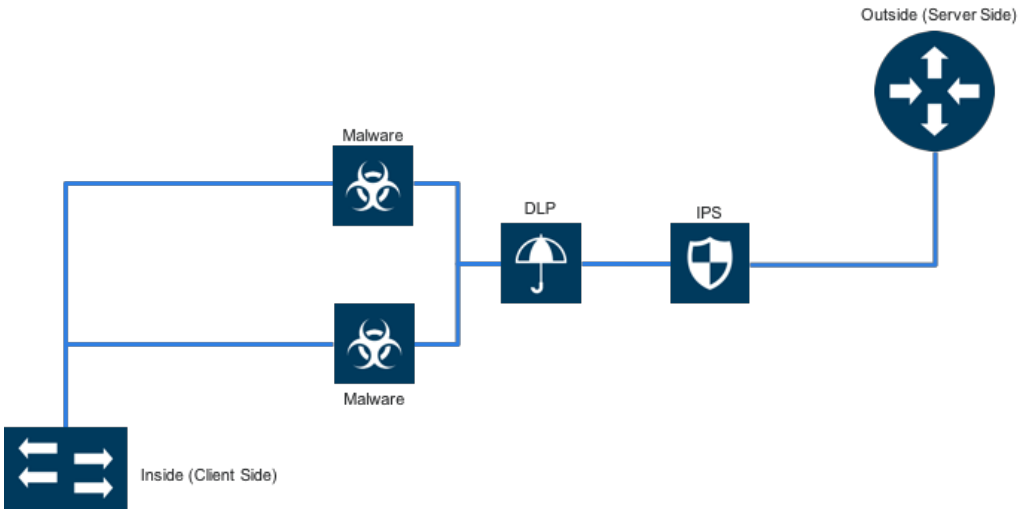


Figure 1-2: Logical Layout for Inline tools

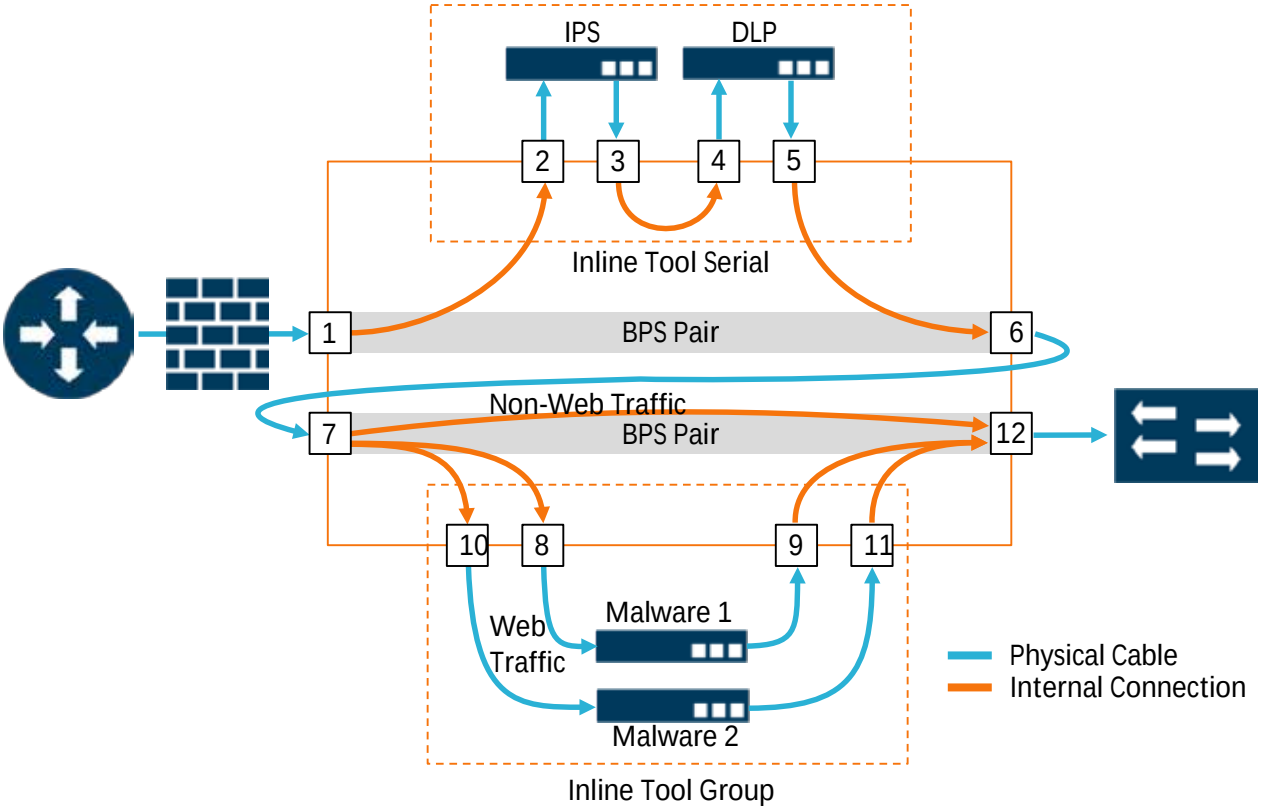


Figure 1-3: Traffic Flow Diagram

Note: For any inline configuration, it is critical to align tools so that the trusted (or inside or client side) connection is on the correct port of the tool or tools. With out-of-band monitoring, port ordering is less important because only a copy of the original packet is delivered to the out-of-band tool with the original packet in the network unaffected. For inline monitoring, failure to ensure that the trusted and untrusted sides are connected properly will cause the inline tool to improperly apply protections. For example, attaching the Internet connection to the inside port would cause a firewall to permit almost any traffic to enter the protected network. Inside client-originated traffic incorrectly connected to the outside port of a firewall would likewise have virtually all communications blocked.

The setup in this guide has FirePOWER virtual sensors deployed and configured with two network port groups – Inside and Outside. Data flows from inside (trusted) side where the clients reside to outside (unprotected) side for Internet access and vice versa. The network adapter (vmnic) assigned to Inside and Outside port group of FirePOWER sensors should match Port A and Port B, respectively, of inline network and inline tool configuration in a GigaVUE-HC2.

Access Credentials

The following are the Gigamon GigaVUE-FM default access credentials:

- Username: admin
- Password: admin123A!
- There is no default management IP address.

The following are the Cisco virtual sensor/management center access defaults:

- Username: admin
- Password: Admin123

NOTE: The GigaVUE-HC2 supports a Graphical User Interface (GUI) named H-VUE and a Command Line Interface (CLI). This document shows only the steps for configuring the GigaVUE-HC2 with Gigamon's centralized management application GigaVUE-FM. For the equivalent H-VUE and CLI configuration commands, refer to the *Gigamon-OS H-VUE User's Guide and GigaVUE-OS CLI User's Guide,* respectively, for the 4.5 release.

2 Configurations

This chapter describes the configuration procedures for GigaVUE-HC2 through GigaVUE-FM and procedures for NGIPSv sensors policies through Cisco FirePOWER Management Center. The procedures are organized as follows:

- Cisco NGIPSv Configuration: Inline Tools
- Gigamon GigaVUE-HC2 Configuration: Inline Network and Inline Tool, Series Groups

The Cisco FirePOWER Management Center provides a centralized management console with a Web interface that you can use to perform administrative, management, analysis, and reporting tasks. For this deployment guide, the procedures focus on setting up the NGIPSv sensors with policies. This chapter assumes that all four FirePOWER virtual sensor nodes are deployed and setup with initial jumpstart configuration. Note that all NGIPSv sensors are deployed virtually with the same ovf image. Based on the licenses applied and policies configured, these sensors can be tuned to perform different roles. In this guide, four sensors are used – one sensor configured with IPS policy, a second sensor configured with file download detection policy and third and fourth sensors, connected in parallel for load balancing, configured with malware detection policy.

All the sensors are directly connected to the GigaVUE-HC2 as shown in Figure 1-1. All GigaVUE-HC2 ports that connect to virtual NGIPSv sensors should be configured as port type *Inline Tool*. Furthermore, all GigaVUE-HC2 inline bypass ports that connect to the inline network should be configured as port type *Inline Network*. For specific instructions on how to complete these tasks, refer to the Help Topics links in GigaVUE-FM.

Cisco FirePOWER Configuration: Inline Tools

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

Step 1: Create default access control policies for each sensor

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, do the following:

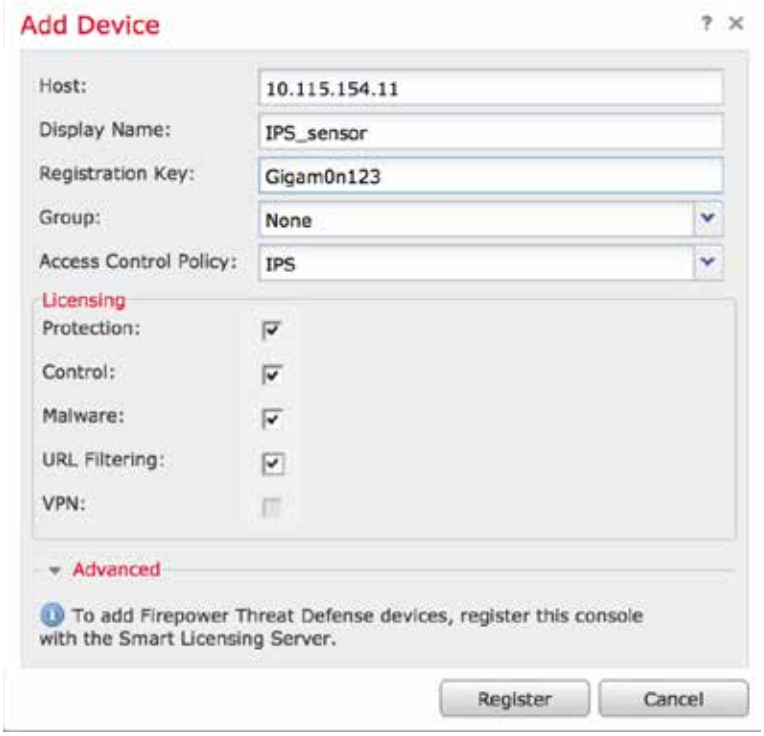
1. Select to **Policies > Access Control > Access Control**.
2. Click **New Policy**, and then create a default policy from any source zone to any destination zone keeping all the default parameters intact.
3. Repeat this step 2 for each sensor.

Step 2: Register Devices

For a sensor to be managed by Cisco FirePOWER Management Center, it needs to be registered.

In the Cisco FirePOWER Management Center, do the following:

1. Select **Devices > Device Management > Add Device**.
2. Fill out the information as shown in the following figure, and then click **Register**.

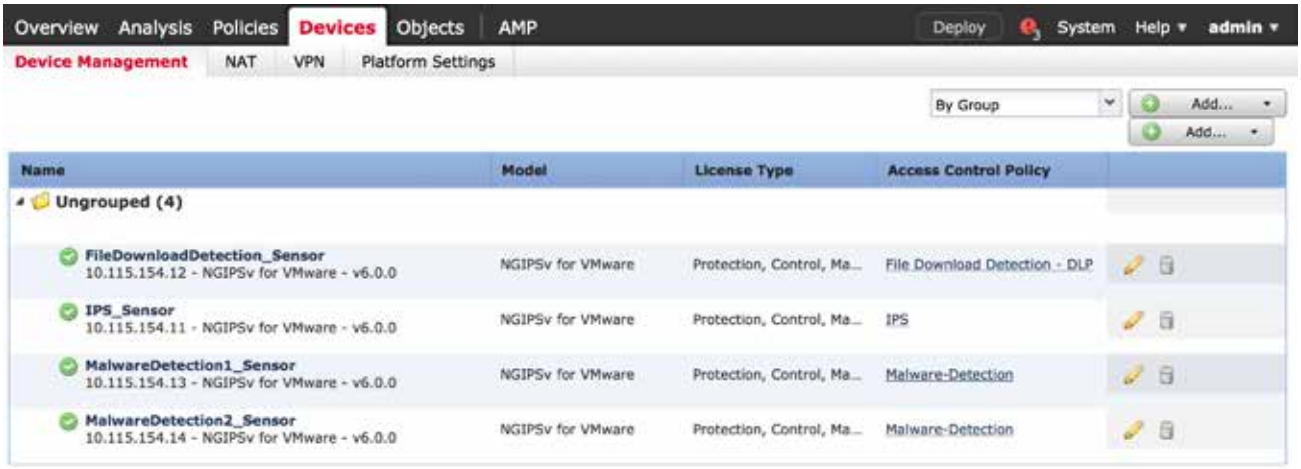


Notes:

- In the Registration Key field, enter the same registration key used while configuring sensor jumpstart settings.
- Choose an Access Control Policy to be used by the device.
- Choose licenses to apply to the device.

3. Repeat step 2 for each sensor.

The finished Device Management page should look similar to what is shown in the following figure.

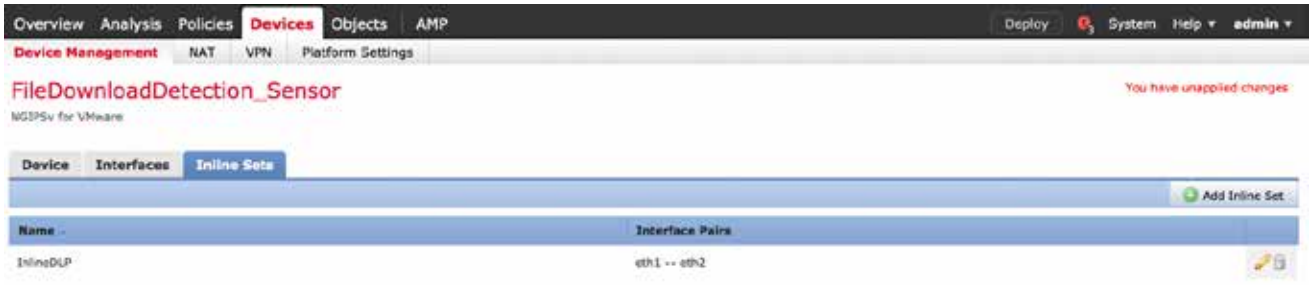


Step 3: Configure Inline Set

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, do the following:

1. Select **Devices > Device Management > Inline Sets**
2. Click **Add Inline Set**.

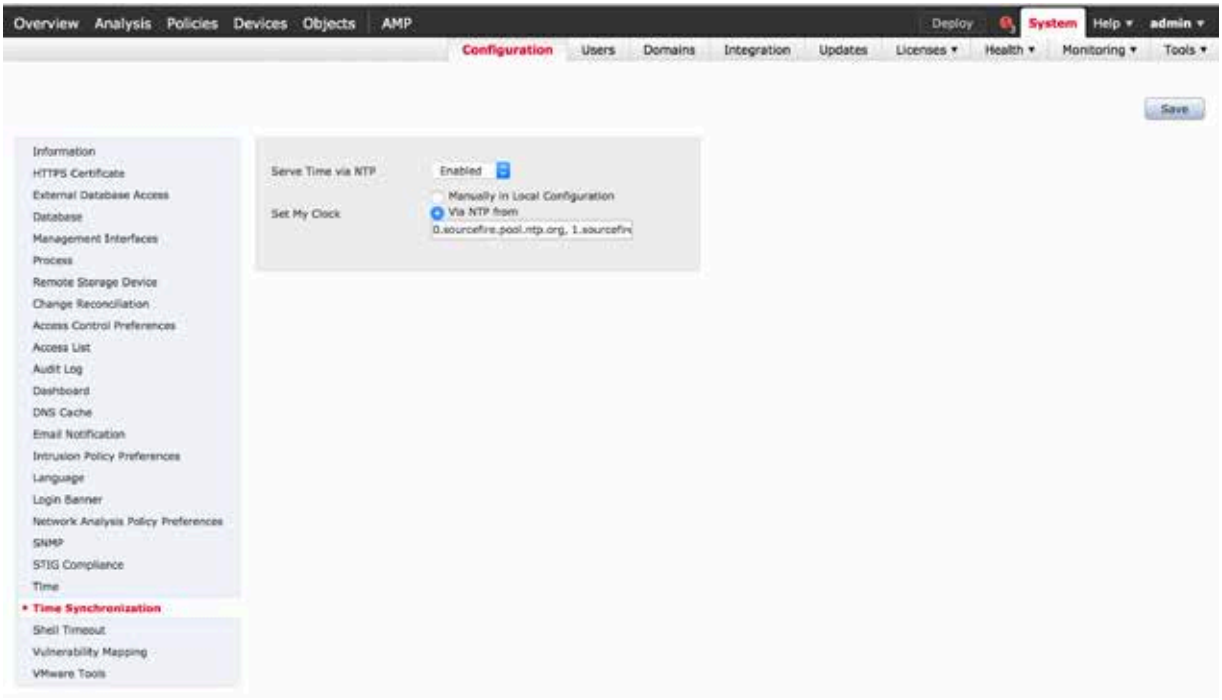


Step 4: Configure Cisco FirePOWER Settings

a) Time Synchronization Setting

In the Cisco FirePOWER Management Center, do the following:

1. Select **System > Configuration**.
2. Select **Time Synchronization** from the navigation panel on the left. Change the NTP server if needed.

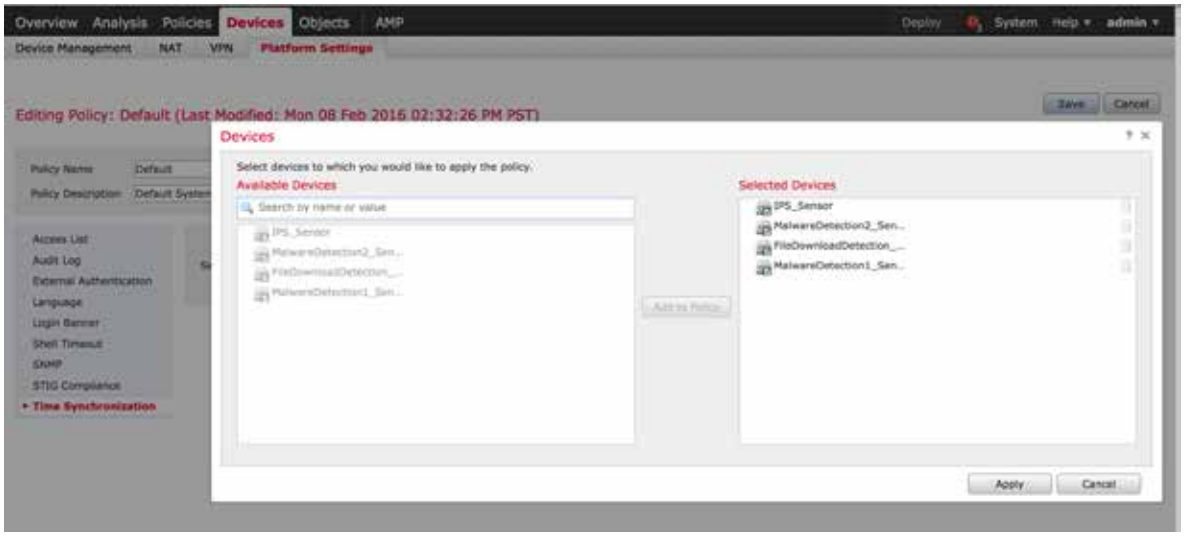


b) Default Settings Policy

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. This is done by configuring “platform settings”. Any changes to a “platform settings” policy affects all managed devices where the policy is applied.

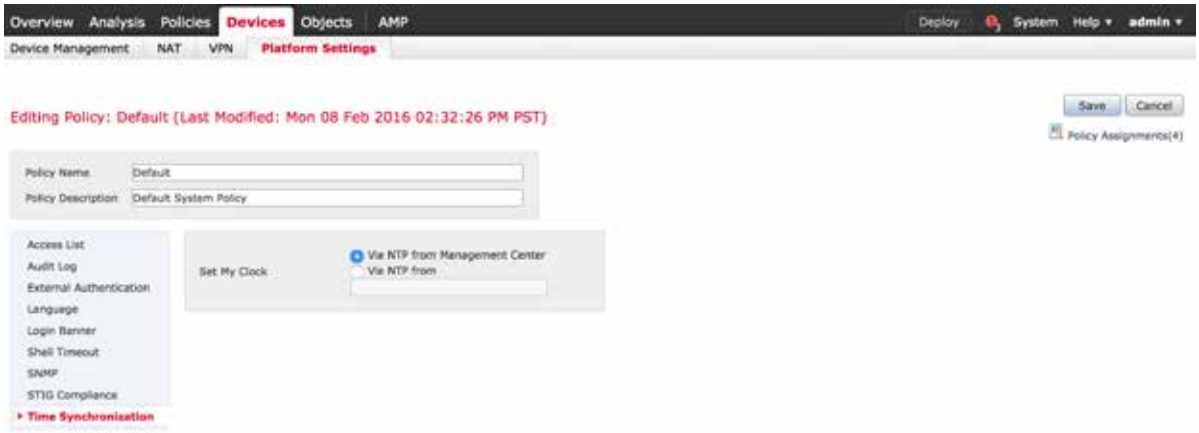
In the FirePOWER Management Center, do the following:

1. Select **Devices > Platform Settings**.
2. Name the policy Default Settings Policy. Add all devices. Refer to the following figure.



c) Time Synchronization for Sensors

Select **Time Synchronization** from the navigation panel on the left. Confirm that the **Via NTP from Management Center** radio button is selected. You can also use a Cisco FirePOWER Management Center as a Network Time Protocol (NTP) server for its managed devices.



Step 5: Create Sensor policies

a) Intrusion Policy

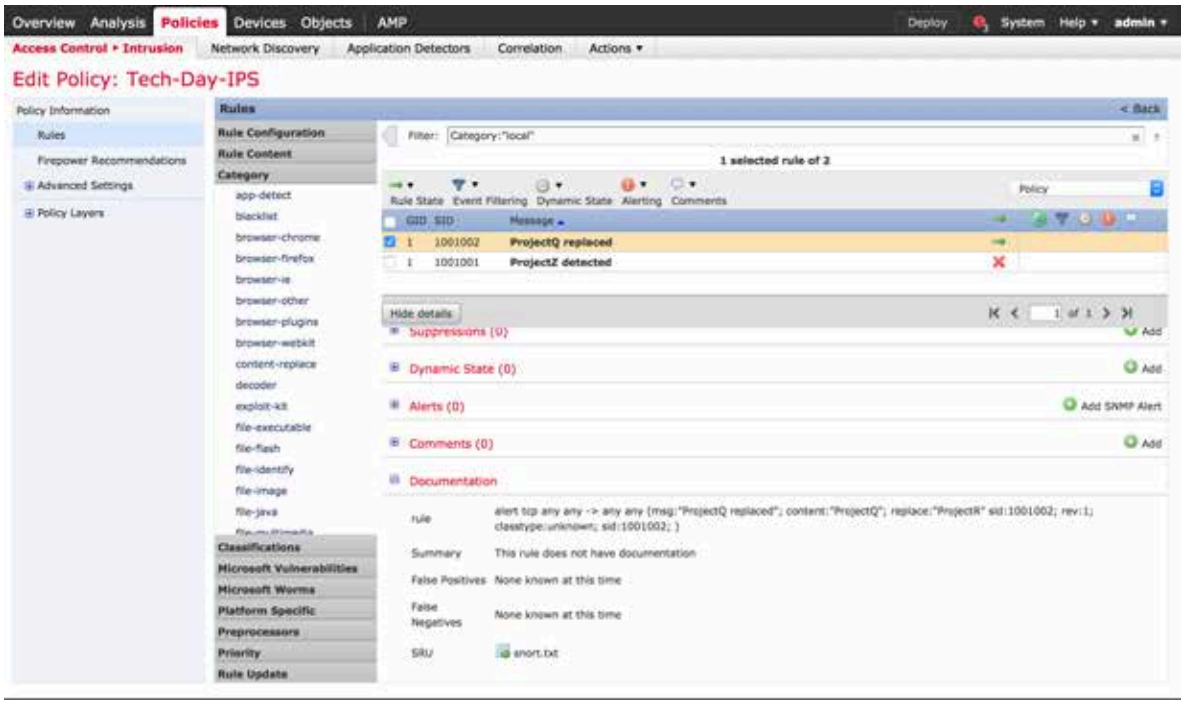
To add Intrusion policy through Cisco FirePOWER Management Center, select **Policies > Access Control > Intrusion**.

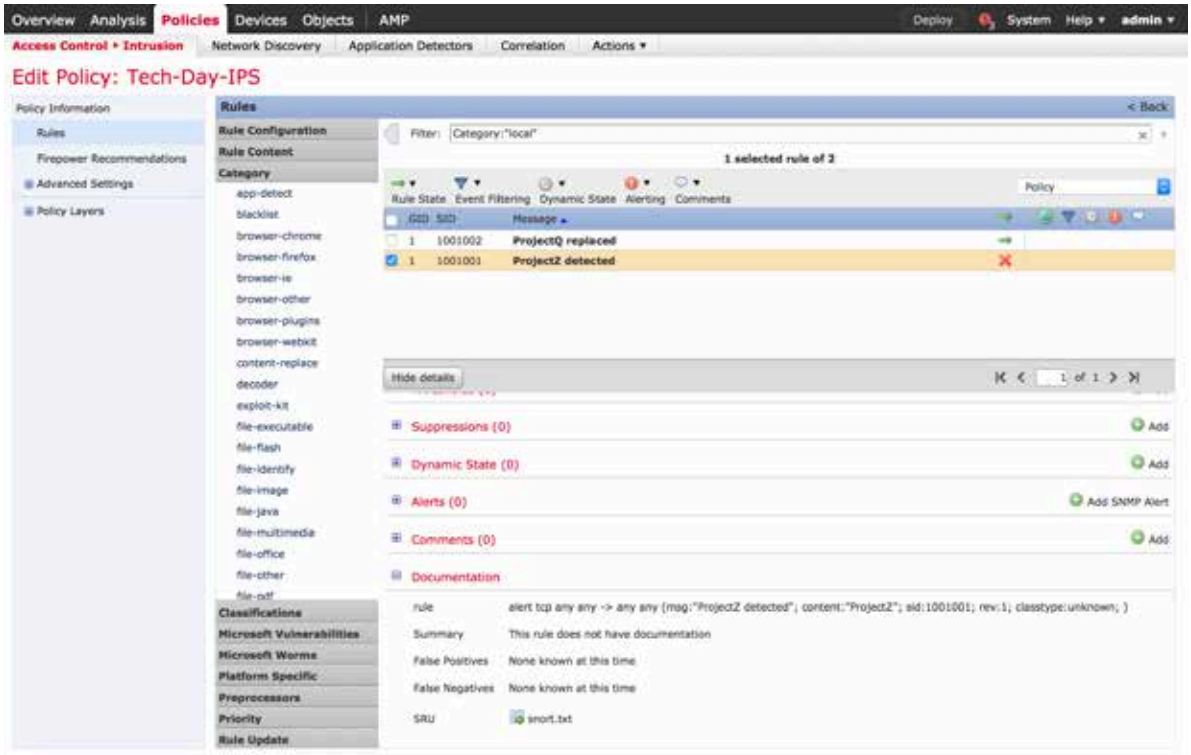
The first example below adds a rule to replace and allow a string with “ProjectQ” text string with “ProjectR” in a traffic flow. The second example detects and blocks a flow when “ProjectZ” text string is detected. These policies are created with following rules,

alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR"; sid: 1001001; rev:1;)

alert tcp any any -> any any (msg:"ProjectZ detected"; content:"ProjectZ"; sid: 1001002; rev:1;)

Note: These simple string match detection rules are created for testing purpose only. Refer to Cisco's documentation to learn how to create policies manually.

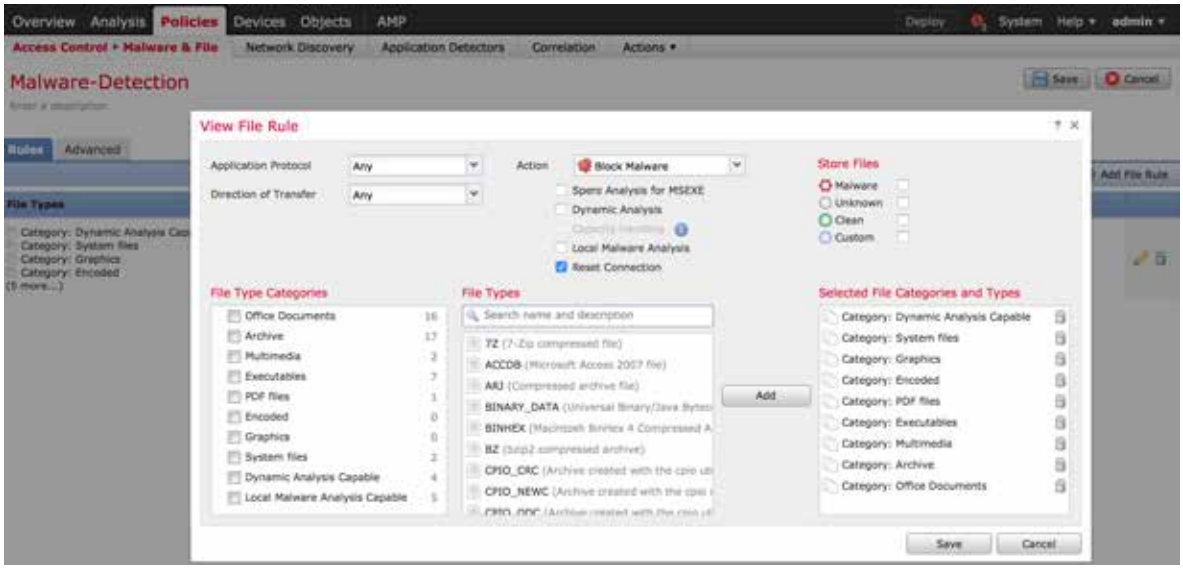




b) Malware Policy

To add Malware policy through Cisco FirePOWER Management Center, select **Policies > Access Control > Malware and File**

In the following example, certain file formats such as PDF, graphics, and executables are checked for malware content. If any malware is detected, file access is blocked.

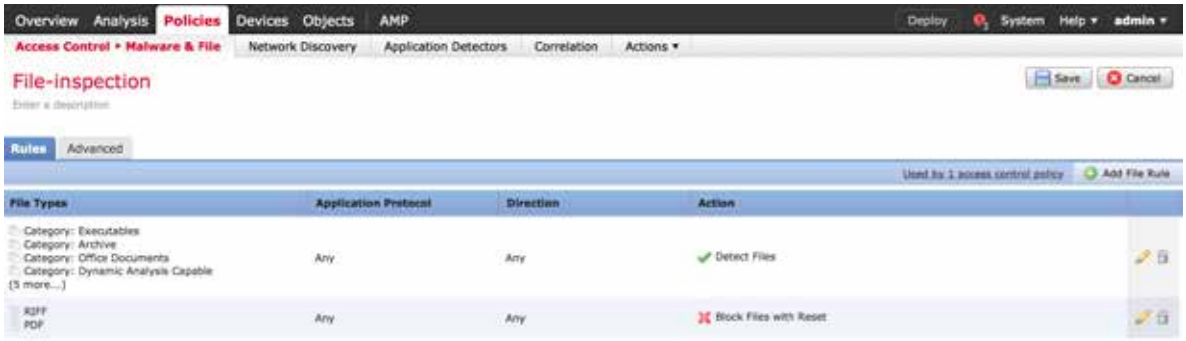


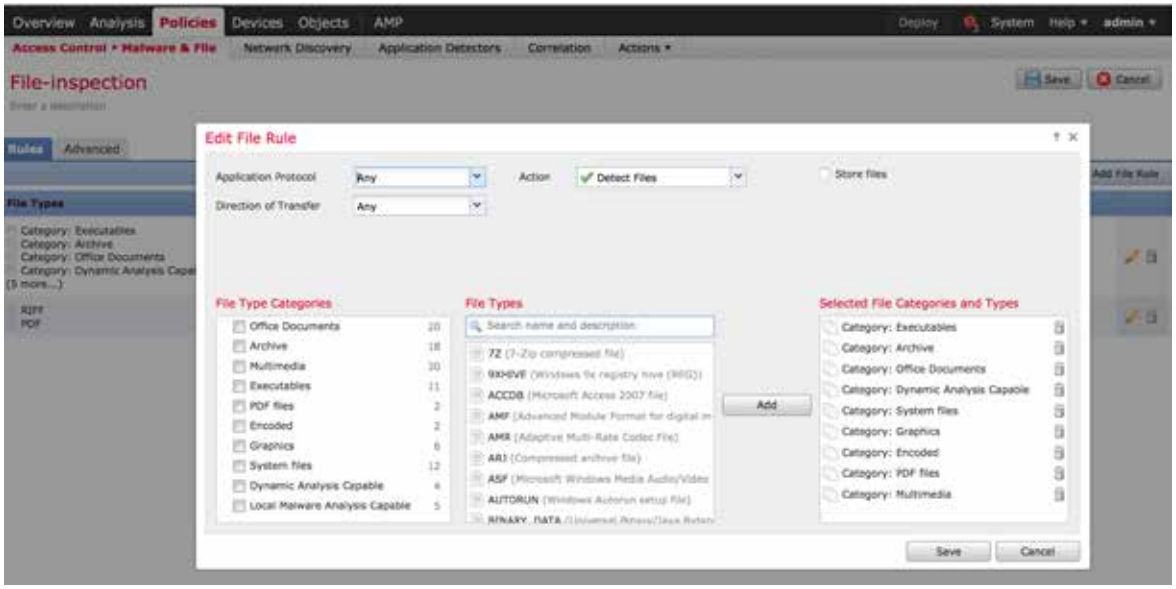
c) File Inspection Policy

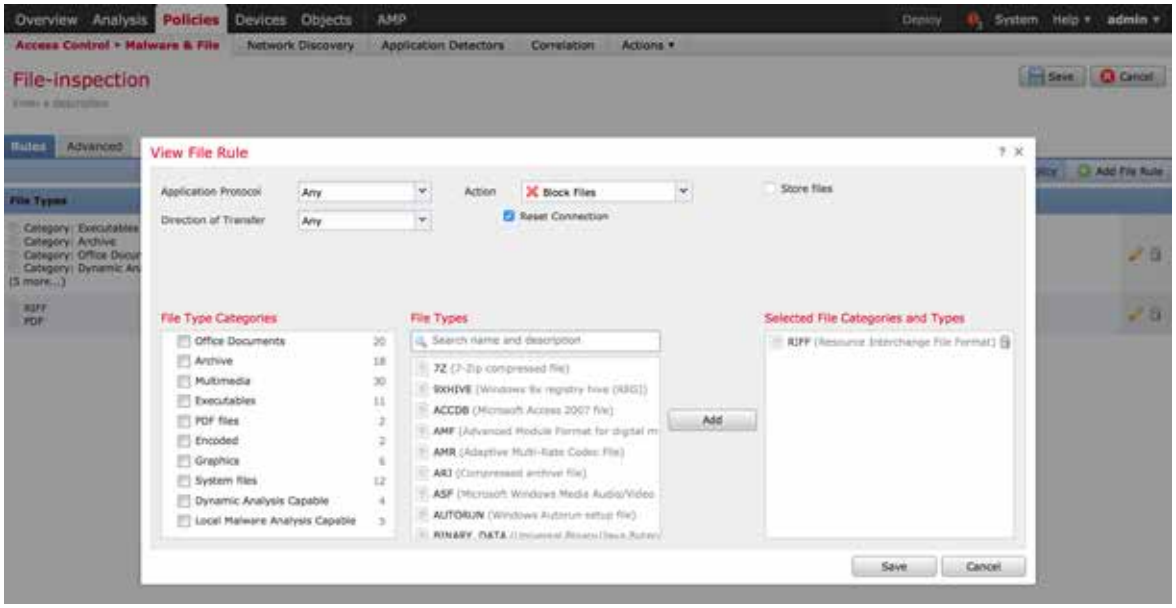
To add File Inspection policy through Cisco FirePOWER Management Center, select **Policies > Access Control > Malware and File**.

In the first example below, certain file formats such as PDFs, graphics, and executables would be reported as detected and event logged for the user.

In the second example, RIFF files such as audio/video would be blocked and event logged for the user.


Overview Analysis Policies Devices Objects AMP
Deploy System Help admin
Access Control ▸ Malware & File Network Discovery Application Detectors Correlation Actions
File-inspection
Save Cancel
Rules Advanced
Used by 1 access control policy Add File Rule
File Types Application Protocol Direction Action
Category: Executables
Category: Archive
Category: Office Documents
Category: Dynamic Analysis Capable
(5 more...)
Any Any Detect Files
RIFF
PDF
Any Any Block Files with Reset


Edit File Rule
Application Protocol Any
Action Detect Files
Store files
Direction of Transfer Any
File Type Categories
Office Documents
Archive
Multimedia
Executables
PDF files
Encoded
Graphics
System files
Dynamic Analysis Capable
Local Malware Analysis Capable
File Types
Search name and description
Add
Selected File Categories and Types
Category: Executables
Category: Archive
Category: Office Documents
Category: Dynamic Analysis Capable
Category: System files
Category: Graphics
Category: Encoded
Category: PDF files
Category: Multimedia
Save Cancel


View File Rule
Application Protocol Any
Action Block Files
Store files
Direction of Transfer Any
Reset Connection
File Type Categories
Office Documents
Archive
Multimedia
Executables
PDF files
Encoded
Graphics
System files
Dynamic Analysis Capable
Local Malware Analysis Capable
File Types
Search name and description
Add
Selected File Categories and Types
RIFF (Resource Interchange File Format)
Save Cancel

Step 6: Apply the device level policy to global access policy and assign to target sensors

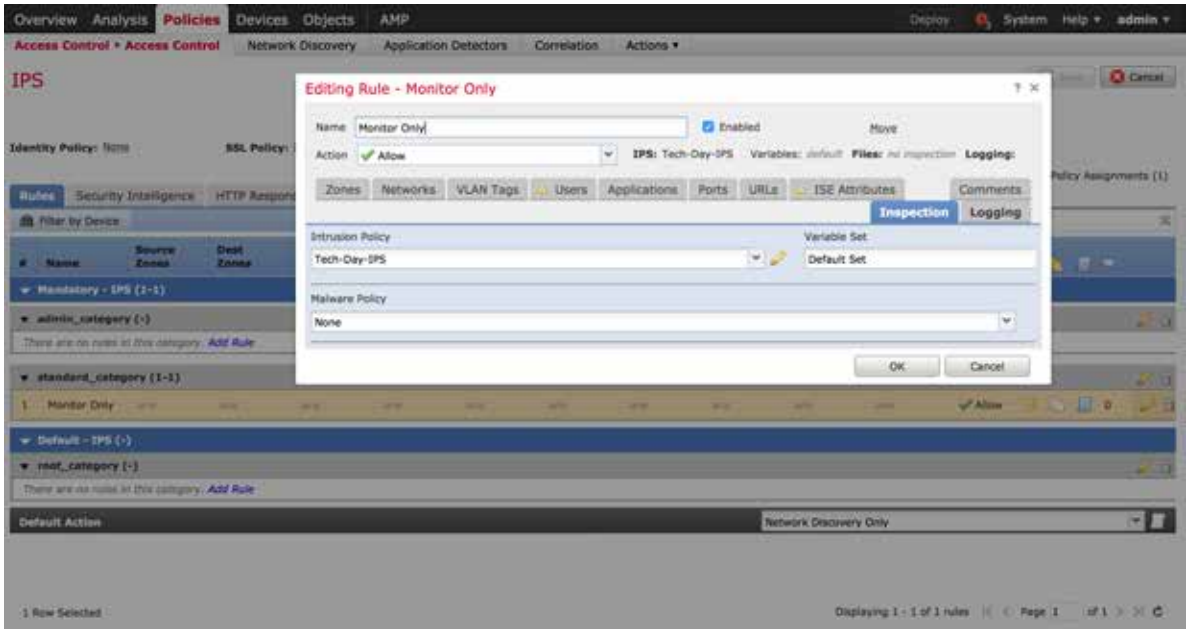
This section describes how to apply the device level policy to the global access policy, and then assign it to the target sensors.

a) IPS Access Control Policy

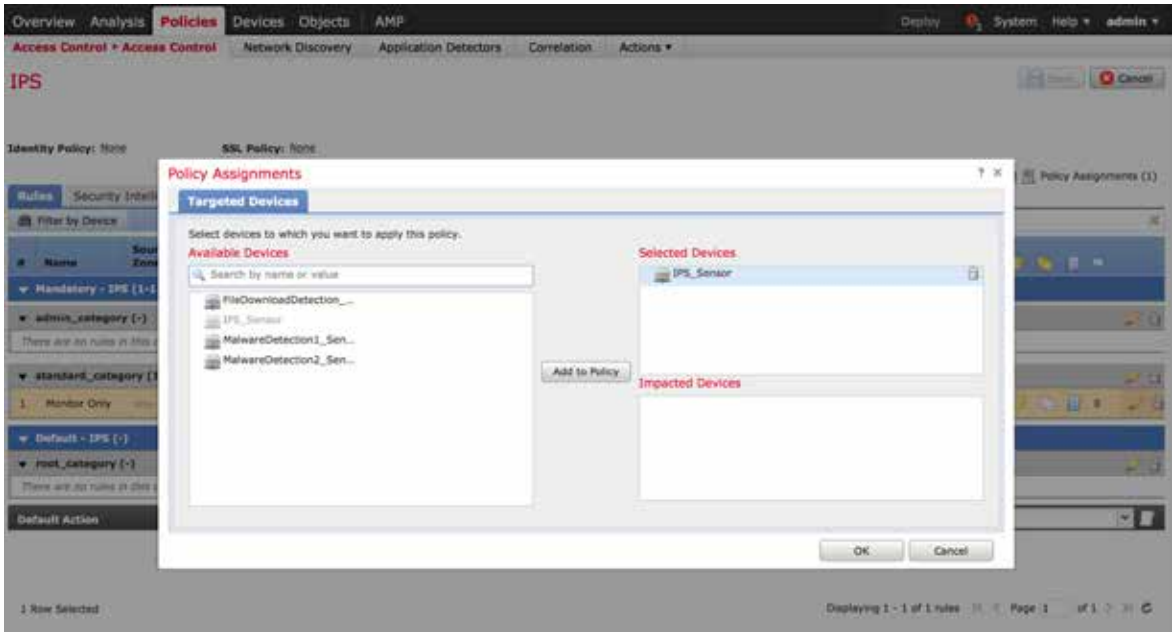
To assign IPS sensor level policy to global access control policy through Cisco FirePOWER Management Center, do the following:

1. Select **Policies > Access Control > Access Control > IPS > Edit > Inspection**.

2. Select the **Intrusion Policy** of interest. In the following example, the **Intrusion Policy** selected is **Tech-Day-IPS**.



3. Now assign it to targeted devices using the **Policy Assignments** link in the right hand side corner.

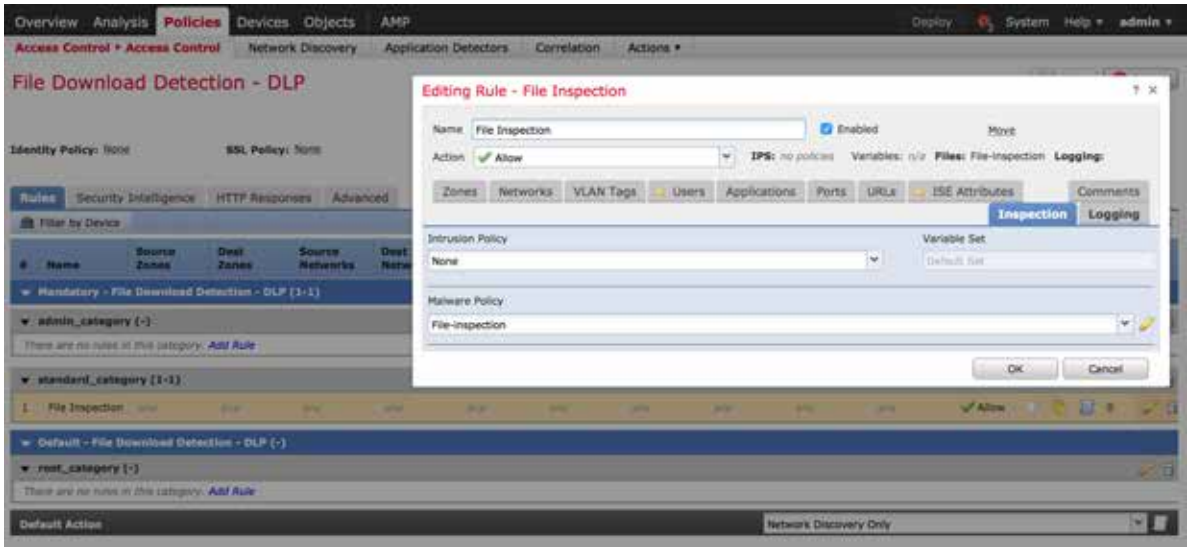


b) File Inspection Access Control policy

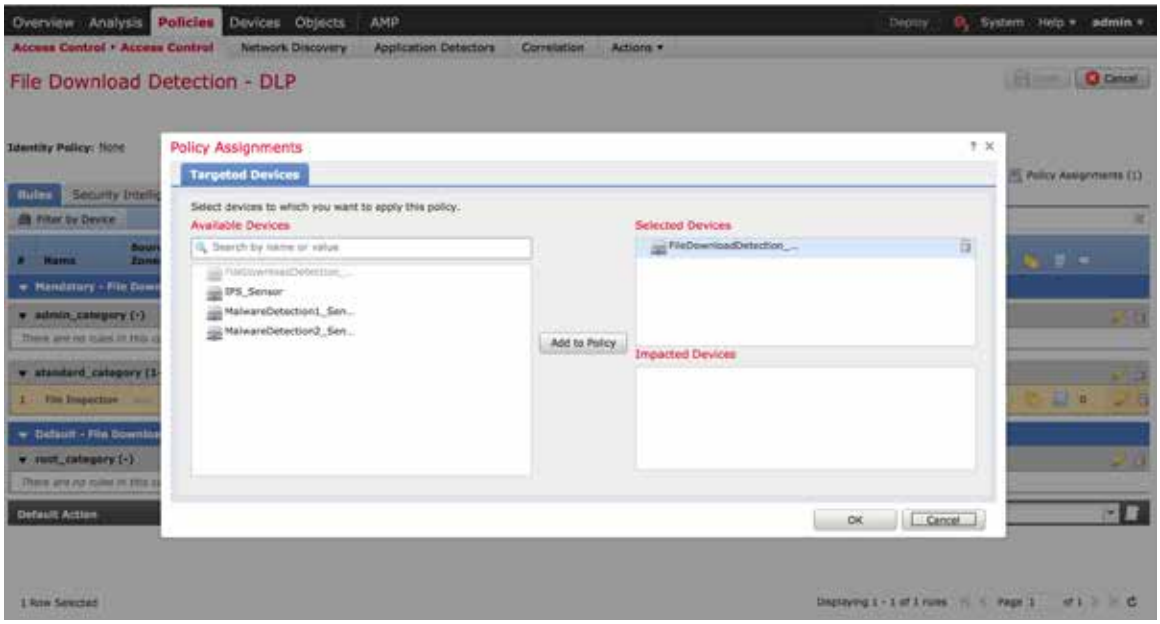
To assign File Inspection sensor level policy to global access control policy through Cisco FirePOWER Management Center, do the following:

1. Select **Policies > Access Control > Access Control > File Download Detection-DLP > Edit > Inspection**.

2. Select **Malware Policy as File-inspection**.



3. Now assign it to targeted devices using the **Policy Assignments** link in the right hand side corner.

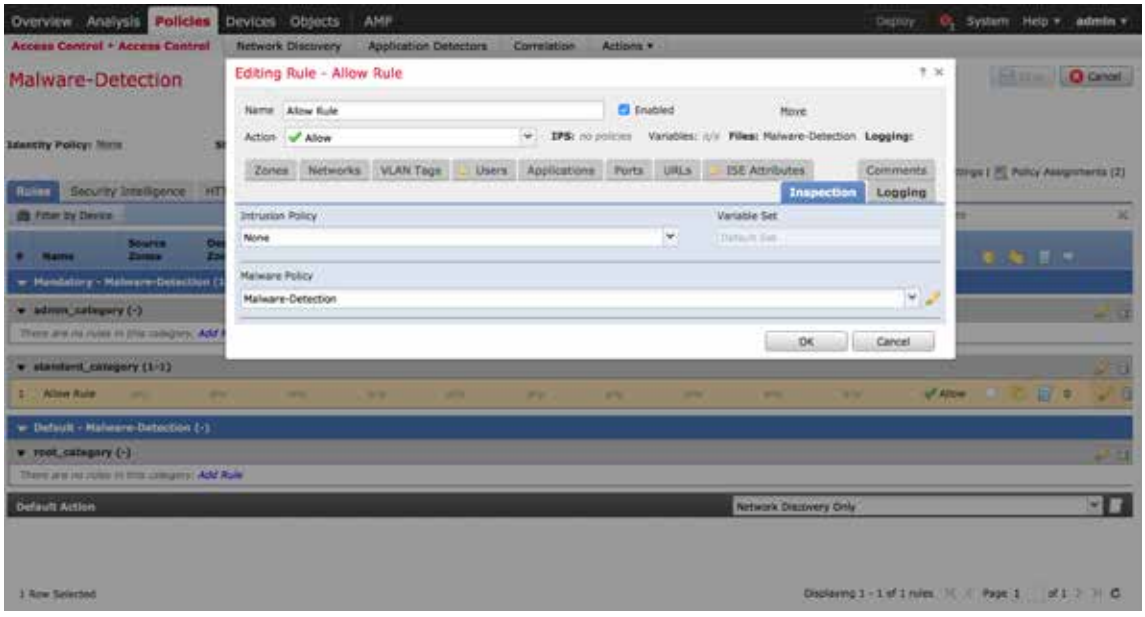


c) Malware Detection Access Control Policy

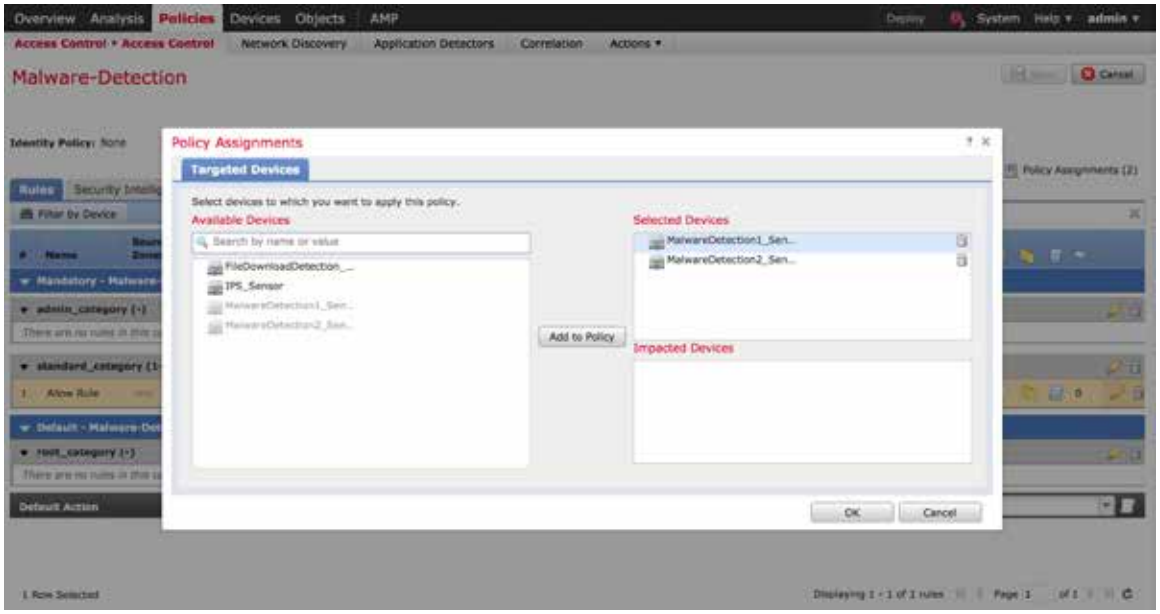
To assign Malware-Detection sensor level policy to global access control policy through Cisco FirePOWER Management Center, do the following:

1. Select **Policies > Access Control > Access Control > Malware-Detection > Edit > Inspection**.

2. Select **Malware Policy as Malware-Detection**.



3. Now assign it to targeted devices using the **Policy Assignments** link in the right hand side corner.



The completed Access control policy page should look similar to what is shown in the following figure.

Step7: Deploy Policies

Click **Deploy** in the upper right hand corner of the Cisco FirePOWER Management Center UI. Check the checkboxes for all devices, and expand the list to see the details.

GigaVUE-HC2 Configuration

This section explains the steps to configure the 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 GigaVUE-HC2 Inline Network and Inline Tools
- Configuring the Inline Traffic Flow Maps
- Testing the Functionality of Cisco FirePOWER Inline Tool

Configuring the GigaVUE-HC2 Inline Network and Inline Tools

This section walks you through the steps needed to configure inline network bypass pairs and an inline network group for those pairs. As the infrastructure grows, additional inline network pairs can be added to the inline network group. The basic steps are as follows:

- Step 1: Configure Network and Tool Ports
- Step 2: Configure the Inline Networks
- Step 3: Configure the Inline Tools
- Step 4: Configure the Inline Tool Group
- Step 5: Configure the Inline Serial Tool

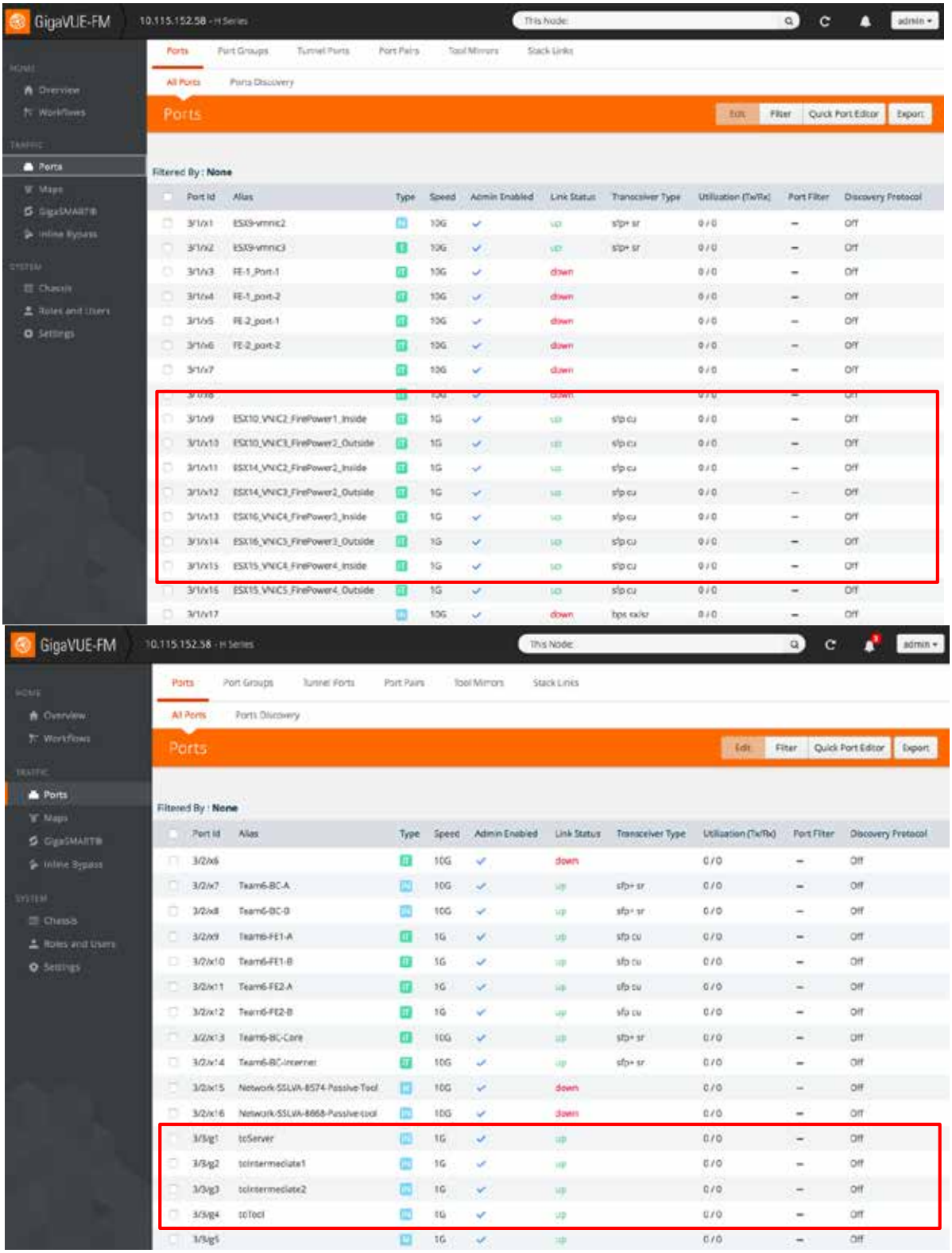
The steps described in this section assume that you are logged in to GigaVUE-FM. To configure the GigaVUE-HC2 of interest, select **Physical Nodes** in the left pane and then select GigaVUE-HC2 on the Physical Nodes page.

NOTE: This section assumes all GigaVUE-HC2 ports connected to network devices are set as Inline Network port type. For specific instructions on completing these tasks, refer to Help Topics links in the GigaVUE-FM or the *Gigamon-FM/VM User's Guide*.

Step 1: Configure Network and Tool Ports

To configure the Network and Tool Ports, do the following:

1. Log into GigaVUE-FM, select **Physical Nodes.**
2. Select the GigaVUE-HC2 from the list of physical nodes managed by GigaVUE-FM.
3. Select **Ports.**
4. Edit the ports of interest. Enable the port and select port type as "inline Tool" or "inline Network".



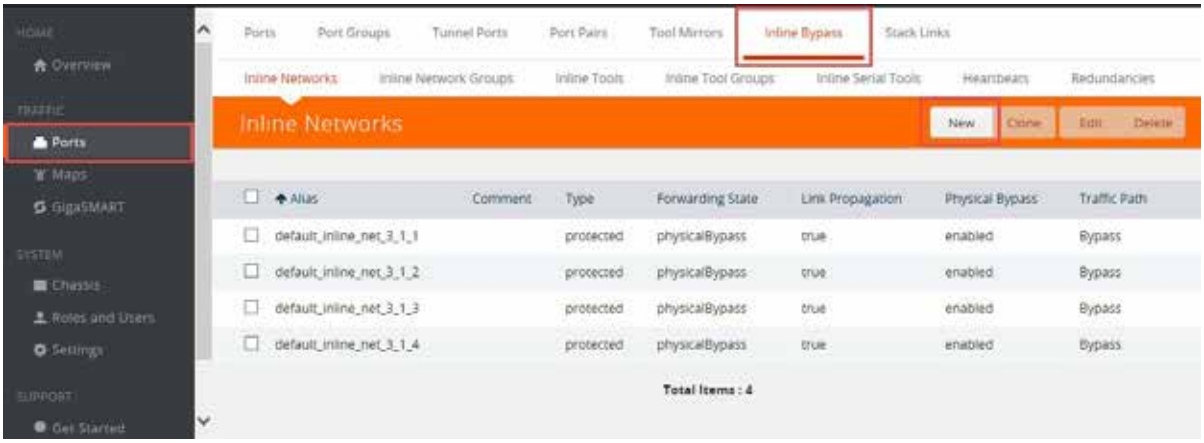
Note: The ports referred to as “intermediate1” and “intermediate2” are connected back-to-back. This is needed to support serial and parallel mode setting of tool in the same configuration. The goal is to have traffic from server side first sent to serial sensors (IPS and DLP) and then sent to the port “intermediate1”. From “intermediate1”, traffic would be looped back to port “intermediate2”, where it is sent to the parallel malware sensors and then to the client connected on the tool side. Refer Figure 1-1 and Figure 1-3.

Step 2: Configure the Inline Networks

To configure the inline networks, do the following:

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

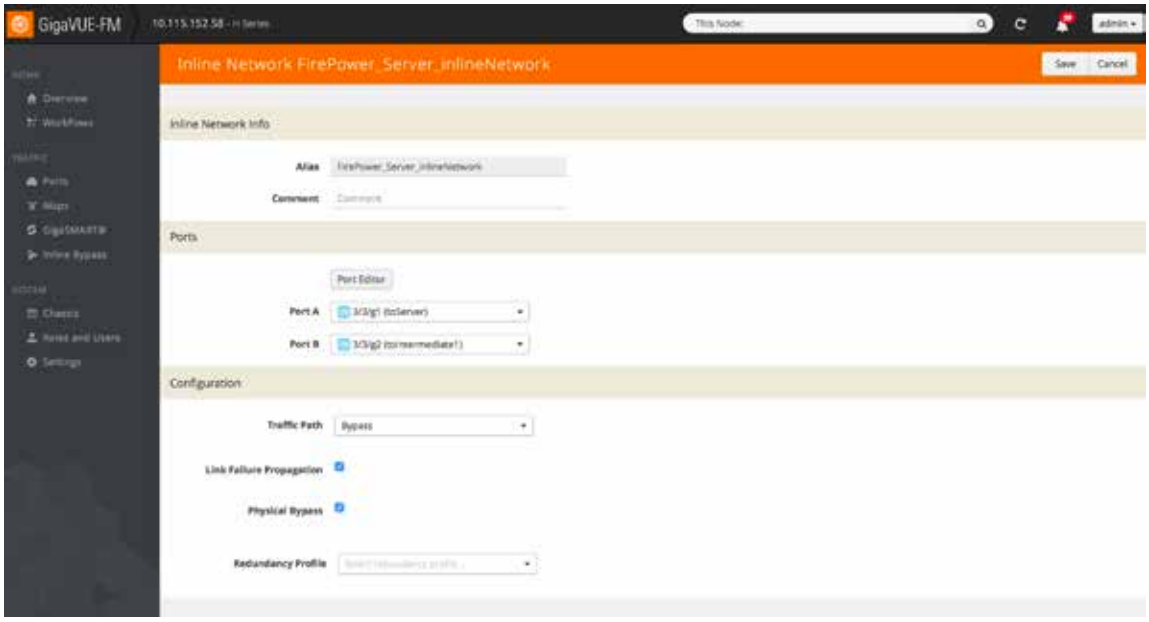
NOTE: If there is a bypass combo module in the GigaVUE-HC2, there will be four preconfigured Inline Network port pairs as shown below. If you are using the physical bypass interfaces, the step will be similar to those covered but limited. Notably you will not be able to change the alias and port A and B are preselected. If your network is 1G or 10G fiber, use one of these preconfigured inline bypass pairs. In this deployment guide, NGIPSv is used with 1 Gb Copper interfaces hence we would be using 1Gb Copper bypass modules for inline bypass testing.

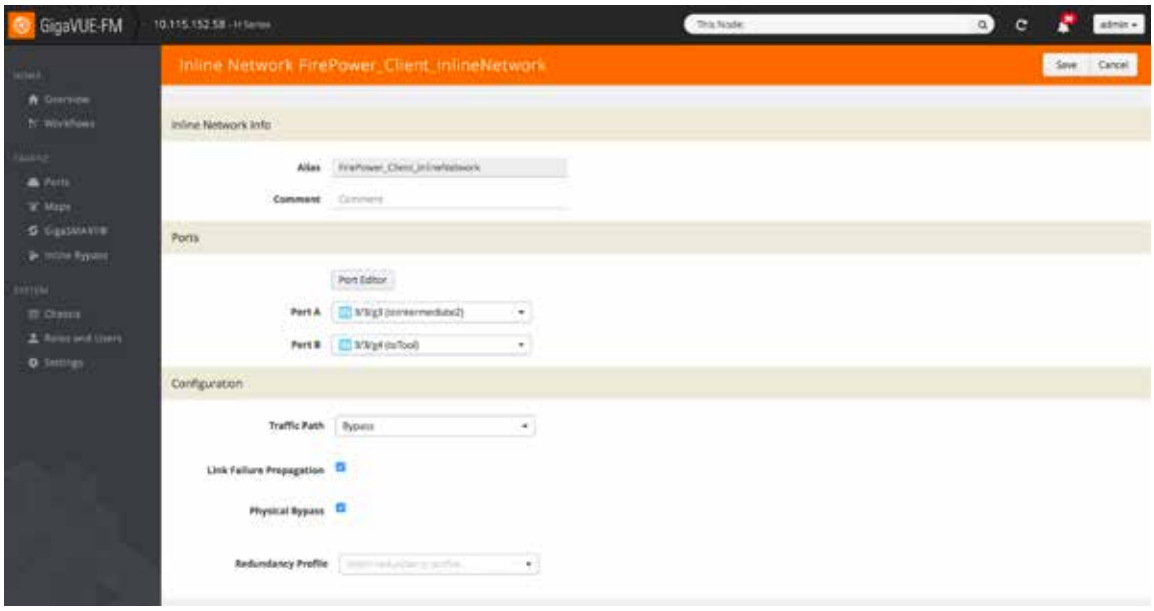


2. Click **New**. The Inline Network configuration page is displayed.
3. On the Inline Network page, do the following, and then click **Save** when you are done:
   a. In the **Alias** field, enter an alias for the network link this Inline Network bypass pair represents. For example, FirePower_Server_inlineNetwork and FirePower_Client_inlineNetwork
   b. Select the port for **Port A** by using the drop-down list or by typing the port label. The value in the **Port B** field is automatically populated once you select **Port A**.
   c. Retain default values for **Traffic Path** and **Link Failure Propagation**.
   d. Select **Physical Bypass**. This minimizes packet loss during traffic map changes.

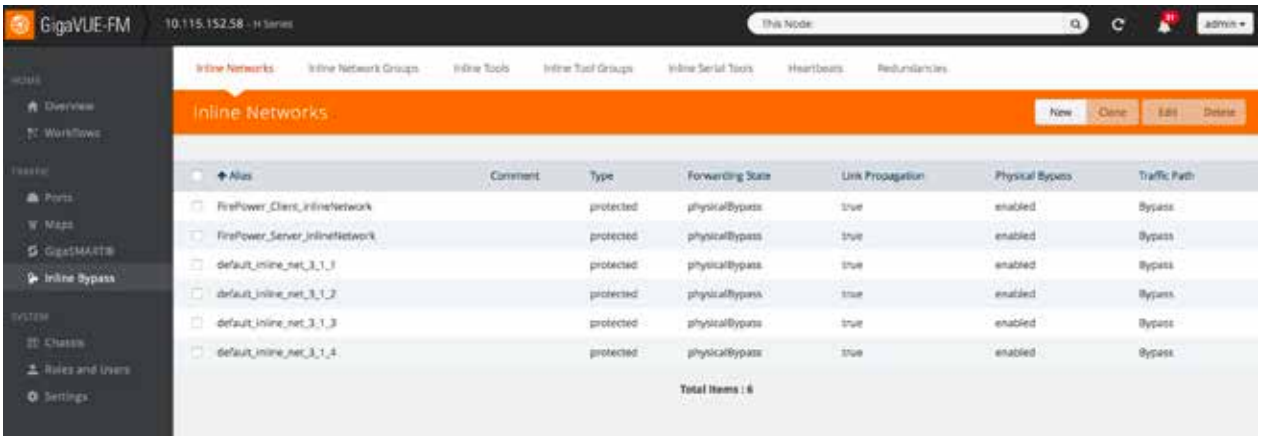
The configuration page should look similar to the example shown in the figure below.

NOTE: Traffic Path is set to Bypass to prevent packet loss until 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 a subsequent section.





The completed Inline Networks page should look similar to what is shown in the following figure.



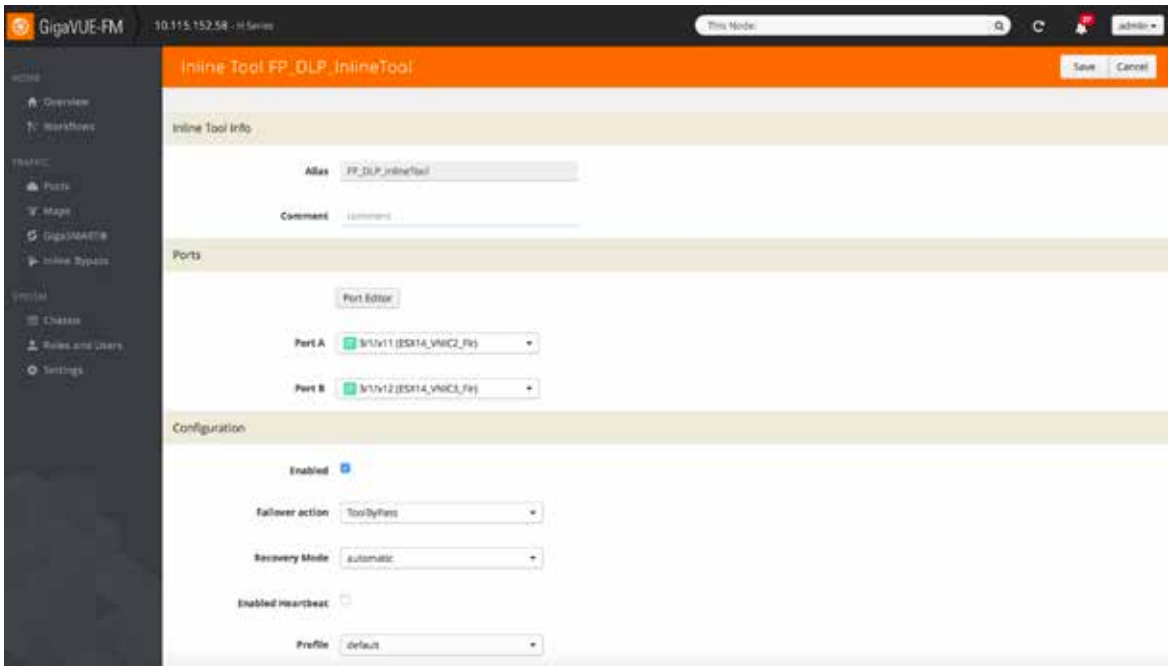
Step 3: Configure the Inline Tools

Steps 3 through 5 walk you through the configuration necessary to define the inline tools, inline tool groups and serial tools that will be used in the traffic flow map defined in subsequent steps.

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

2. Click **New** to open the configuration page for inline tools.
3. In the **Alias** field, enter an alias for the inline tool this inline tool pair represents. For example, `FP_DLP_InlineTool`.
4. In the Ports section, specify the ports as follows:
   - For **Port A**, specify the port that corresponds to the inside network of the sensors.
   - For **Port B**, specify the port that corresponds to the outside network of the sensors.
5. Leave the default setting for the remaining configuration options.

Your configuration should be similar to the example shown below.

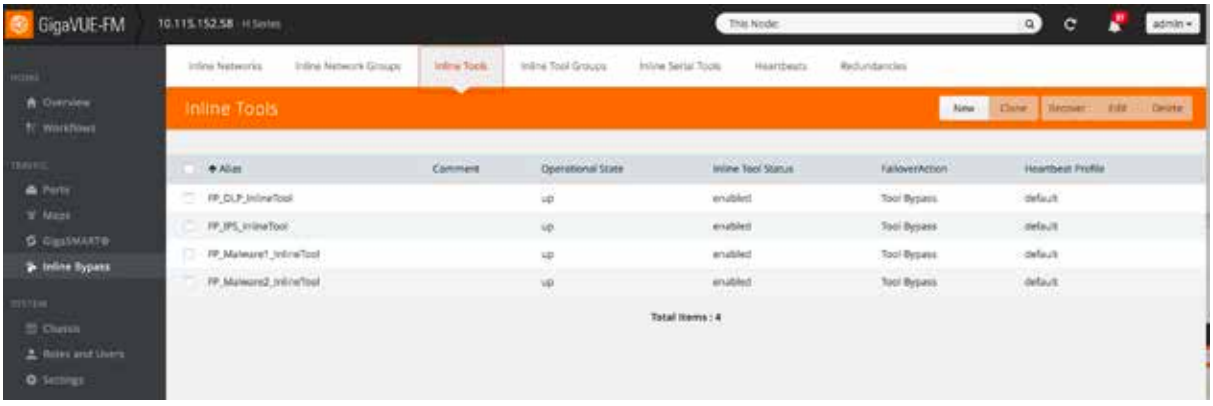


6. Click **Save**.

7. Repeat steps 2 through 6 for all additional inline tools.

NOTE: The failure action for this inline tool is **ToolBypass**. This means that the 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 and GigaVUE-OS Configuration Guide. The other options have very different effects on the overall traffic flow. Because the heartbeat feature is not enabled, the failover action will only take place if one of the tool port interfaces fails.

The completed Inline Tools page should look similar to what is shown below.

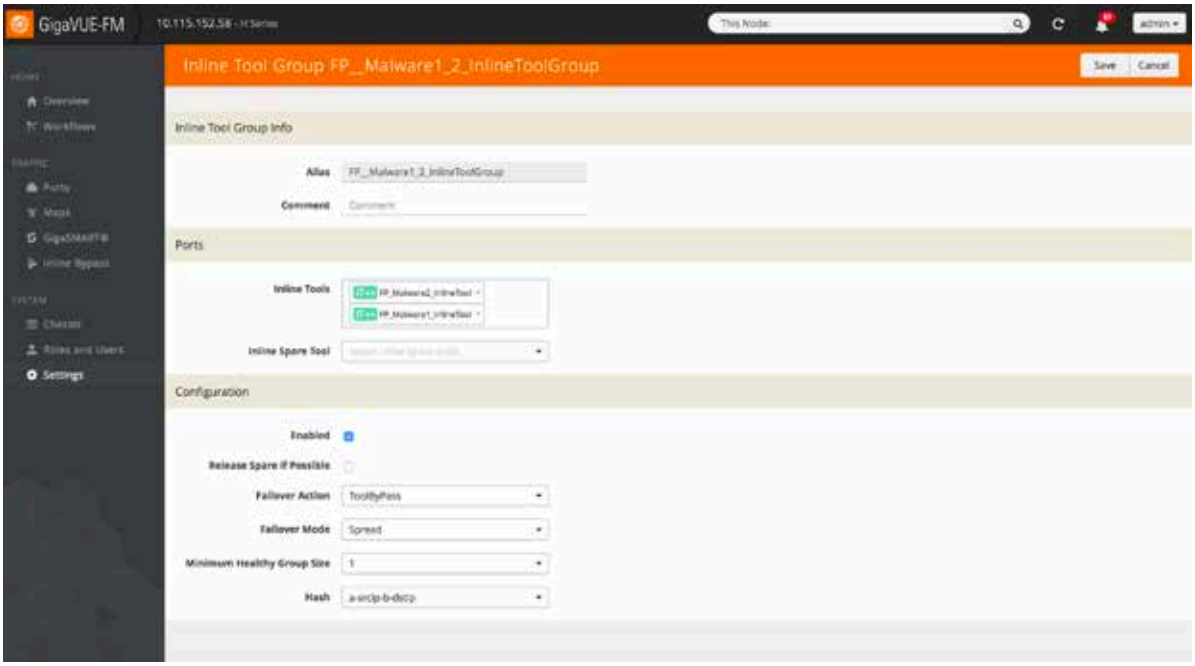


Step 4: Configure the Inline Tool Group

To configure the inline tool group, do the following:

1. In GigaVUE-FM, select **Inline Bypass > Inline Tool Groups**.
2. Click **New** to open the Inline Tool Groups configuration page.
3. In the **Alias** field, type an alias that describes the inline tool groups. For example, `FP_Malware1_2_InlineToolGroup`.
4. In the Ports section, click the **Inline tools** field and select all the inline tools for this group from the l
5. ist of available inline tools.
6. In the Configuration section, do the following, and then click **Save** when you are done:
   - Select **Enable**.
   - Select **Release Spare If Possible** if applicable.
   - Keep the defaults for **Failover action**, **Failover Mode**, and **Minimum Healthy Group Size**.
   - Select a-srcip-b-dstip for **Hash**.

The configuration should look similar to the example shown below:



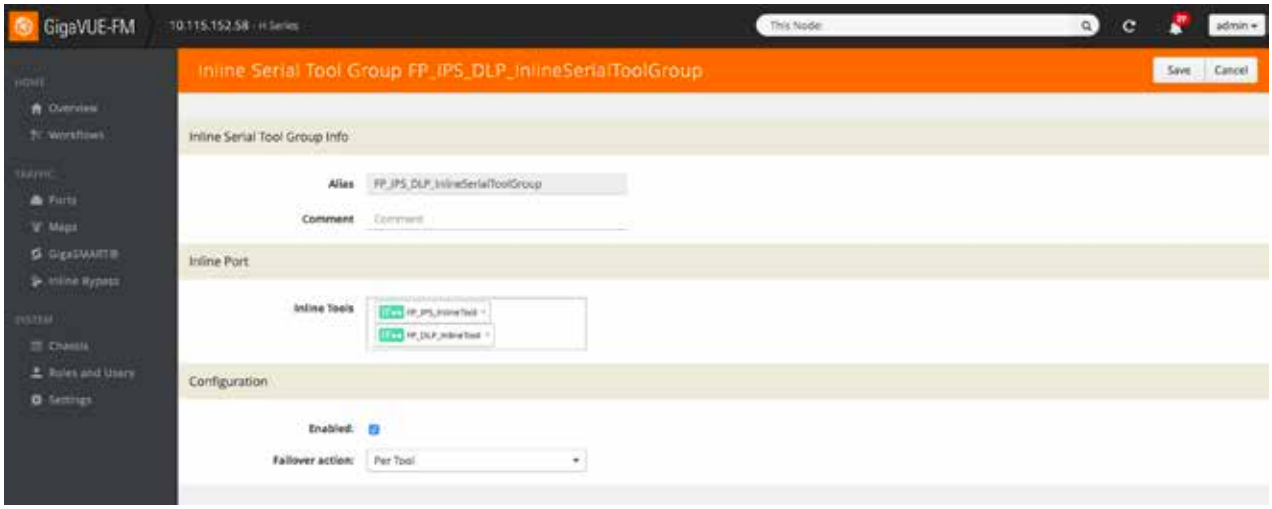
Step 5: Configure the Inline Serial Tools

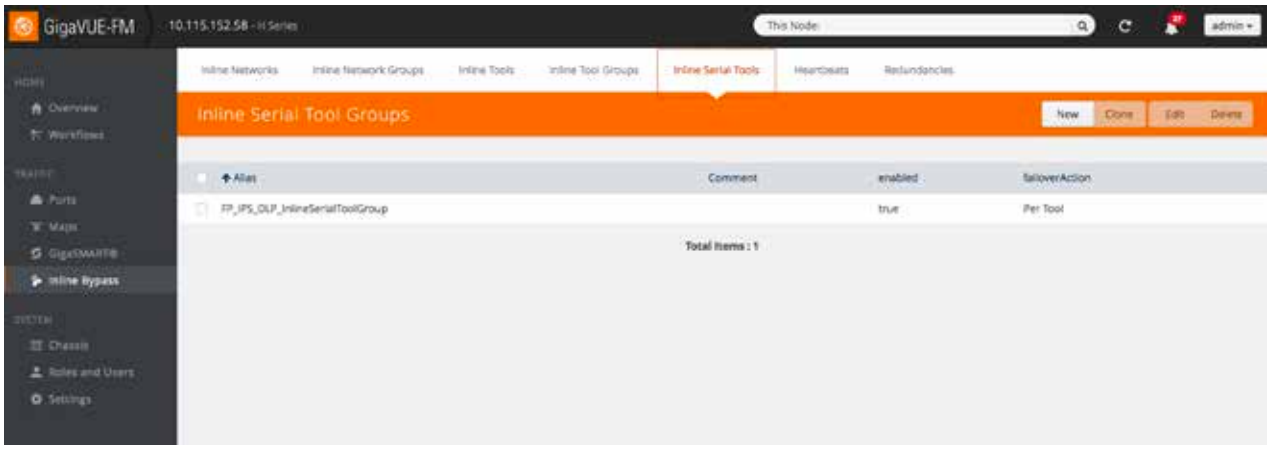
To configure the inline serial tool group, do the following:

1. In GigaVUE-FM, select **Inline Bypass > Inline Serial Tools**.
2. Click **New** to open the Inline Serial Tool Groups configuration page.
3. In the **Alias** field, type an alias that describes the inline tool groups. For example:

   `FP_IPS_DLP_InlineSerialToolGroup`.
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 serial tools.
5. In the Configuration section, do the following, and then click **Save** when you are done:
   - Select **Enable**.
   - Select **Failover action** as **Per Tool**

The configuration should look similar to the example shown below:





Configuring the Inline Traffic Flow Maps

This section describes the high level process for configuring traffic to flow from the inline network links to the inline FirePOWER tool group allowing you to test the deployment functionality of the FirePOWER virtual sensors within the group. This will be done in three steps as follows:

- Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule
- Step 2: Configure the Inline Traffic Collector Map
- Step 3: Change Inline Network Traffic Path to Inline Tool

After completing these steps, you will be ready to test the deployment of the FirePOWER sensors. The test procedure is described in *Testing the Functionality of the FirePOWER Inline Tool* .

Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule

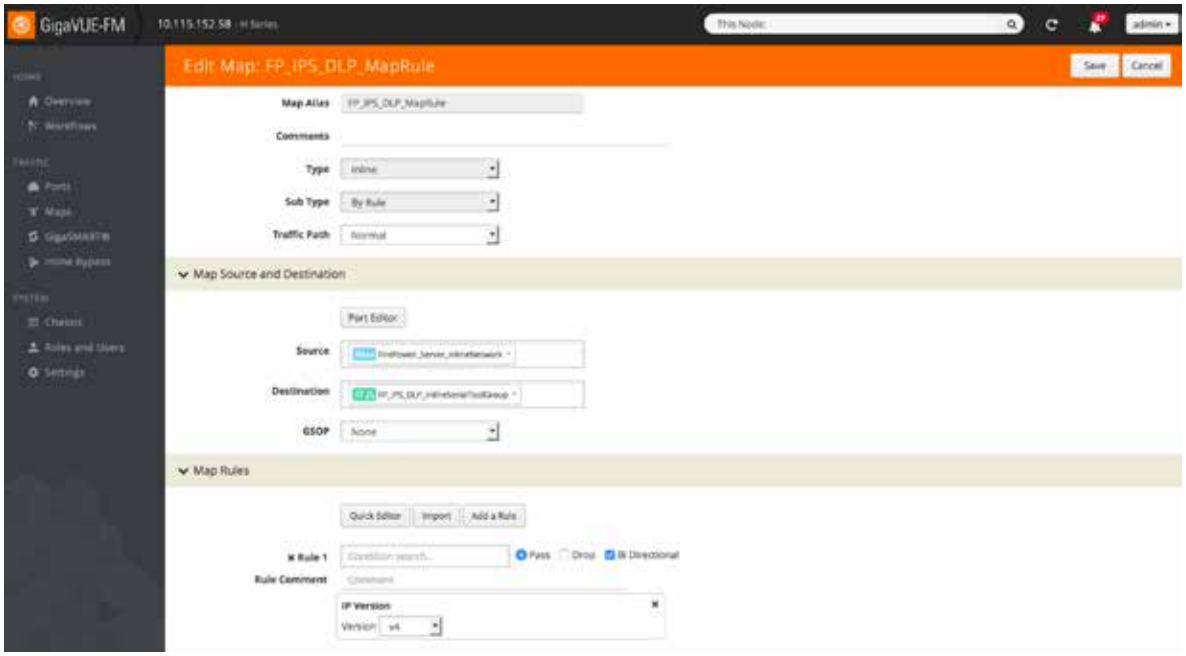
This section walks through the configuration of traffic flow map between the Inline Network Group and the Inline Tool Group.

1. In GigaVUE-FM, go to the **Maps** page.
2. Click **New.** The New Map page displays.
3. In the Map Info section, do the following:
   - In the **Alias** field, enter a map alias that represents the network source and tool destination.
   - Set **Type** to Inline.
   - Set **Sub Type** to By Rule.
   - Set **Traffic Path** to Normal.
4. In Map Source and Destination, set the **Source** and **Destination** as follows:
   - Set Source to the inline network group that you created in *Step 2: Configure the Inline Network Group* of the previous section.
   - Set Destination to the inline tool group and inline serial groups that you created in *Step 4: Configure the Inline Tool Group* and *Step 5: Configure the Inline Serial Tools Group*, respectively, in the previous section.
5. In Map Rules, click **Add a Rule**.
6. Specify the following for the rule:
   - Click in the Condition search field for the Rule and select **IP Version v4** from the drop-down list.
   - Select **Pass**. (This is the default.)
   - Select **Bi Directional**.

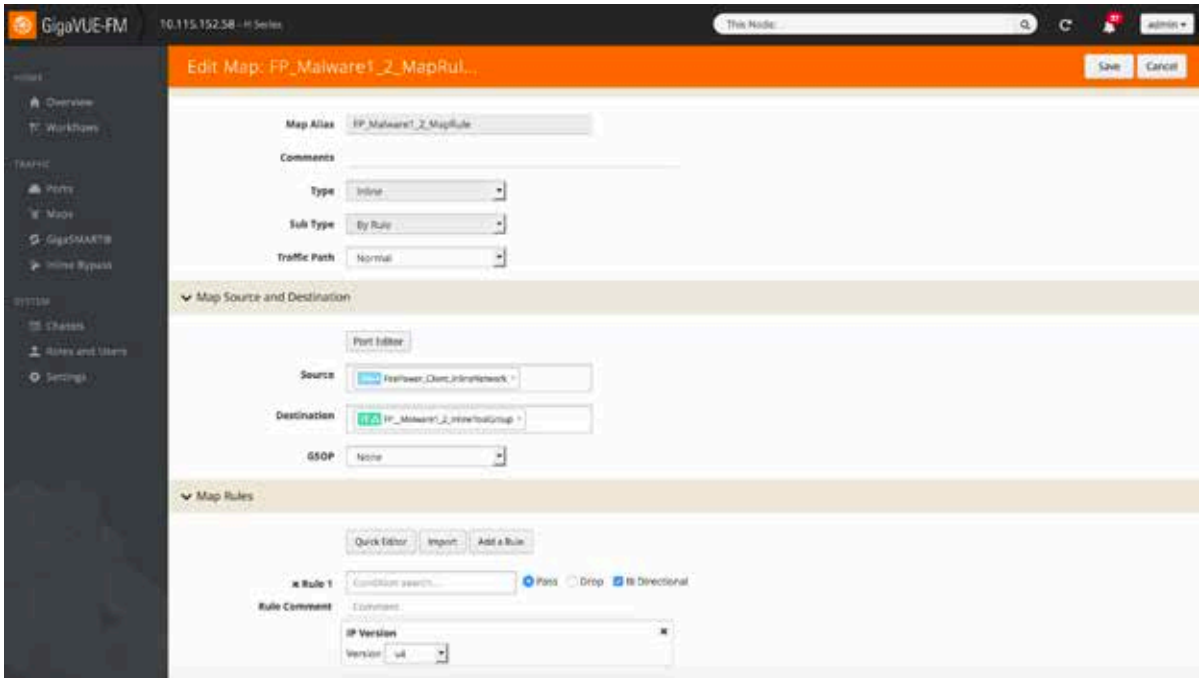
- Add a rule to pass all IPv4 traffic.

The map rule should look like the rule shown in the following figures:

Inline flow map for Server to IPS_DLP inline tool group:



Inline flow map for Malware inline tool group to Client:



NOTE: Additional traffic can be bypassed by adding rules to the map.

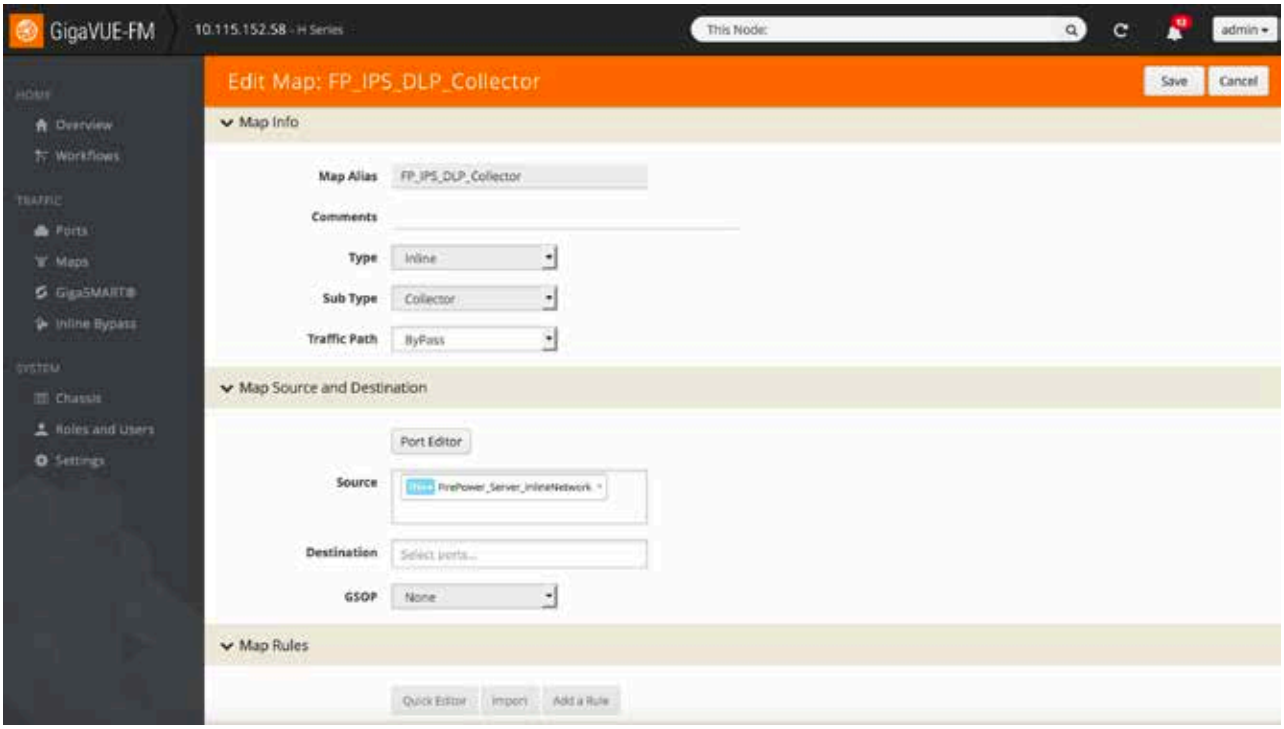
7. Click **Save**.

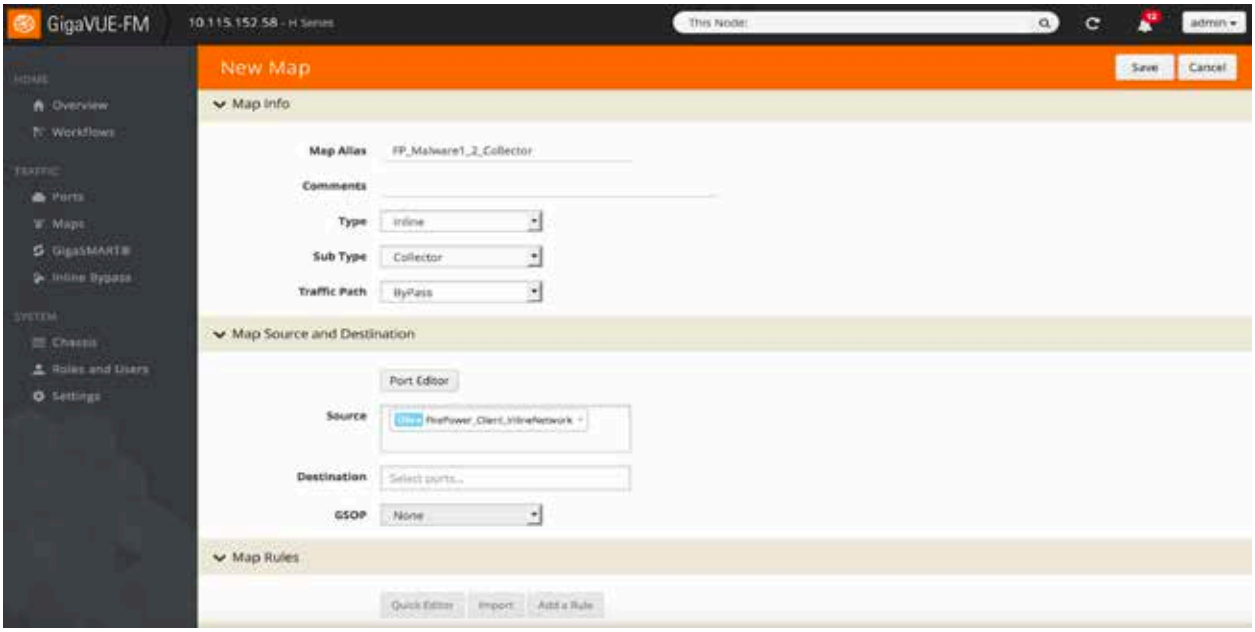
Step 2: Configure the Inline Traffic Collector Map

This section walks you through the steps to create another traffic map, which is a collector. This map sends all the traffic not matched in the first traffic flow map to the inline tool group. This Collector pass rule must be created because there is no implicit pass for traffic, meaning all inline traffic from any given inline network not matched by a pass rule is discarded.

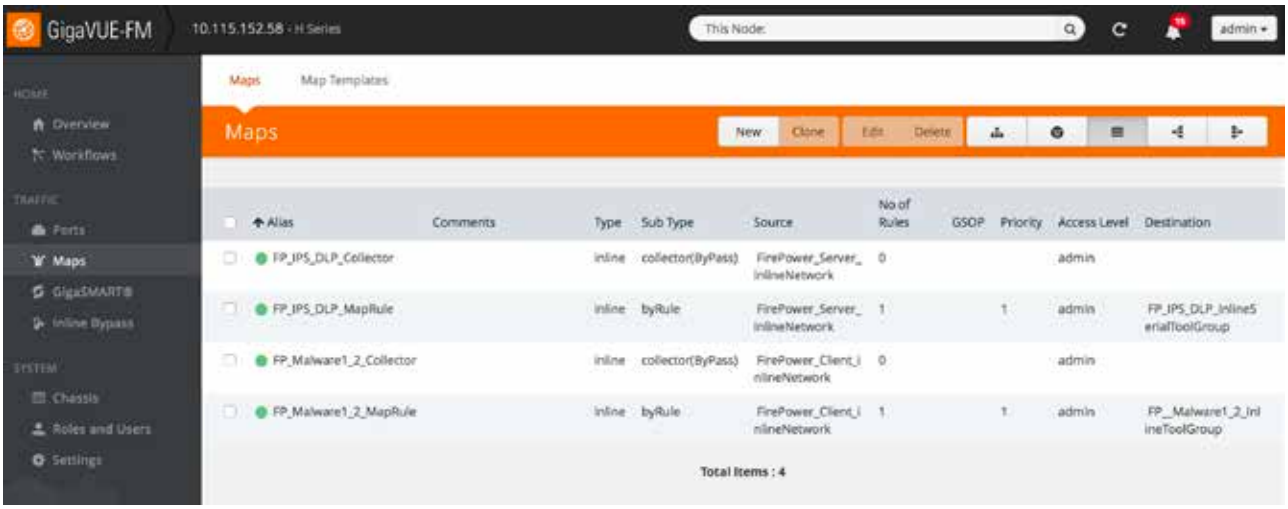
To configure the collector map, do the following:

1. In GigaVUE-FM, navigate to **Maps** page, and then click **New.** The New Map page displays.
2. In the Map Info section, do the following:
   - In the **Alias** field, type a map alias that identifies that this collector map is for the same inline network as the traffic map you created in *Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule*.
   - Set **Type** to Inline.
   - Set **Sub Type** to Collector.
   - Set **Traffic Path** to ByPass.
3. In Map Source and Destination, set the **Source** to the same source as the first rule map configured in *Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule*.





The finished screen for maps should look as shown in the following figure.

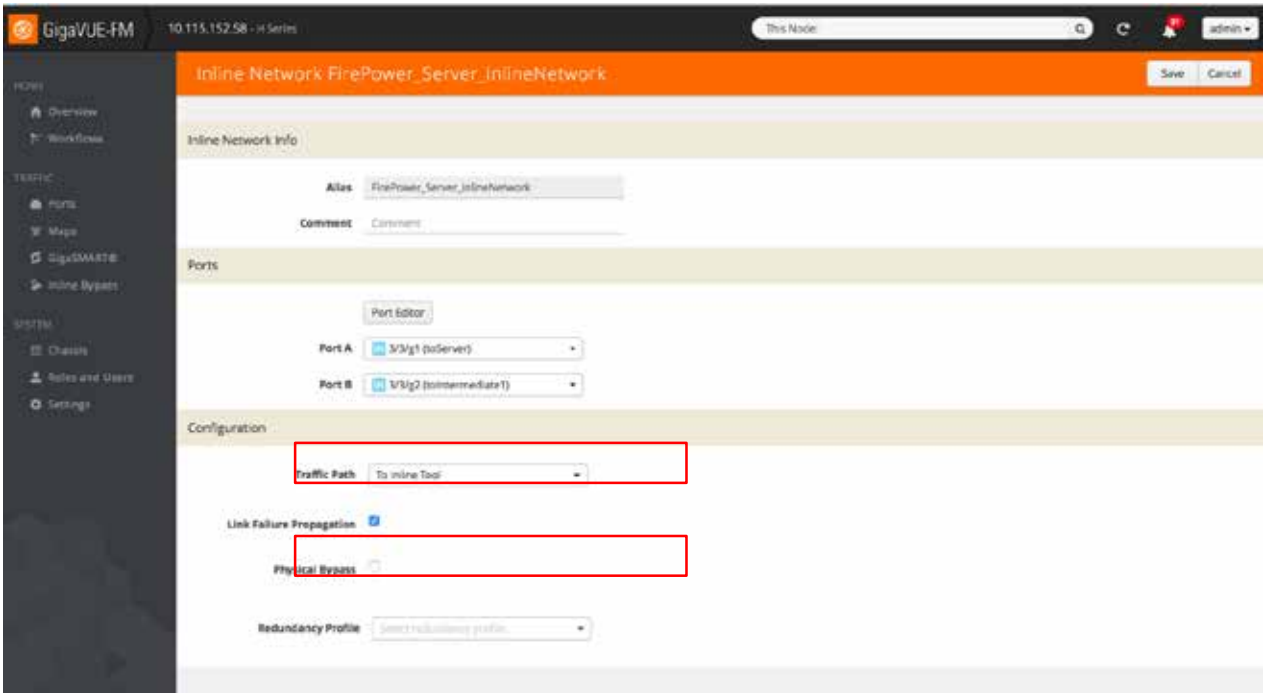


Step 3: Change Inline Network Traffic Path to Inline Tool

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 Tool, make sure that the inline tool ports are up. You can check the status of the ports by going to the Chassis View page in GigaVUE-FM by selecting **Chassis** from the main navigation pane.

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

1. In GigaVUE-FM, select Ports > Inline Bypass > Inline Networks.
2. Select one of the inline networks that you defined previously (refer to *Step 2: Configure the Inline Network Group*), and then click **Edit**.
3. In the Configuration section, make the following changes:
   - Set **Traffic Path** to Inline Tool.
   - Uncheck **Physical Bypass**.



4. Click **Save**.
5. Repeat step 3 and step 4 for each inline network in the inline network group.

Testing the Functionality of the FirePOWER Inline Tool

The configuration procedure described in the previous section configures the GigaVUE-HC2 to send live traffic to all FirePOWER NGIPSv sensors. While testing the functionality of the sensors, it may be helpful to monitor the port statistics on the GigaVUE-HC2. To access the port statistics for the inline network and inline tool ports, do the following:

1. Get the statistics for the inline network and the inline tool ports from the GigaVUE-HC2.

2. Launch a serial console or SSH session to the GigaVUE-HC2.

3. Log in as admin and enter the following commands at the command prompt (HC2>), where the port lists in the command are the inline network and inline tool ports:

   HC2 > en
   HC2 # config t
   HC2 (config) # clear port stats port-list 3/1/x9..x16,3/3/g1..g4
   HC2 (config) # show port stats port-list 3/1/x9..x16,3/3/g1..g4

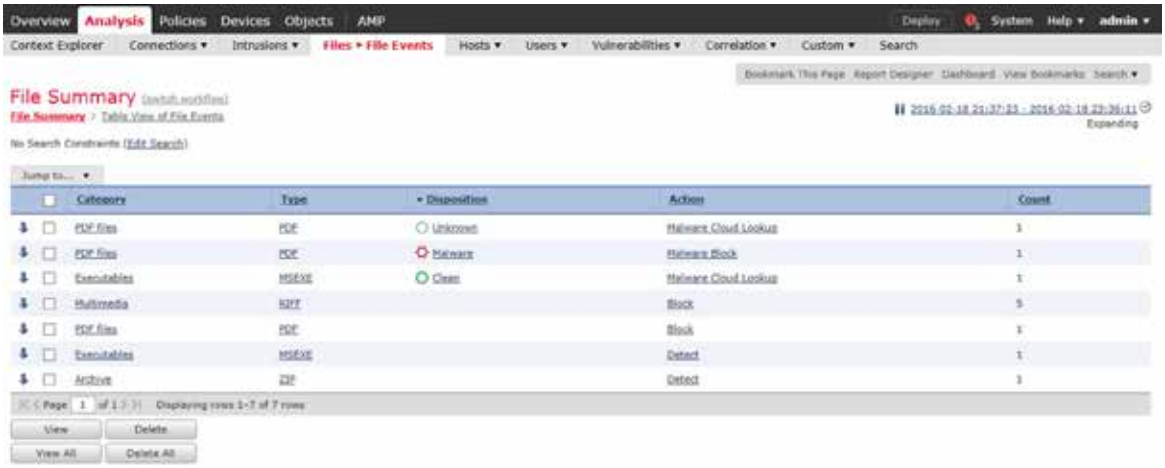
After entering the show port command, you should see the port statistics for the specified port list.

Inline Network and Inline Tool Port Statistics:

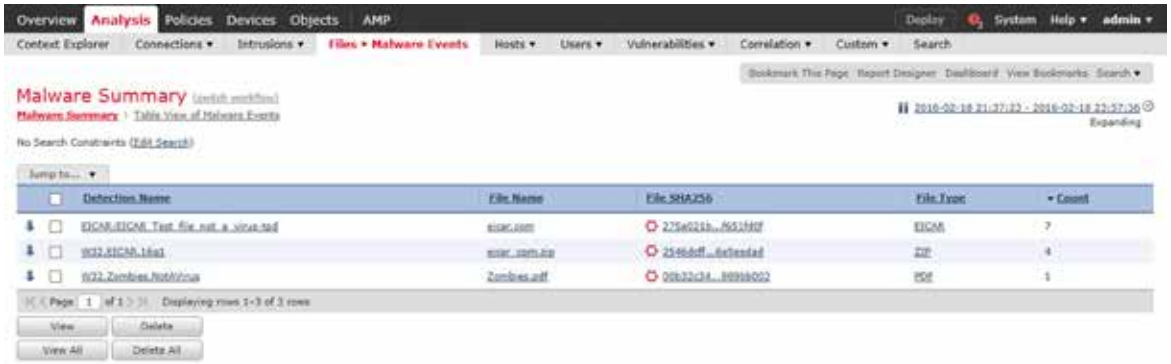
```
HC2-C04-31 (config) # show port stats port-list 3/1/x9..x14,3/3/g1..g4

       Counter Name     Port: 3/1/x9    Port: 3/1/x10    Port: 3/1/x11    Port: 3/1/x12
 ================== ================ ================ ================ ================
         IfInOctets:            38370           446877            38370           443841
       IfInUcastPkts:              216              365              216              364
      IfInNUcastPkts:               46              379               46              378
        IfInPktDrops:                0                0                0                0
        IfInDiscards:                0                0                0                0
          IfInErrors:                0                0                0                0
    IfInOctetsPerSec:               83              472               83              472
  IfInPacketsPerSec:                 1                7                1                7
        IfOutOctets:           446941           38370           446813           38626
      IfOutUcastPkts:              365              216              365              220
     IfOutNUcastPkts:              380               46              378               46
       IfOutDiscards:                0                0                0                0
         IfOutErrors:                0                0                0                0
   IfOutOctetsPerSec:              472               83              472               83
 IfOutPacketsPerSec:                 7                1                7                1


       Counter Name     Port: 3/1/x13    Port: 3/1/x14    Port: 3/3/g1     Port: 3/3/g2
 ================== ================ ================ ================ ================
         IfInOctets:            13362           416360           445575           38056
       IfInUcastPkts:              140              291              363              218
      IfInNUcastPkts:                1              238              367               45
        IfInPktDrops:                0                0                0                0
        IfInDiscards:                0                0                0                0
          IfInErrors:                0                0                0                0
    IfInOctetsPerSec:                0              229              472               83
  IfInPacketsPerSec:                 0                4                7                1
        IfOutOctets:           416360           13362           37800           442539
      IfOutUcastPkts:              291              140              214              362
     IfOutNUcastPkts:              238                1               45              366
       IfOutDiscards:                0                0                0                0
         IfOutErrors:                0                0                0                0
   IfOutOctetsPerSec:              229                0               83              472
 IfOutPacketsPerSec:                 4                0                1                7


       Counter Name     Port: 3/3/g3     Port: 3/3/g4
 ================== ================ ================
         IfInOctets:           442539            38056
       IfInUcastPkts:              362              218
      IfInNUcastPkts:              366               45
        IfInPktDrops:                0                0
        IfInDiscards:                0                0
          IfInErrors:                0                0
    IfInOctetsPerSec:              472               83
  IfInPacketsPerSec:                 7                1
        IfOutOctets:            38056           442475
      IfOutUcastPkts:              218              362
     IfOutNUcastPkts:               45              365
       IfOutDiscards:                0                0
         IfOutErrors:                0                0
   IfOutOctetsPerSec:               83              472
 IfOutPacketsPerSec:                 1                7

HC2-C04-31 (config) #
```

IPS Test Results

DLP test results



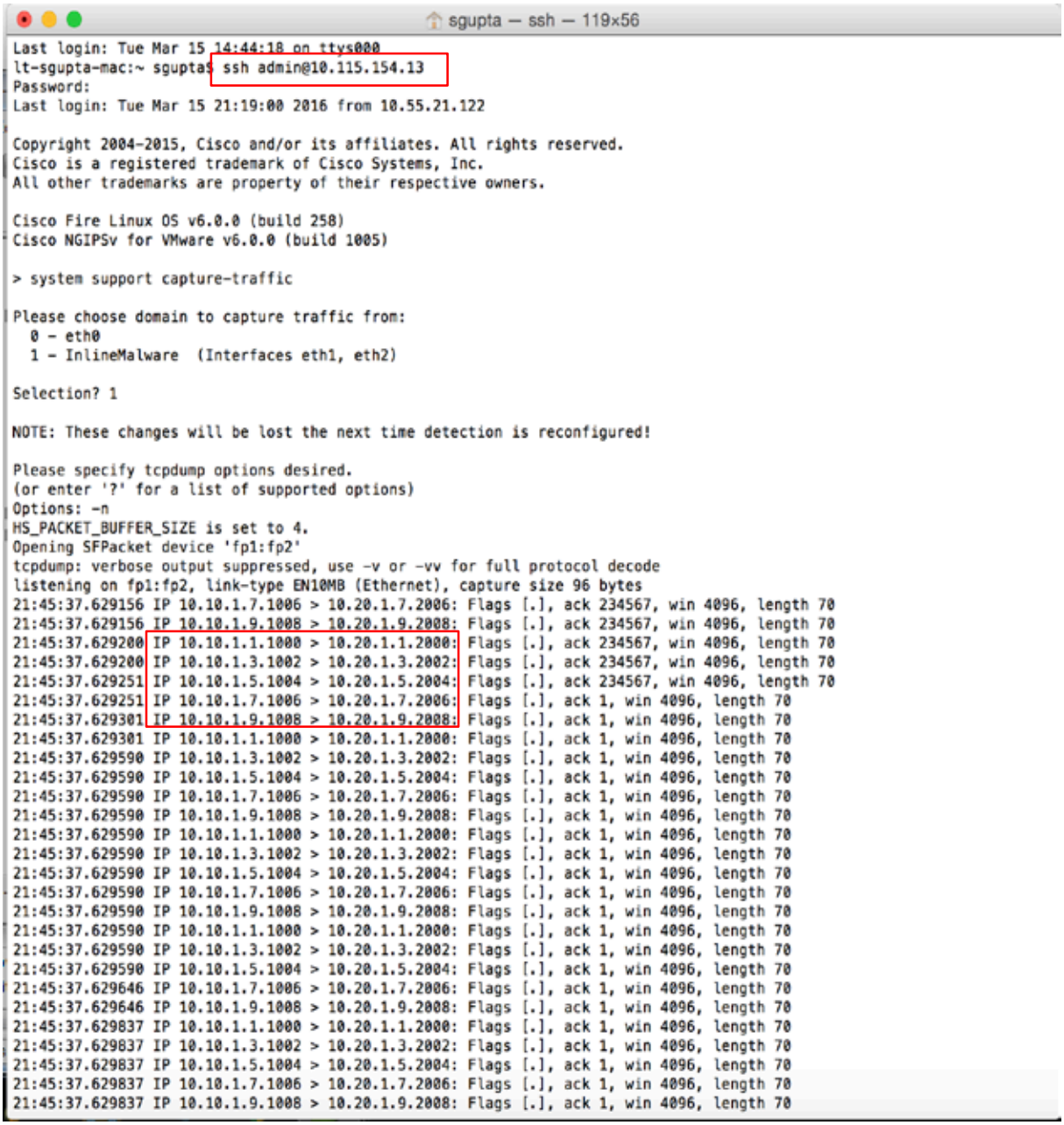
Malware test results



Load Balancing between Malware Sensors:

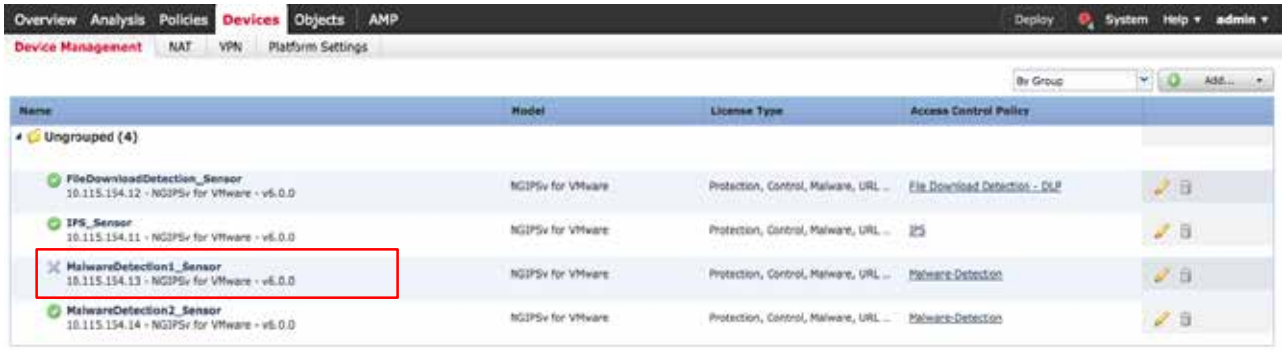
The hashing done with *a-srcip-b-dstip* configured as part of Step 4 under *"Configuring the GigaVUE-HC2 Inline Network and Inline Tools"* ensures all packets in a given TCP/UDP session go to the same malware group member. It also ensures that if any member of the group goes offline for any reason, the traffic will be distributed amongst the remaining members, thereby ensuring availability of the security functions provided by Cisco FirePOWER. For this test, ten unique IP streams are sent through Inline network port using Spirent test center.

Traffic across Malware sensor 1:



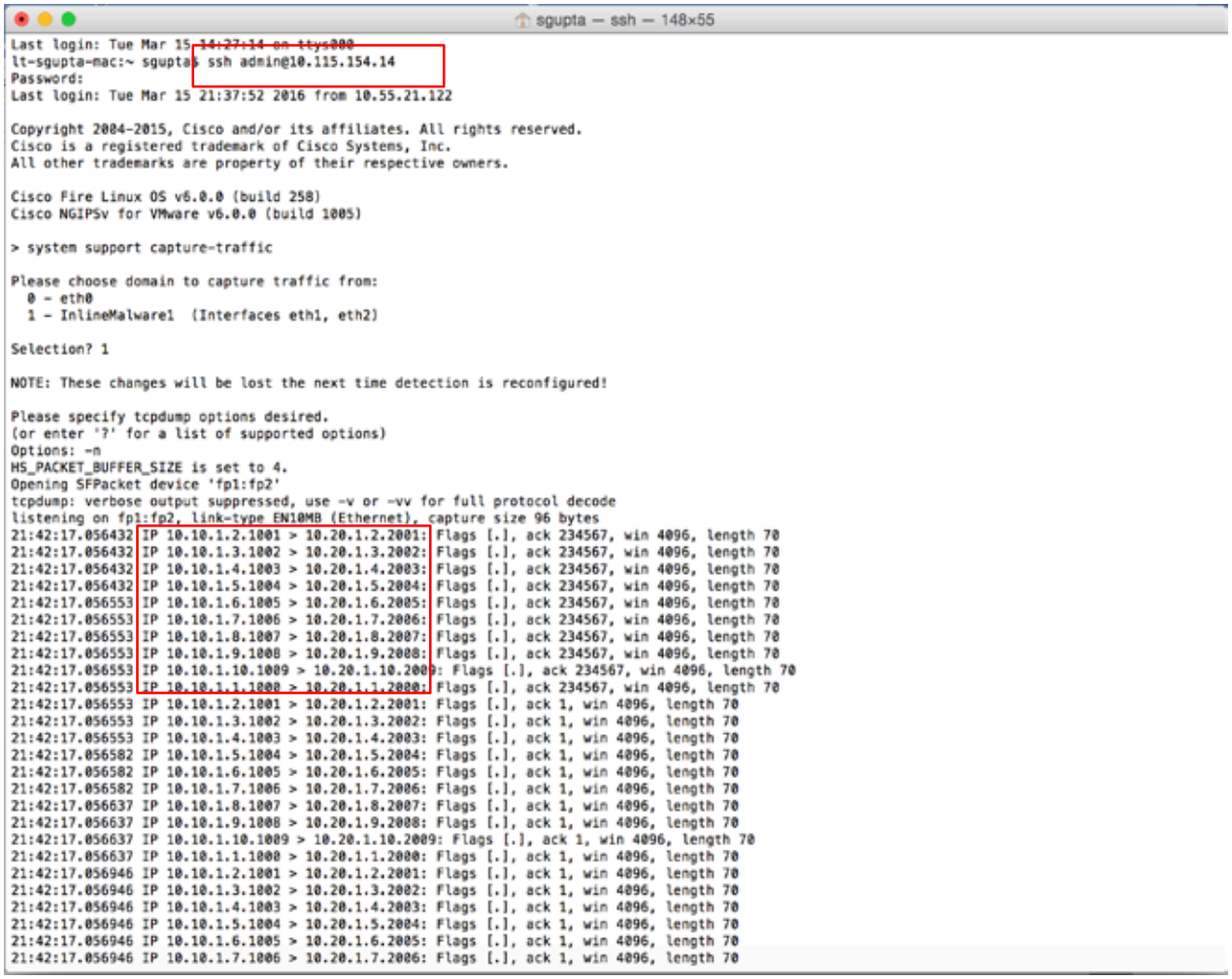
Traffic across Malware sensor 2:

```
sgupta — ssh — 125×56
Last login: Tue Mar 15 14:45:12 on ttys000
lt-sgupta-mac:~ sgupta$ ssh admin@10.115.154.14
Password:
Last login: Tue Mar 15 21:44:34 2016 from 10.55.21.122

Copyright 2004-2015, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.0.0 (build 258)
Cisco NGIPSv for VMware v6.0.0 (build 1005)

> system support capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - InlineMalware1  (Interfaces eth1, eth2)

Selection? 1

NOTE: These changes will be lost the next time detection is reconfigured!

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n
HS_PACKET_BUFFER_SIZE is set to 4.
Opening SFPacket device 'fp1:fp2'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on fp1:fp2, link-type EN10MB (Ethernet), capture size 96 bytes
21:47:02.168580 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], ack 234567, win 4096, length 70
21:47:02.168580 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], ack 234567, win 4096, length 70
21:47:02.168580 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], ack 234567, win 4096, length 70
21:47:02.168580 IP 10.10.1.10.1009 > 10.20.1.10.2009: Flags [.], ack 234567, win 4096, length 70
21:47:02.168580 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], ack 234567, win 4096, length 70
21:47:02.168580 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], ack 1, win 4096, length 70
21:47:02.168580 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], ack 1, win 4096, length 70
21:47:02.168580 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], ack 1, win 4096, length 70
21:47:02.168580 IP 10.10.1.10.1009 > 10.20.1.10.2009: Flags [.], ack 1, win 4096, length 70
21:47:02.168580 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], ack 1, win 4096, length 70
21:47:02.168638 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], ack 1, win 4096, length 70
21:47:02.168638 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.10.1009 > 10.20.1.10.2009: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.10.1009 > 10.20.1.10.2009: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], ack 1, win 4096, length 70
21:47:02.168892 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], ack 1, win 4096, length 70
21:47:02.168944 IP 10.10.1.8.1007 > 10.20.1.8.2007: Flags [.], ack 1, win 4096, length 70
21:47:02.168944 IP 10.10.1.10.1009 > 10.20.1.10.2009: Flags [.], ack 1, win 4096, length 70
21:47:02.169143 IP 10.10.1.2.1001 > 10.20.1.2.2001: Flags [.], ack 1, win 4096, length 70
21:47:02.169143 IP 10.10.1.4.1003 > 10.20.1.4.2003: Flags [.], ack 1, win 4096, length 70
21:47:02.169143 IP 10.10.1.6.1005 > 10.20.1.6.2005: Flags [.], ack 1, win 4096, length 70
```



Malware sensor 1 goes down:

Traffic re-distributed to Malware sensor 2:



3 Summary and Conclusions

The previous chapters showed how to deploy Gigamon GgiaVUE-HC2 bypass protection with Cisco FirePOWER network security sensor. This combined solution using the Gigamon-GigaVUE-HC2 chassis for inline tool high availability and traffic distribution achieves the following objectives:

- High availability of FirePOWER NGIPSv Platform because each inline security solution can be put into a Gigamon inline tool group with tool failover actions. The inline tool group can be optimized for each security need, regardless of whether the tool goes off-line due to an outage or planned maintenance.

- Seamless scalability for an increasing network infrastructure as well as the inline security tools to accommodate the additional traffic.

- Ultimate flexibility of adding new types of inline security tools without physical change control because all new tools are physically added to the GigaVUE-HC2 and logically added to the path through traffic flow maps.

For more information on the GigaVUE-HC2 bypass protection, high availability, and scalability provided by Gigamon's Security Delivery Platform, go to *www.gigamon.com.*

How to get Help

For issues with Gigamon products, please refer to http://www.gigamon.com/support-and-services/contact-support and your Support Agreement with Gigamon. You can also email Technical Support at support@gigamon.com.

For issues related to FirePOWER products, please refer to your Support Agreement with Cisco and follow the directions on how to open a Support Case.

See Inside Your Network™

4061-01 04 / 16