TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Gigamon

Contents

Partner Information

Partner information	
Date	June 28th, 2019
Partner Name	Gigamon
Web Site	https://www.gigamon.com
Product Name	Gigamon GigaVUE-HC2
Partner Contact	Phil Griston – Sr. Director – Strategic Alliances phil.griston@gigamon.com – 408-831-4148 Email: ecopartners@gigamon.com
Support Contact	Gigamon Support – 855-430-0813 – support@gigamon.com - https://www.gigamon.com/support/support-and-services/contact-support.html
Partner Product for Integration	GigaVUE-HC2 Bypass
Product Description	The GigaVUE-HC2 visibility node offers incorporates a broad spectrum of GigaSMART® traffic intelligence capabilities such as: Application Filtering Intelligence and Inline Bypass, and embedded TAP modules. With a combined throughput exceeding 1Tb, the node easily accommodates non-blocking port speeds of 1Gb, 10Gb, 40Gb and 100Gb. GigaVUE-HC2 scales as your network needs evolve, accommodating thousands of flow map rules and featuring some of the industry's highest-density line cards, all in a compressed form factor.

Use Cases for Integration into Palo Alto Networks Next Generation Security Operating Platform

Customers may need multiple Palo Alto Networks NGFW appliances to scale to the volume of traffic generated on their network. When the aggregate traffic exceeds the capacity of any single Palo Alto Networks NGFW, you must deploy multiple NGFWs with the ability to select traffic of interest, while bypassing the rest, and then distributing the selected traffic of interest among two or more NGFWs.

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 Gigamon-HC2 will distribute traffic amongst the remaining members, thereby ensuring availability of the security functions provided by the Palo Alto Networks NGFW.

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 the setting in the inline network link, eliminating the need for physical change control procedures.

The combined GigaVUE-HC2 and Palo Alto Networks Next Generation Firewalls use the Giamon-GigaVUE-HC2 chassis for inline high availability and traffic distribution achieves the following objectives

- High availability of NGFW 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.
- Traffic distribution to multiple NGFW appliances for load sharing across multiple instances.
- 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.

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Gigamon versions tested
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW	Complete	PAN-OS 9.0	GigaVUE-OS 5.6.00
Panorama			
Prisma Access			
Prisma Public Cloud			
Prisma SaaS			
Traps			
VM-Series	Complete	PAN-OS 9.0	GigaVUE-OS 5.6.00
WildFire			
Other			

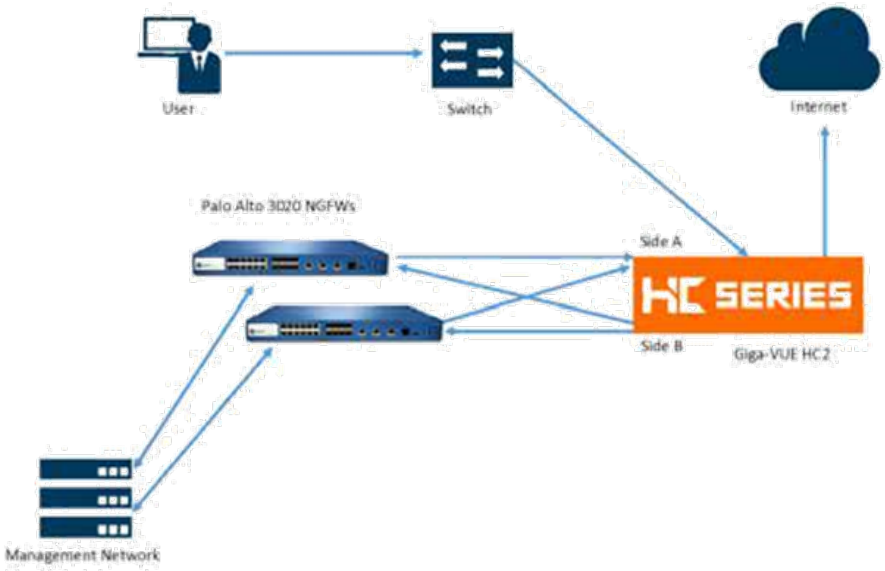
Integration Benefits

The Gigamon Bypass Module in the GigaVUE-HC2 Series provides bypass protection to NGFWs. The module leverages two levels of bypass protection: physical and logical. Physical bypass preserves network traffic, failing to wire in the event of a power outage. Logical bypass protects against inline tool failures that could disrupt network traffic. Bidirectional heartbeats monitor the health of the inline tool and in the event of a loss of link or loss of heartbeat the GigaVUE-HC2 can bypass traffic around the failing tool. Alternatively, the GigaVUE-HC2 can bring down the network link so that the traffic can be routed to a redundant network path. The Gigamon Bypass Module is designed to work with fiber links. For copper bypass, Gigamon offers a GigaVUE-HC2 copper TAP and Bypass module. This module includes electrical relays that can be used for bypass protection.

- Traffic Distribution for Load Sharing
    - Improve the scalability of inline security by distributing the traffic across multiple Palo Alto Networks NGFW appliances, allowing them to share the load and inspect more traffic.
- Agile Deployment

- Add, remove, and/or upgrade Palo Alto Networks NGFW appliances without disrupting network traffic; converting Palo Alto Networks NGFW appliances from out-of-band monitoring to inline inspection on the fly without rewiring.

Integration Diagram



- *Figure 1-1: Gigamon Inline Bypass with Palo Alto Networks NGFW*

This section presents the combined solution using a GigaVUE-HC2 inline bypass module with two NGFW appliances. The reference architecture in Figure 1-1 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.

- Notice in Figure 1-1 that there is a sidedness to the architecture because data flows to and from side A while the clients reside to side B where the Internet and resources they request also reside.
- NOTE: It is essential that you connect the inline network and inline tool device bridge links to the GigaVUE-HC2 correctly relative to Side A and Side B so that traffic is distributed correctly to the NGFW devices of the inline tool group.

Before You Begin

The Gigamon plus Palo Alto Networks Next Generation Firewall (NGFW) solution consists of the following:

- GigaVUE-HC2 chassis with GigaVUE-OS 5.6.00 software, one PRT-HC0-X24, and one TAP-HC0-G100C0 (a BPS-HC0 line card can also be used)
- GigaVUE-FM version 5.6 software for GigaVUE-HC2 GUI configuration
- Two Palo Alto Networks NGFW appliances (hardware appliances or VM-Series)
- PAN-OS 9.0

NOTE: This guide assumes all appliances are fully licensed for all features used, management network interfaces have been configured, and an account with sufficient admin privileges is used.

Overview

This section describes the configuration procedures for the GigaVUE-HC2 and Palo Alto Networks 3020 NGFW as an inline tool group solution through Gigamon GigaVUE-FM. The procedures are organized as follows:

- NGFW Configuration: Virtual Wire
- Gigamon GigaVUE-HC2 Configuration: Inline Networks and Inline Tool Groups

The procedures configure the GigaVUE-HC2 to send live traffic to the Palo Alto Networks inline tool group, which will allow the use of Palo Alto Networks' NGFW protection capabilities.

Per best practices guidelines from Palo Alto Networks, the Gigamon GigaVUE-HC2 will be configured to distribute the traffic to the two Palo Alto Networks appliances in the inline tool group, assuring all traffic for any given client (by IP address) goes to the same member of the Palo Alto Networks inline tool group.

NOTE: This chapter assumes that you have connected the Palo Alto Networks appliances directly to the GigaVUE-HC2 as shown in Figure 1-1. You should configure all GigaVUE-HC2 ports that connects the Palo Alto Networks appliances as port type Inline Tool. Furthermore, you should configure the GigaVUE-HC2 inline bypass ports connected to the network devices as Inline Network ports. For specific instructions on how to complete these tasks, refer to the User Guides and Technical Documentation in the Customer Portal, which you can access from the Gigamon web site.

Palo Alto Networks Configuration

Palo Alto Networks NGFW Configuration: Virtual Wire

The procedures described in this section apply to the shaded area highlighted in the reference architecture diagram shown in Figure 2-1.

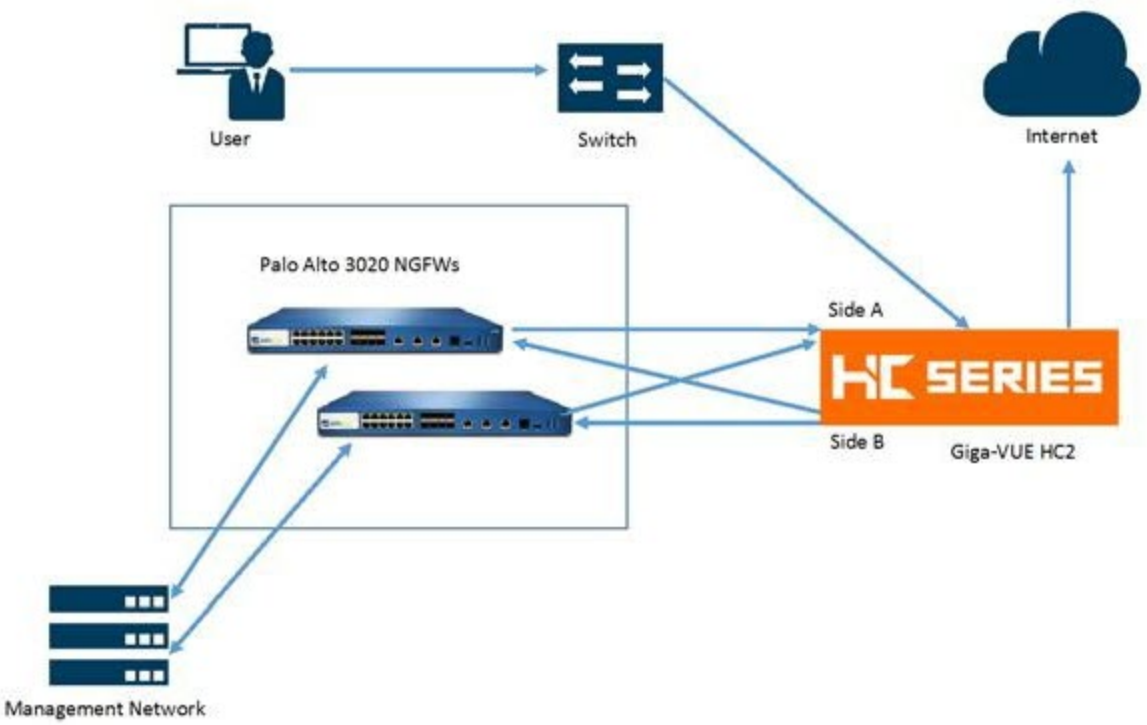
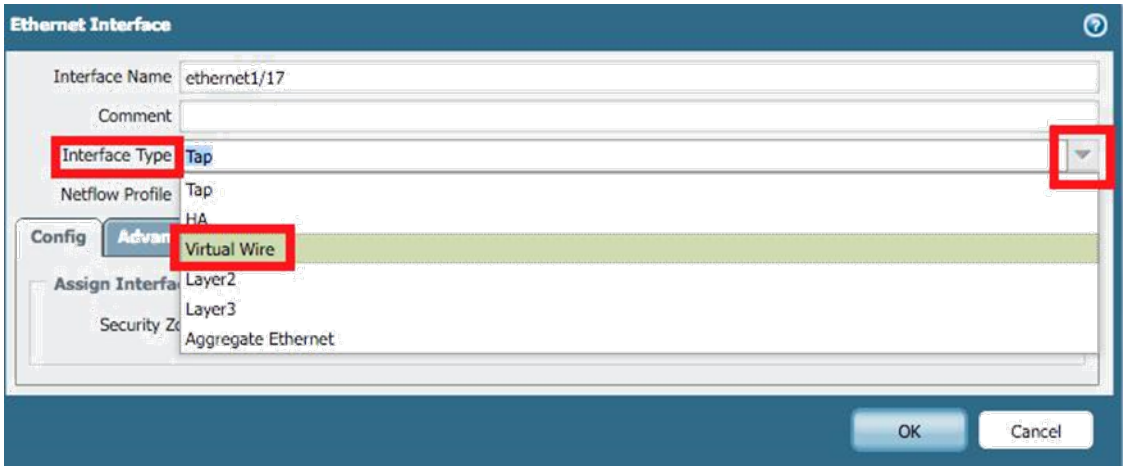


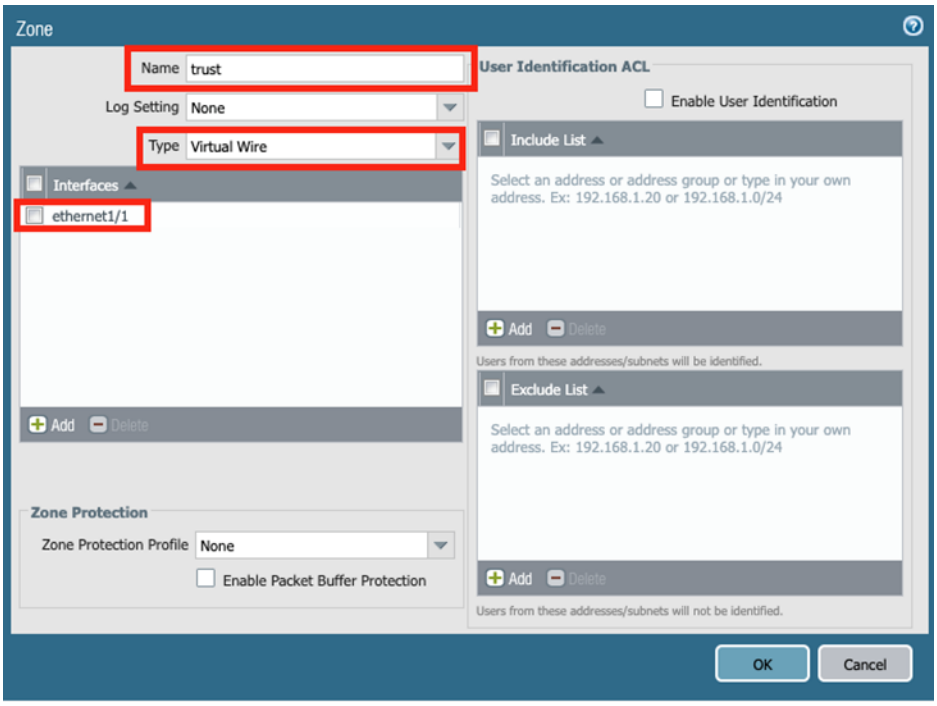
Figure 2-1: Palo Alto Networks NGFW

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

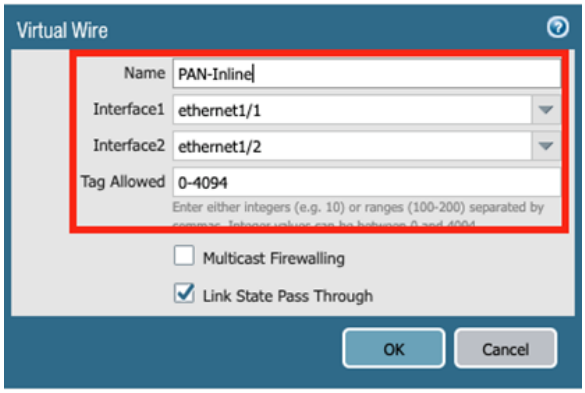
1. In the NGFW web interface, go to the Network tab > Interfaces:
   a. Click on the first interface you want to configure as part of the pair.
   b. Set the **Interface Type** to **Virtual Wire** by clicking on the down arrow to the right.



2. On the Config tab next to **Virtual Wire** click the down arrow to the right.
3. Repeat for the second interface as well.
4. Select **Network > Zones**.
    a. Click Add at the bottom.

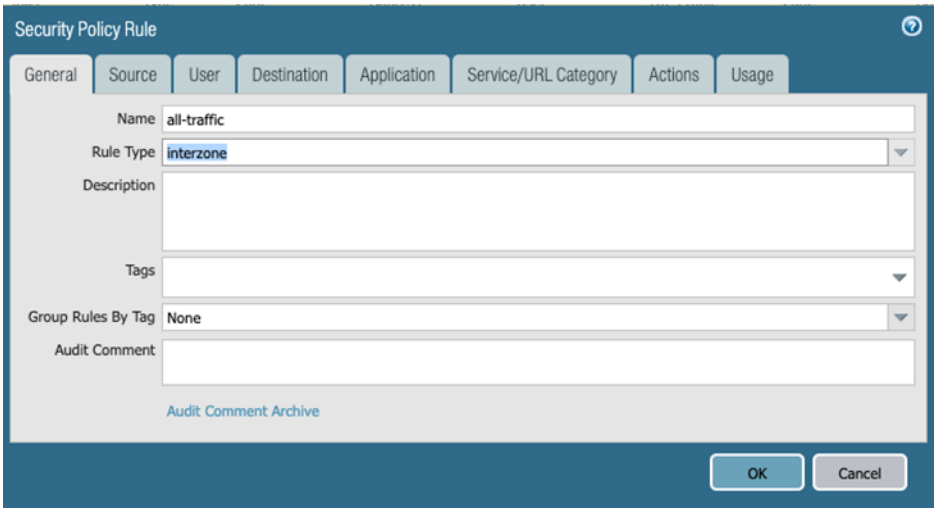


    b. Pick an appropriate name for zone; type would be virtual wire and lastly select interface for that zone.
    c. Create another zone for the second interface as well.
5. Next select **Network > Virtual Wires**
    a. Click **Add** from the bottom.

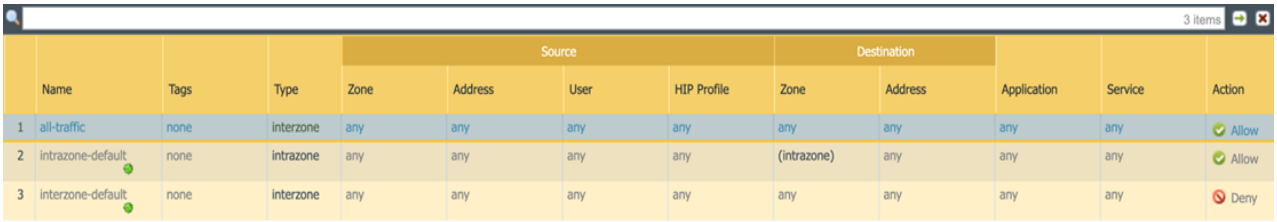


    b. Pick appropriate name.
    c. Select each interface from drop down.
    d. Enter 0-4094 in Tags allowed field. Gigamon adds an outer vlan tag to allow correct packet flow.

6. Next Click **Policies > Security**
   a. Click **Add** at the bottom



   b. Pick a name for the policy. For this example, we allowed any/any for all policies. This can be tailored to desired needs.



7. When done, be sure to click **Commit** to apply the changes.
8. Repeat these steps on the additional NGFW devices/instances

Partner Product Configuration

GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups

This section covers configuring the GigaVUE-HC2 for all inline network and inline tool elements that you will use to create traffic flow maps. There are some configuration differences depending upon whether you are using BPS (Bypass fiber) or BPC (Bypass copper) interfaces for inline bypass. This section explains these differences. The 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 the Palo Alto Networks NGFW

The configuration procedures described in this section apply to the highlighted area in Figure 2-4.

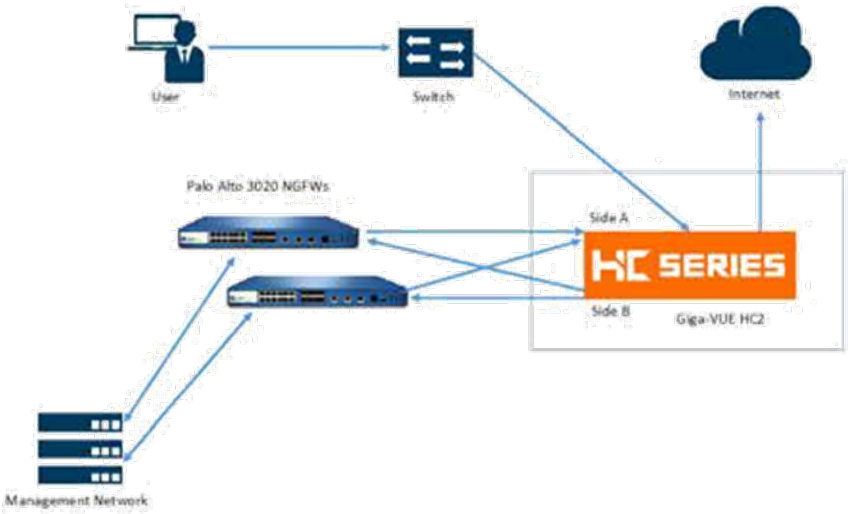


Figure 2-4: Gigamon GigaVUE-HC2 Configurations

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 enterprise infrastructure grows, you can add additional inline network pairs to the inline network group. The basic steps are as follows:

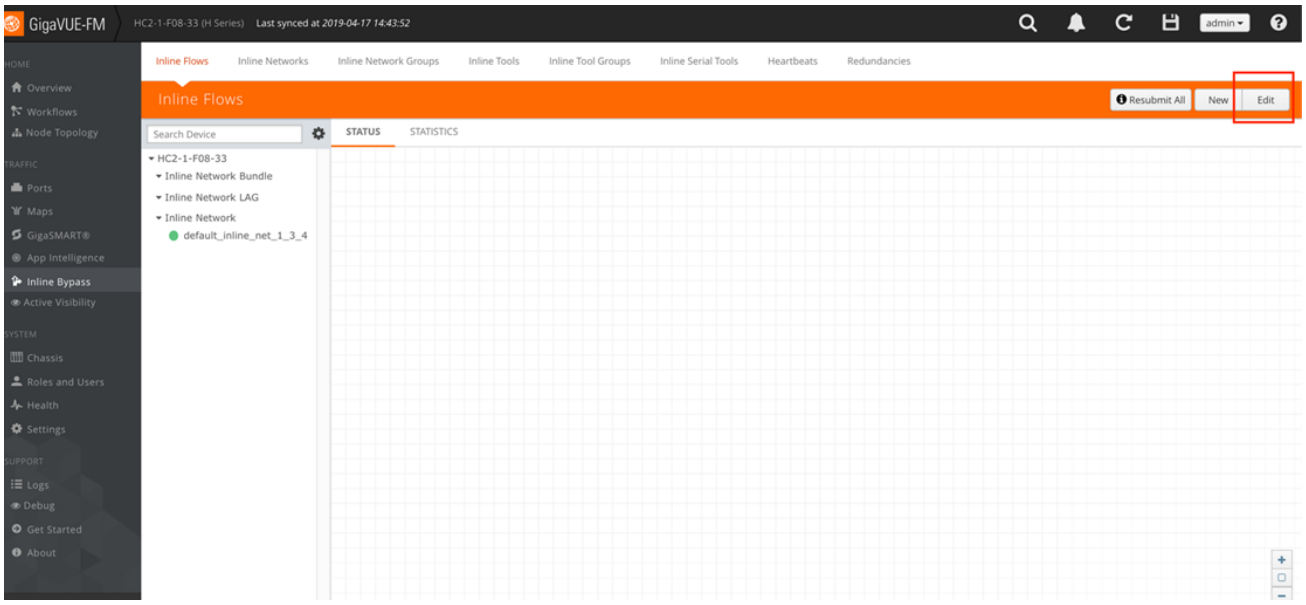
- Step 1: Configure the Inline Network Bypass Pair
- Step 2: Configure the Inline Network Group
- Step 3: Configure the Inline Tools

NOTE: This section assumes all the ports to which the network devices connected to are set as Inline Network port types. For specific instructions on completing these tasks, refer to the User Guides and Technical Documentation in the Customer Portal, which you can access from the Gigamon website.

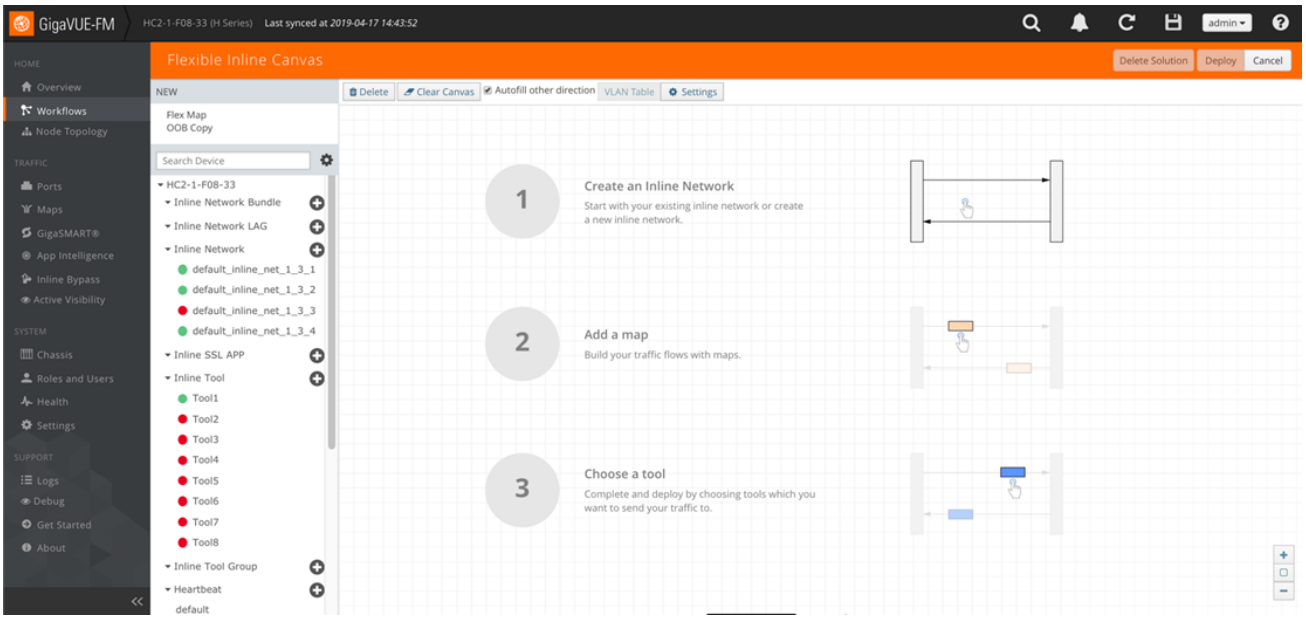
Step 1: Configure the Inline Network Bypass Pair

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

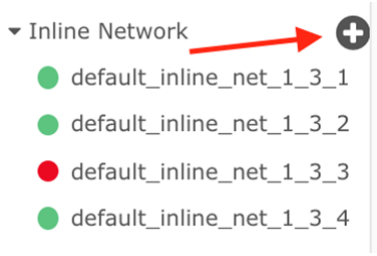
1. Log into GigaVUE-FM, select **Physical Nodes**
2. Select the GigaVUE-HC2 from the list of physical nodes GigaVUE-FM is managing.
3. Select **Inline Bypass > Edit**. This will take you to Flexible Inline Canvas where all inline configuration is done.



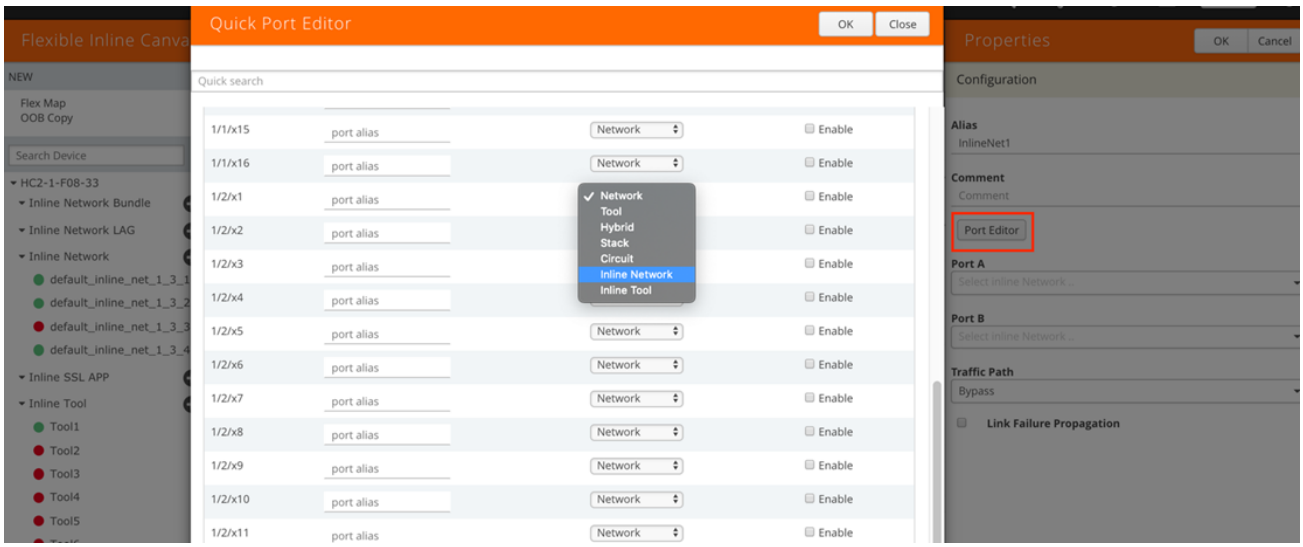
NOTE: If there is a bypass combo module in the GigaVUE-HC2, there will be four preconfigured Inline Network port pairs as shown in Figure 2-5. If your network is 1G or 10G fiber, use one of these preconfigured inline bypass pairs and move on to Step 2. If your network is 1G copper, follow the instructions below.



4. Click **Plus** sign next to Inline Network.



5. On the new Properties page, do the following, and then click **Save** when you are done.
   a. In the **Alias** field, type an alias that will help you remember which network link this Inline Network bypass pair represents. For example, `InLineNet1`.
   b. Click **Port Editor** and choose desired network ports and make them **Inline Network** and check **Enable**.



   c. Select the port for **Port A** and **Port B** by using the drop-down list or by typing the port label in the Port A field for the A Side port and same thing for B side as it is represented in the network topology diagram shown in Figure 1-1.

NOTE: You'll need at least two ports to make an inline network.

   d. Leave the **Traffic Path** and **Link Failure Propagation** set to the default values.
   e. Select **Physical Bypass** (if available). This minimizes packet loss during traffic map changes.

The configuration page should look like the example shown in Figure 2-6.

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 a subsequent section. Physical Bypass Option is only available with protected ports.

6. Leave Redundancy Profile to None.
7. Repeat these steps for all other network links.

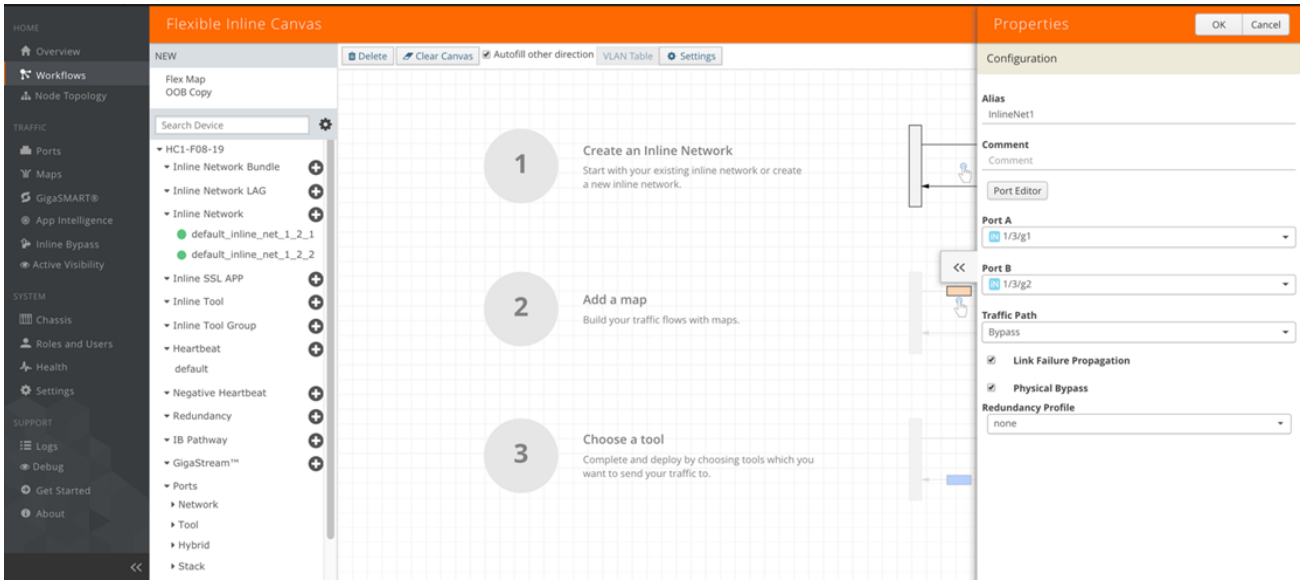
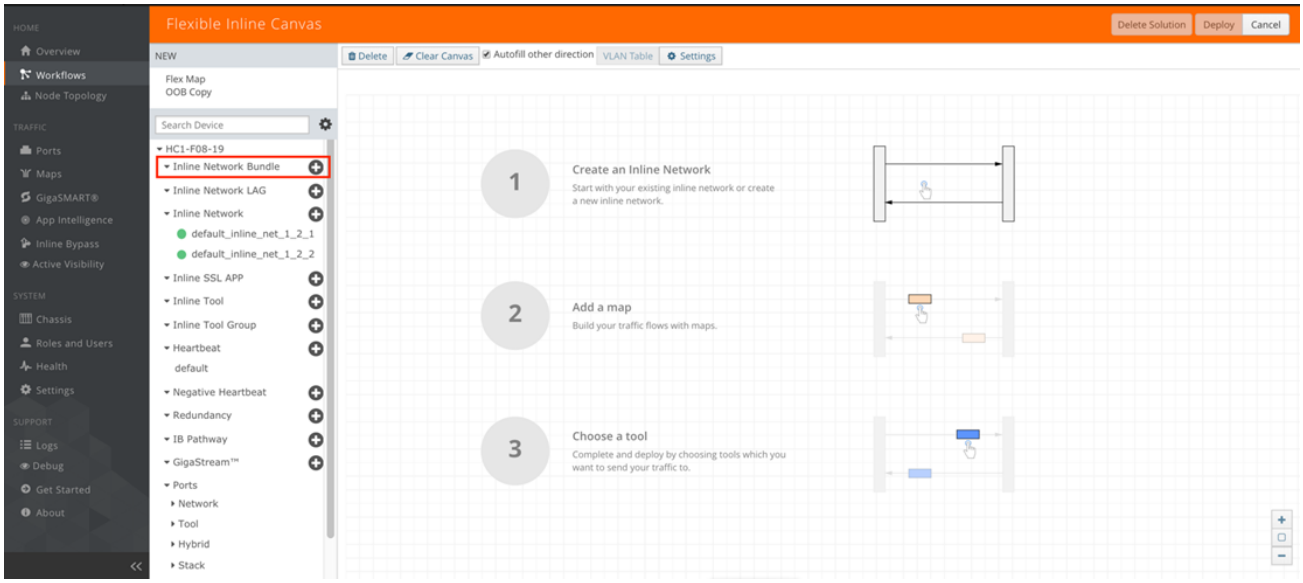


Figure 2-6: Inline Network Pair Configuration

Step 2: Configure the Inline Network Group

To configure the inline network group, do the following:

1. In Flexible Inline Canvas, Click **Plus** sign next to **Inline Network Bundle**.



2. In the **Alias** field, type an alias that represents the inline network group. For example, `PaloAlto-A_NGroup`.
3. Click the **Inline Network** field and either select from the drop-down list as shown in Figure 2-8 or start typing any portion of the alias associated with Inline Network you want to add to the Inline Network Group.
4. Continue adding inline networks until all port pairs are in the **Inline Network** field as shown in Figure 2-8.

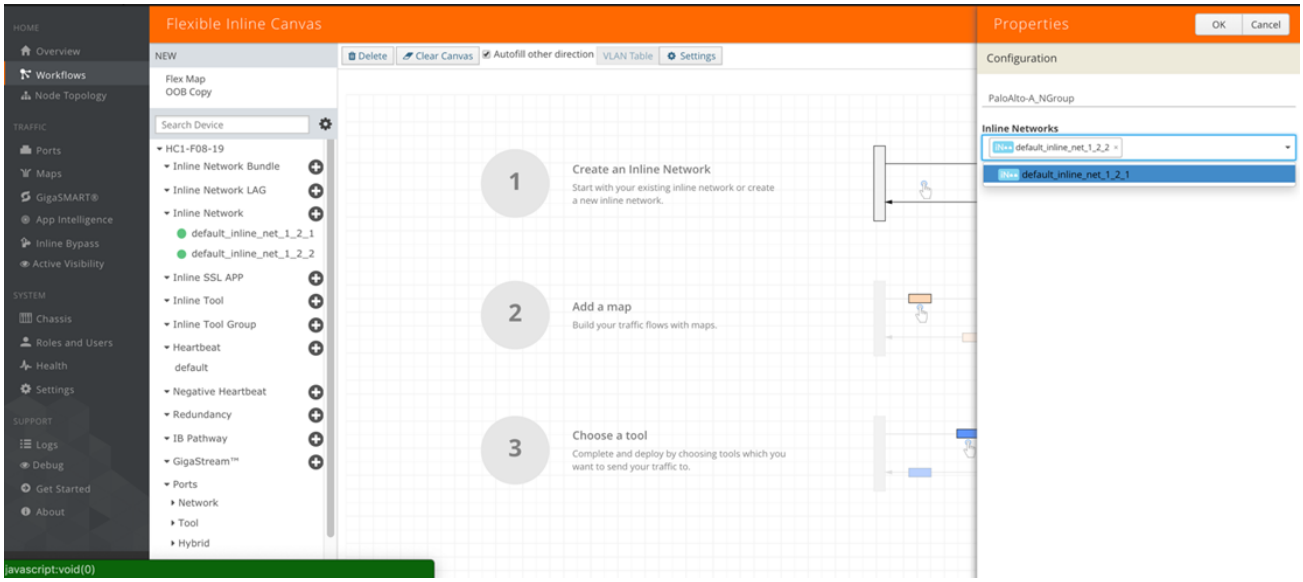


Figure 2-8: Inline Networks added to the Inline Network Group

5. Click **OK** when you are done.

   The Inline Network Groups page should look similar to what is shown in Figure 2-9.

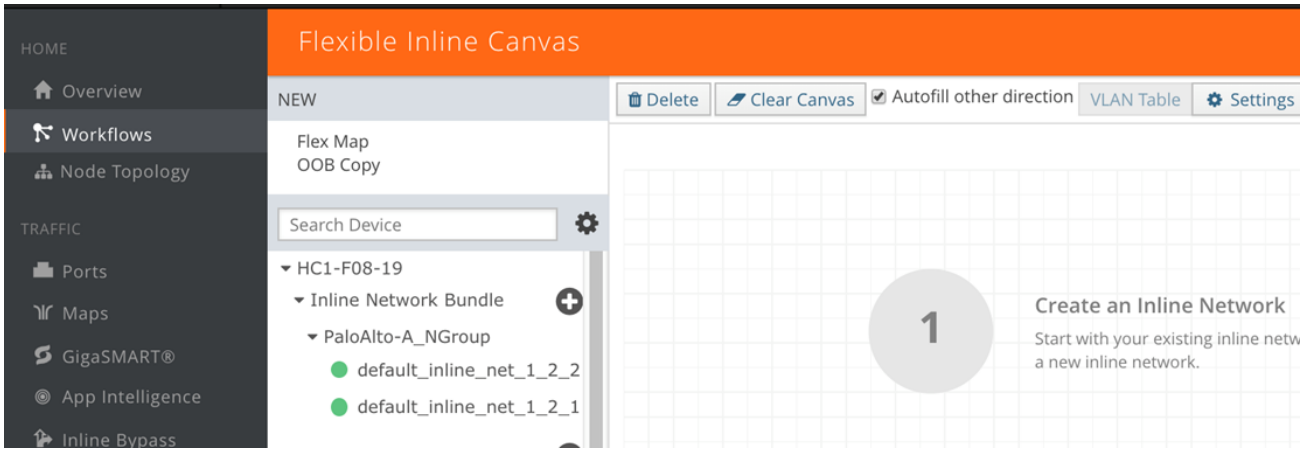


Figure 2-9: Finished list of Inline Network Groups

Step 3: Configure the Inline Tools

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 defined in later steps.

1. In Flexible Inline Canvas, click **Plus** sign next to **Inline Tool**.

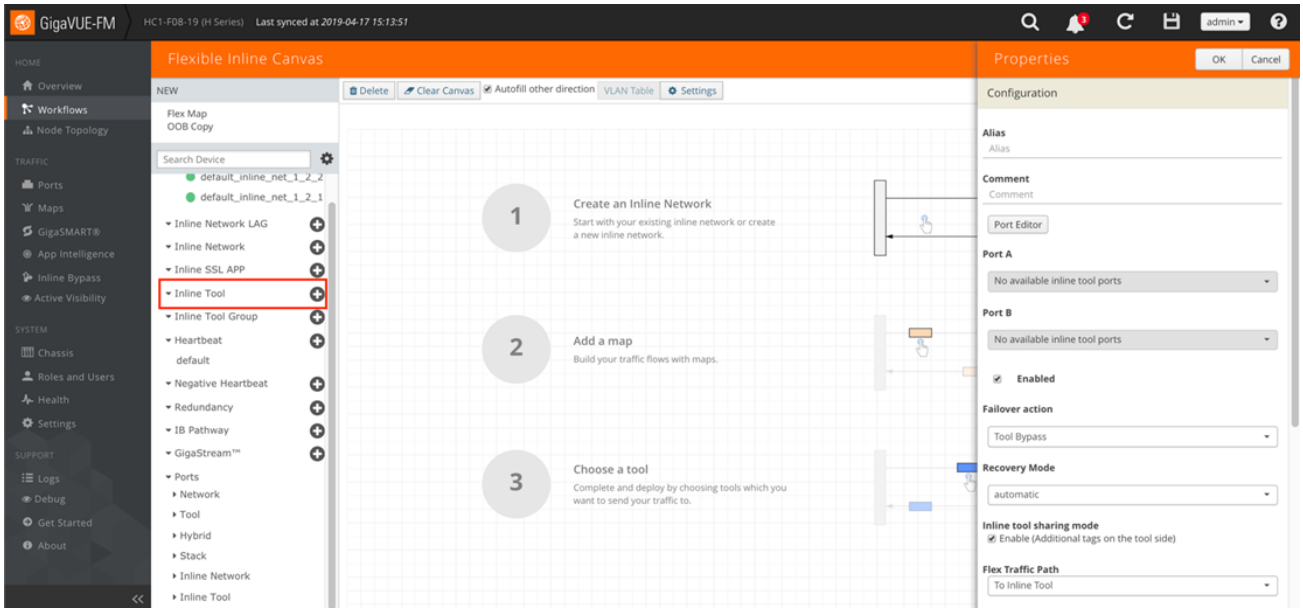
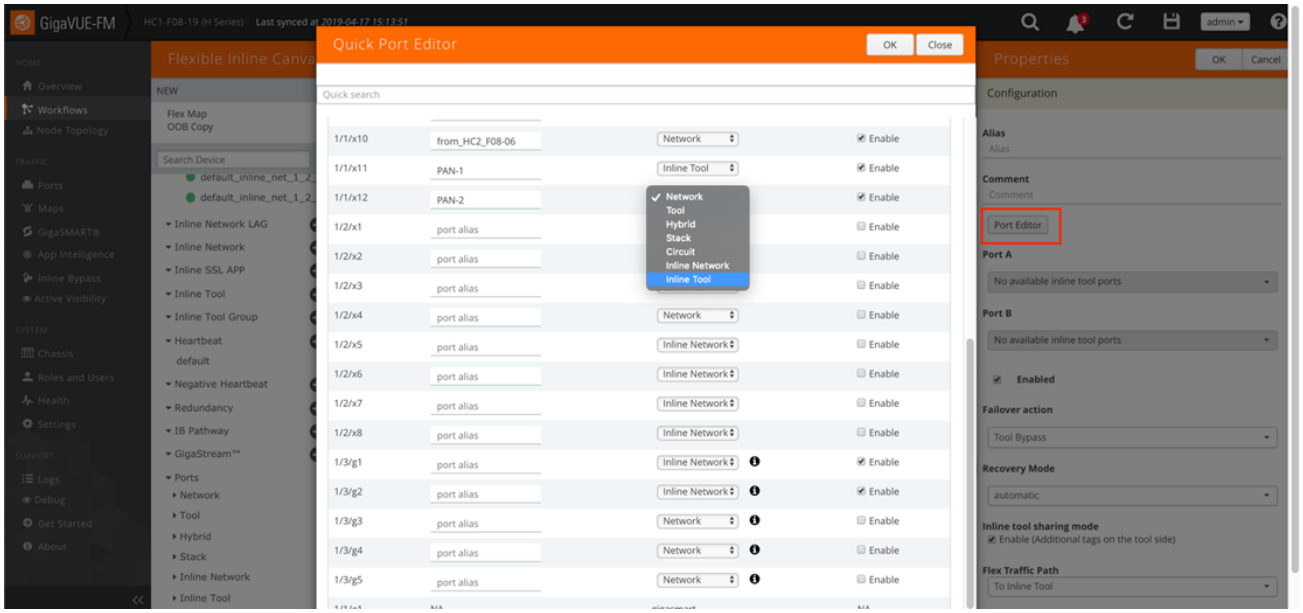


Figure 2-10: Creating Inline Tools

2. Click **Port Editor** and choose desired ports and make them **Inline Tool** and check **Enable**.



3. In the **Alias** field, type an alias that will help you remember which inline tool this inline tool pair represents. For example, `PaloAlto1`.
4. In the Ports section, specify the ports as follows:
   a. For **Port A**, specify the port that corresponds to Side A in the network diagram.
   b. For **Port B**, specify the port that corresponds to Side B in the network diagram.
   For the network diagram, refer to Figure 1-1.

   Important: It is essential Port A and Port B match Side A and B, respectively, of the inline network port pairs.

5. Check **Enable** under **Regular Heartbeat**.
6. Leave the default setting for the remaining configuration options.

   Your configuration should be similar to the example shown in Figure 2-11.

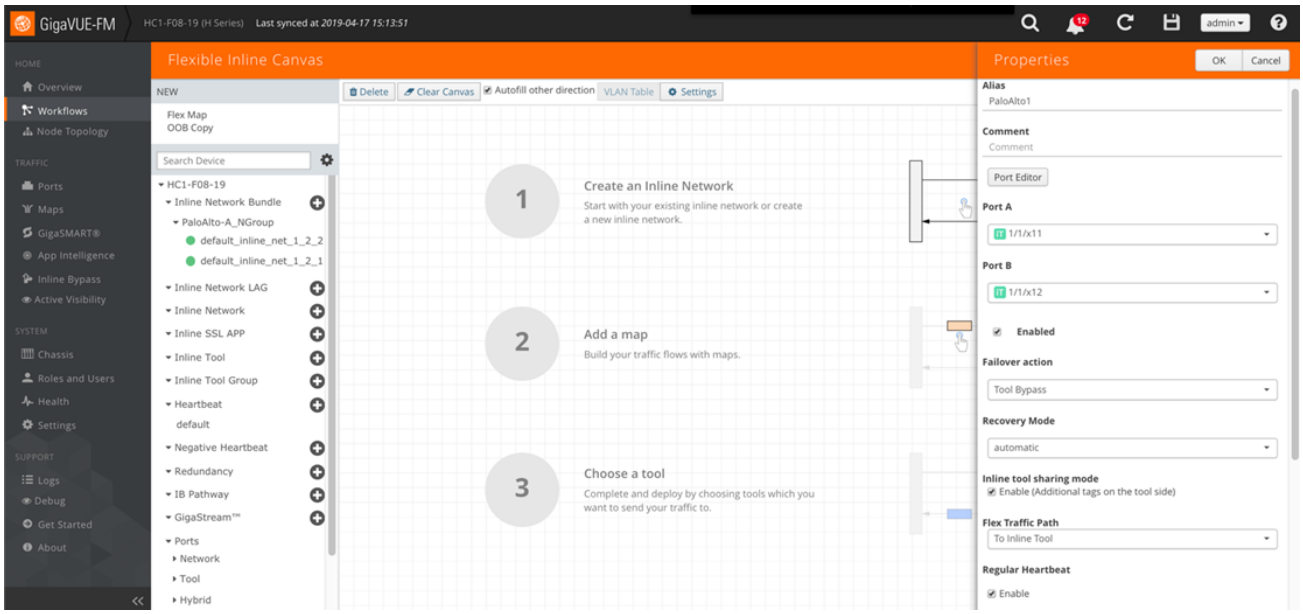


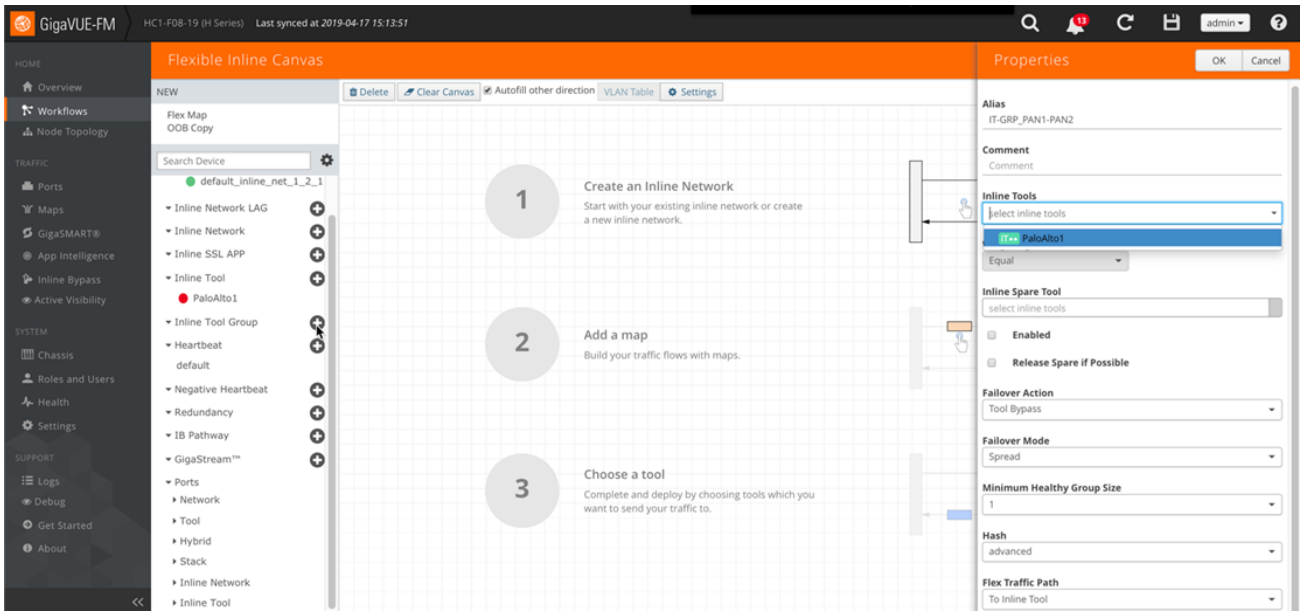
Figure 2-11: Inline Tool Pair Configuration

7. Click OK.
8. 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. The online help fully describes other options for inline tool. The other options have very different effects on the overall traffic flow. If you have not enabled the heartbeat feature, the failover action will only take place if one of the tool port links go down.

Step 4: Configure the Inline Tool Group

To configure the inline tool group, do the following:

1. In Flexible Inline Canvas, Click **Plus** sign next to **Inline Tool Group**.



2. New Properties Window will pop up on the left.
3. In the **Alias** field, type an alias that describes the inline tool groups. For example, `IT-GRP_PAN1-PAN2`.
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.

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

5. In the Configuration section, do the following, and then click **Save** when you are done:
   a. Select **Enable**.
   b. Select **Release Spare If Possible** if applicable.
   c. Keep the defaults for **Failover Action**, **Failover Mode**, and **Minimum Healthy Group Size**.
   d. Select **Equal** under **Weighting**. This will load share among multiple NGFW devices.

   The configuration should look similar to the example shown in Figure 2-12.

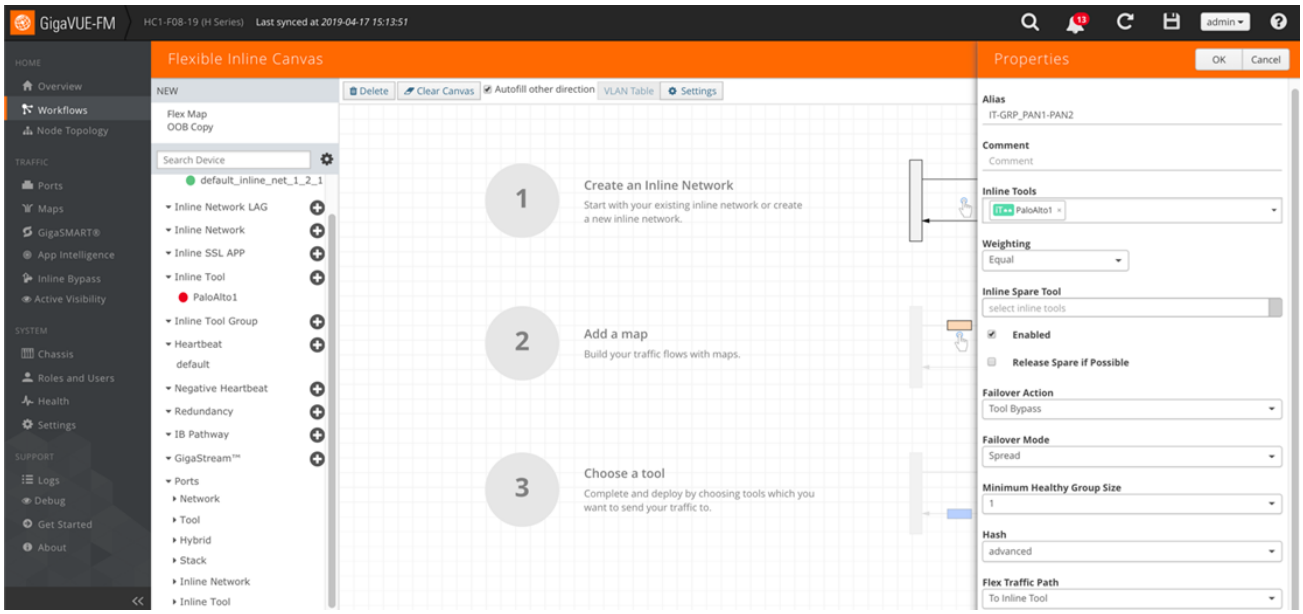


Figure 2-12: Inline Tool Group Configuration

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 Palo Alto Networks tool group, allowing you to test the deployment functionality of the Palo Alto Networks appliances within the group. This is done in the following steps:

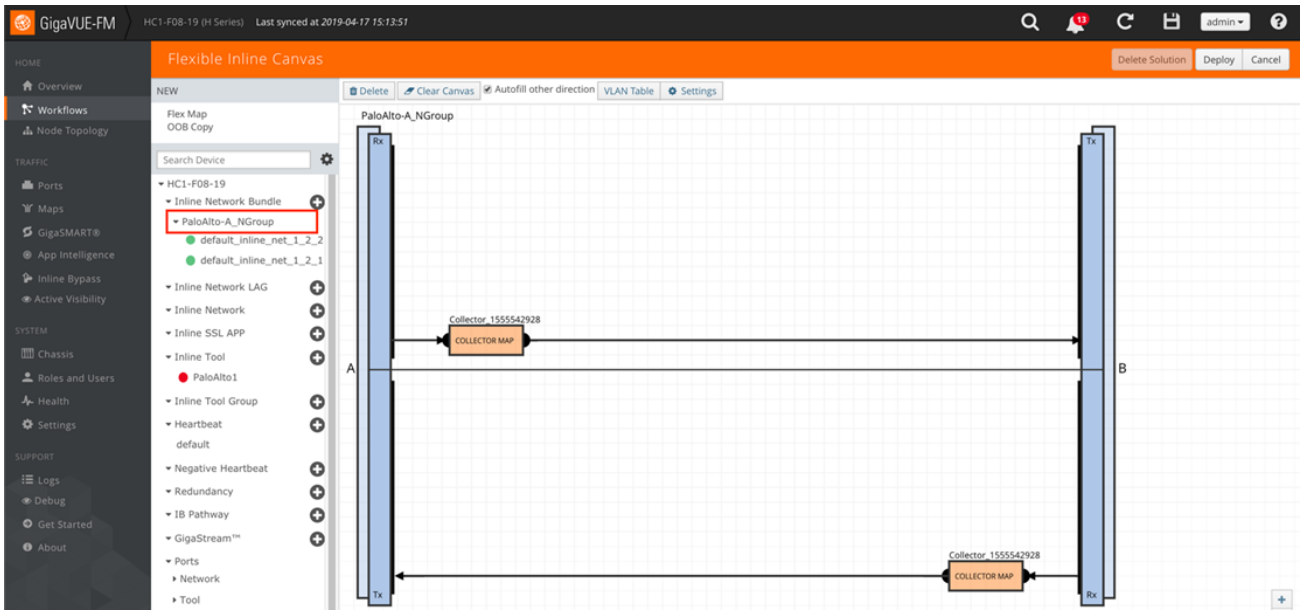
- Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule
- Step 2: Change Inline Network Traffic Path to Inline Tool

After completing these steps, you will be ready to test the deployment of the Palo Alto Networks appliances. The section Testing the Functionality of the Palo Alto Networks Inline Tool on page 26 describes the test procedure.

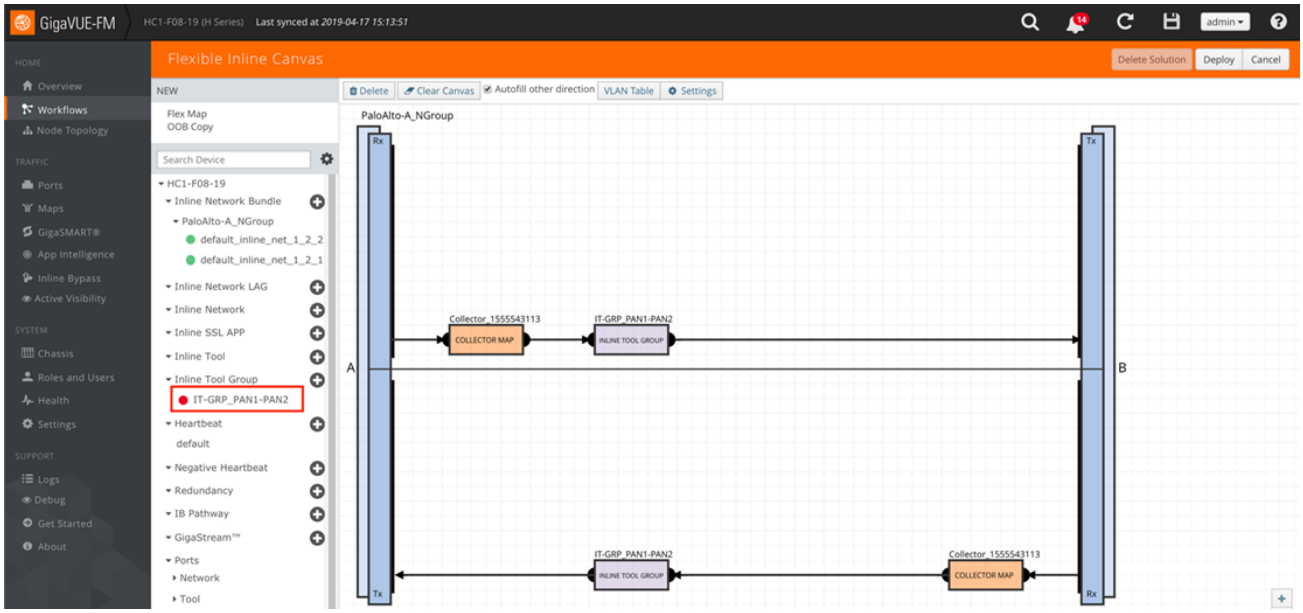
Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule

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

1. In **Flexible Inline Canvas**, **Drag and Drop** the **Inline Network** group that was created earlier.



2. If you want to send all traffic to the NGFW systems, simply **Drag and Drop** the **PAN Tool Group** in the path of the **Collector Map**. The map can be renamed by clicking on it.



- If you want to send specific traffic to the NGFW systems, simply **Drag and Drop** the **Flex Map** from top.

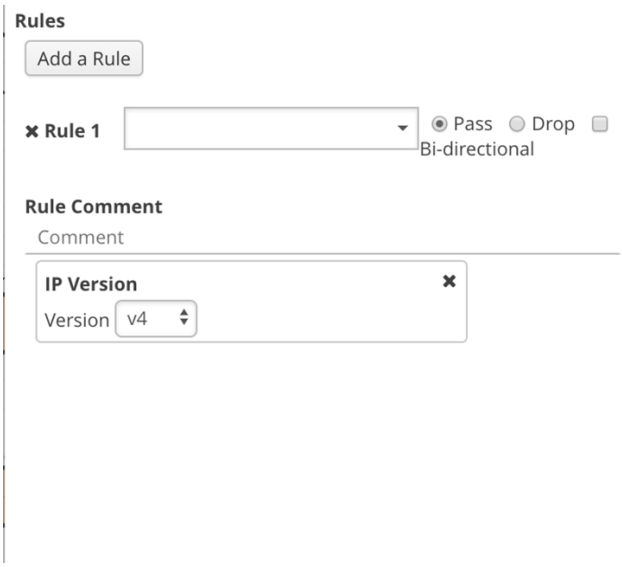
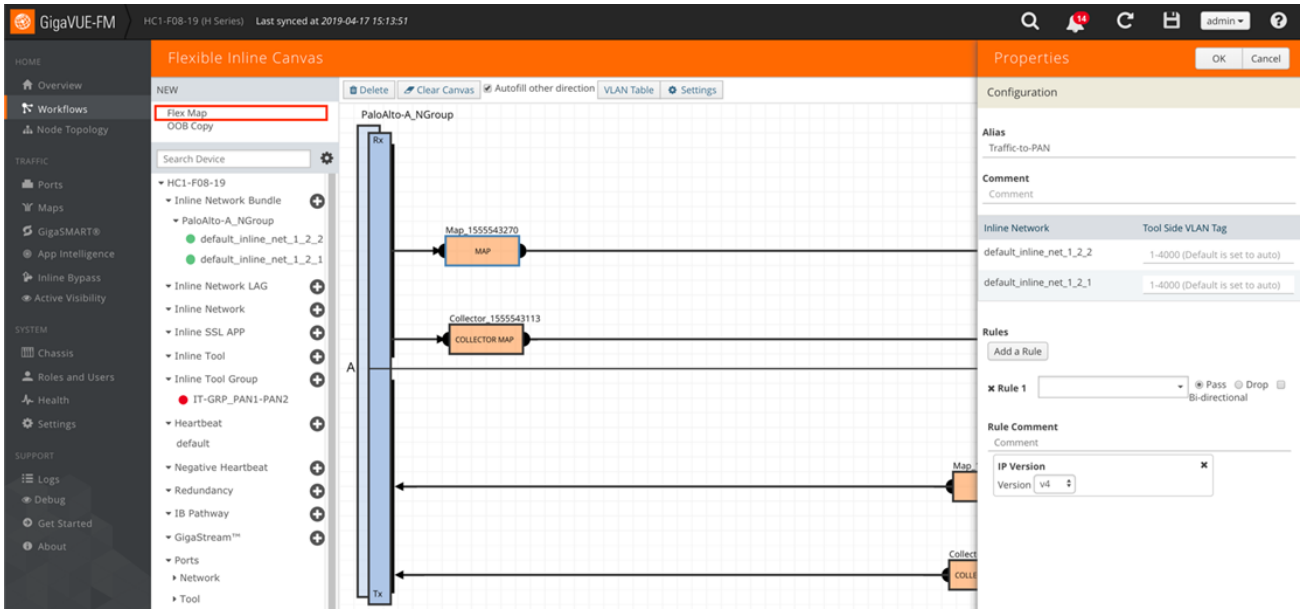


Figure 2-13: Rule for Inline Tool Flow Map

3. In new window, type the map name. For example, `Traffic-to-PAN`
4. Click **Add Rule**:
   a. Click in the Condition search field for the rule and select **IP Version** from the drop-down list.
   b. Select **Pass**. (This is the default.)
   c. Select **Bidirectional**.
   d. In the **IP Version** drop-down list, select **4**.

The map rule should look like the rule shown in Figure 2-13.



7. Click **OK** to close the window.

8. **Drag and Drop** the **PAN Inline Tool Group** on the Map Path.

9. Click **Deploy** to deploy the solution.

Step 2: 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 **Inline Bypass > Edit**.
2. Click one of the inline networks that you defined previously (refer to Step 2: Configure the Inline Network Group in *Configure the GigaVUE-HC2 Inline Network and Inline Tools* section above).
3. In the Configuration section, make the following changes:
   a. Set **Traffic Path** to **Inline Tool**.
   b. Uncheck **Physical Bypass**.

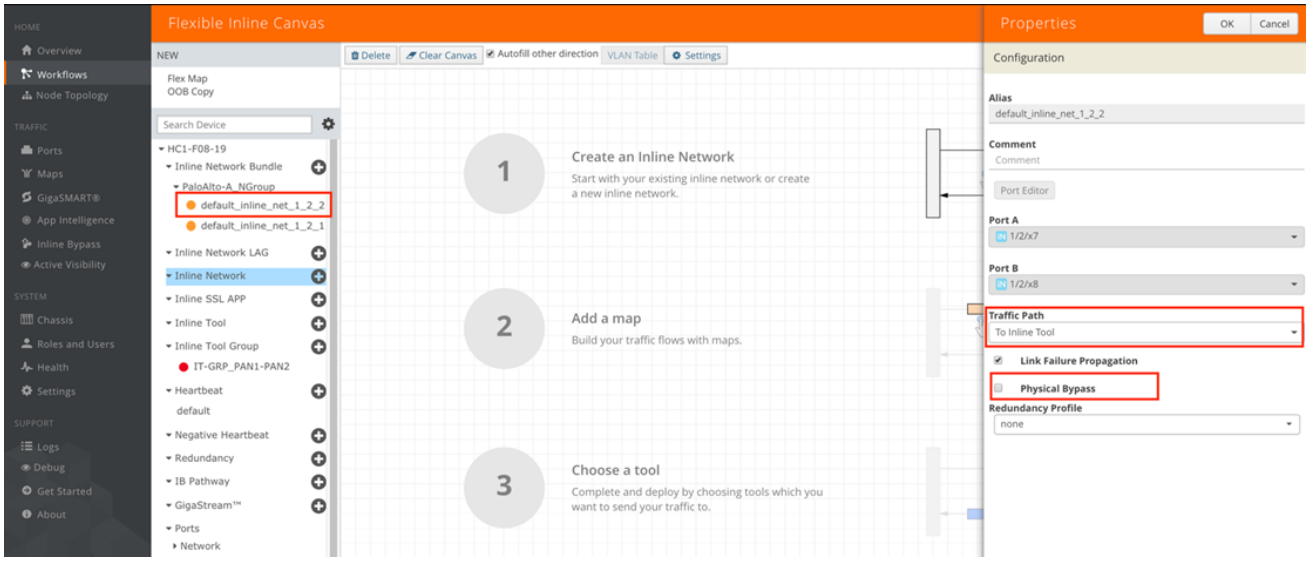


Figure 2-15: Inline Network Traffic Path Changed to Inline Tool, Physical Bypass Unchecked

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

Troubleshooting

One of the easiest ways to determine if the Palo Alto Networks NGFW is working properly is by attempting to access a website that should be blocked. An example of this is www.eicar.org, which hosts the eicar test virus for download. It is not an actual virus, but all major anti-malware vendors should detect it.

To test the functionality, do the following:

1. Go to a client computer that connects to the internet through the Palo Alto Networks NGFW's.
2. Open a web browser and go to www.eicar.org. Click ANTIMALWARE-TESTFILE as shown in the following figure.

3. Click the Download link

4. Scroll down and click on eicar.com.txt under the standard protocol http.

5. You should get a block page from Palo Alto Networks that looks like the page below:

NOTE: You can also view Threat Log statistics from the NGFW GUI to confirm it is blocking.

Summary and Conclusions

The previous sections described how to deploy Gigamon GigaVUE-HC2 bypass protection with Palo Alto Networks NGFW appliances. This combined solution using the Gigamon-GigaVUE-HC2 chassis for inline tool high availability and traffic distribution achieves the following objectives:

- High availability of Palo Alto Networks NGFW can be achieved 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.

- Traffic distribution to multiple NGFW appliances for load sharing across multiple instances.

- 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, 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 Palo Alto Networks products, refer to your Support Agreement with Palo Alto Networks and follow the directions on how to open a Support Case.