Palo Alto Networks NGFW with Gigamon Inline Deployment Guide

Contents

1 Overview 4
Use Case: Inline Bypass (Virtual Wire) Mode 4
Deployment Prerequisites 5
Architecture Overview 5
Access Credentials 6
2 Configurations 7
Palo Alto Networks 3020 NGFW Configuration: Virtual Wires 8
Configuring Palo Alto Networks for Virtual Wire mode 8
GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups 10
Configuring the GigaVUE-HC2 Inline Network and Inline Tools 11
Step 1: Configure the Inline Network Bypass Pair 11
Step 2: Configure the Inline Network Group 13
Step 3: Configure the Inline Tools 14
Step 4: Configure the Inline Tool Group 17
Configuring the Inline Traffic Flow Maps 18
Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule 18
Step 2: Configure the Inline Traffic Collector Map 19
Step 3: Change Inline Network Traffic Path to Inline Tool 20
Testing the Functionality of the Palo Alto Networks NGFW 21
3 Summary and Conclusions 23

1 Overview

The Palo Alto Networks® next-generation firewall is the core of the Enterprise Security Platform, designed from the ground up to address the most sophisticated threats. The next-generation firewall inspects all traffic — inclusive of applications, threats, and content — and ties it to the user, regardless of location or device type. The application, content, and user become integral components of the enterprise security policy. The result is the ability to align security with the key business initiatives, reduce response times to incidents, discover unknown threats, and streamline security network deployment with the Palo Alto Networks next-generation security platform.

The GigaVUE-HC2 Series is part of the GigaSECURE® Security Delivery Platform from Gigamon. The GigaBPS module in the GigaVUE-HC2 Series provides bypass protection to the Palo Alto Networks 3020 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 Gigamon-HC2 can bypass traffic around the failing tool. Alternatively, the Gigamon-HC2 can bring down the network link so that the traffic can be routed to a redundant network path. GigaBPS pertains specifically to fiber links. For copper bypass, Gigamon offers a GigaVUE-HC2 copper TAP module. This module includes electrical relays that can be used for bypass protection.

Aside from the above, deploying Palo Alto Networks and Gigamon together has the following benefits:

- 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.

The solution tested and described in this guide is based on a standard active inline network and tool deployment where two or more Palo Alto Networks appliances are directly cabled to one GigaVUE-HC2 chassis. The solution was tested with one GigaVUE-HC2 visibility node, one GigaVUE-FM Fabric Manager, and two Palo Alto Networks 3020 appliances.

This chapter covers the following:

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

Use Case: Inline Bypass (Virtual Wire) Mode

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.

Deployment Prerequisites

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

- GigaVUE-HC2 chassis with GigaVUE-OS 4.6.00 software, one PRT-HC0-X24, and one TAP-HC0-G100C0 (a BPS-HC0 line card can also be used).
- GigaVUE-FM version 3.3 software for GigaVUE-HC2 GUI configuration
- Two Palo Alto Networks NGFW appliances, model 3020. This includes the following:
  - Software version 7.1.1.

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.

Architecture Overview

This section presents the combined solution using a GigaVUE-HC2 inline bypass module with two Palo Alto Networks 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.

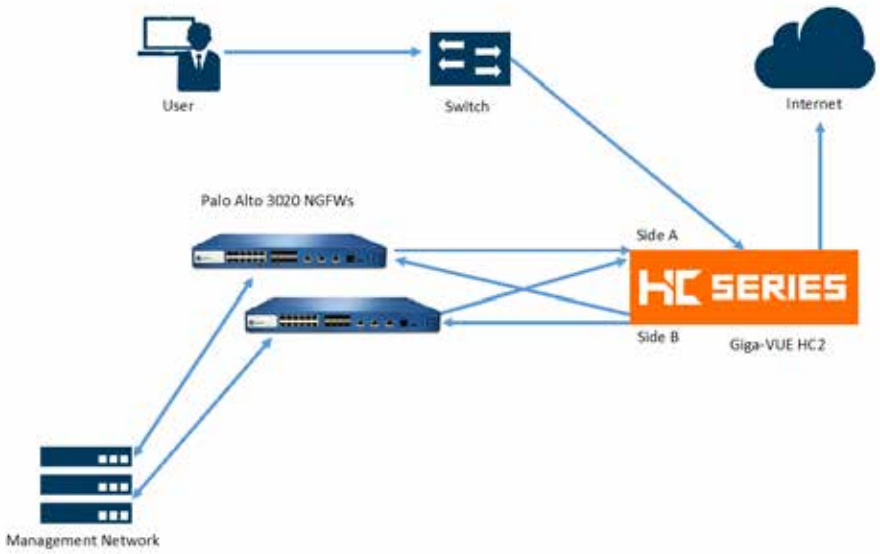


Figure 1-1: Gigamon Inline Bypass with Palo Alto Networks NGFW

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 Palo Alto Networks devices of the inline tool group.

Access Credentials

The default access credentials for the Gigamon GigaVUE-FM and Palo Alto Networks 3020 NGFW are as follows:

- Gigamon GigaVUE-FM access defaults:
  - Username: admin
  - Password: admin123A!
  - There is no default management IP address
- Palo Alto Networks 3020 NGFW access defaults:
  - Username: admin
  - Password: admin
  - Default management IP address: 192.168.1.1

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-HC with Giga-VUE-FM. For the equivalent H-VUE and CLI configuration commands, refer to the *GigaVUE-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 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:

- Palo Alto Networks 3020 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's 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 3020 NGFW Configuration: Virtual Wires

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

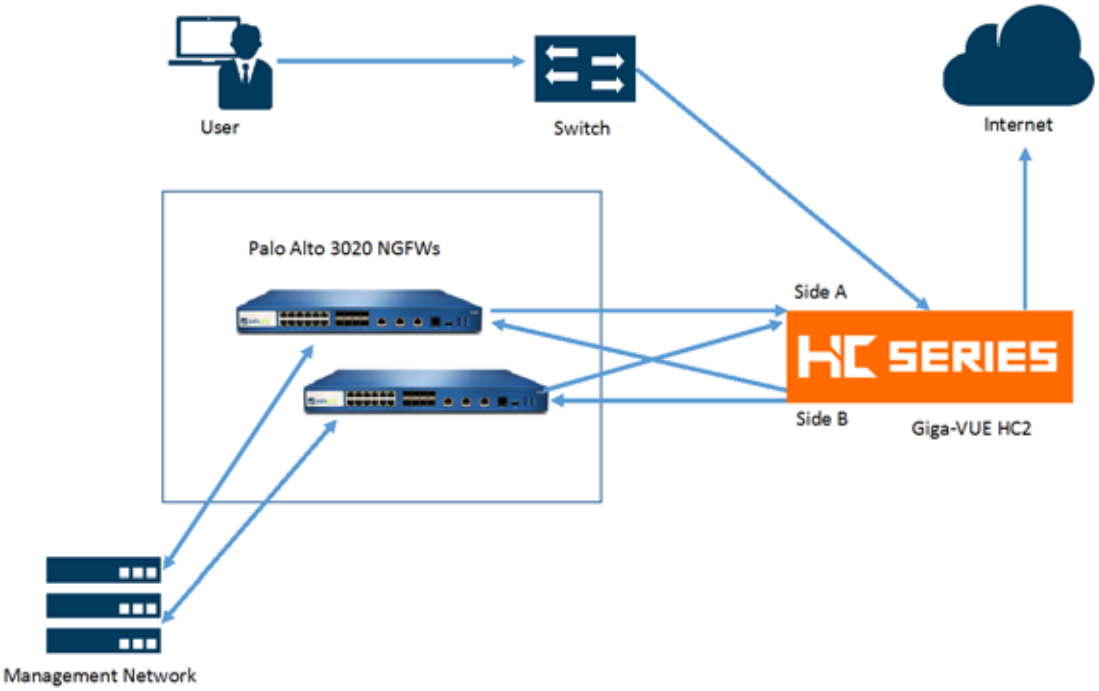


Figure 2-1: Palo Alto Networks 3020 NGFW

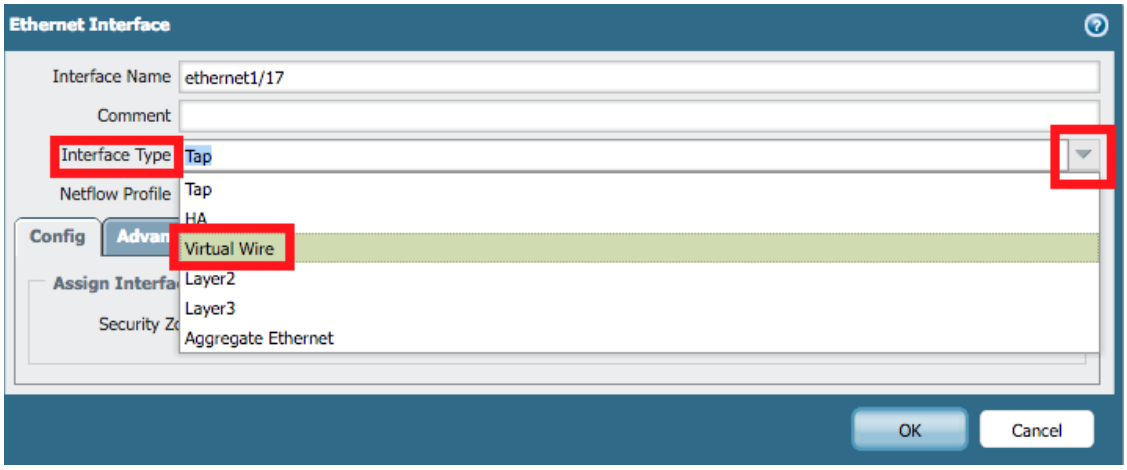
Configuring Palo Alto Networks for Virtual Wire mode

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

1. In the Palo Alto Networks GUI, go to the Network tab:

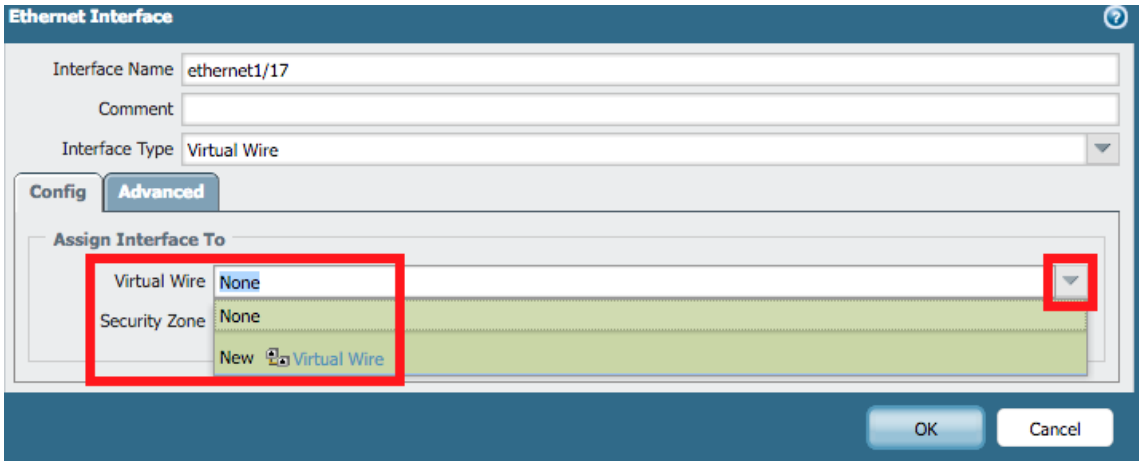
a. Click on the first interface you want to configure as part of the pair.

b. Set the **Interface Type** to **Virtual Wire** by clicking on the down arrow to the right.

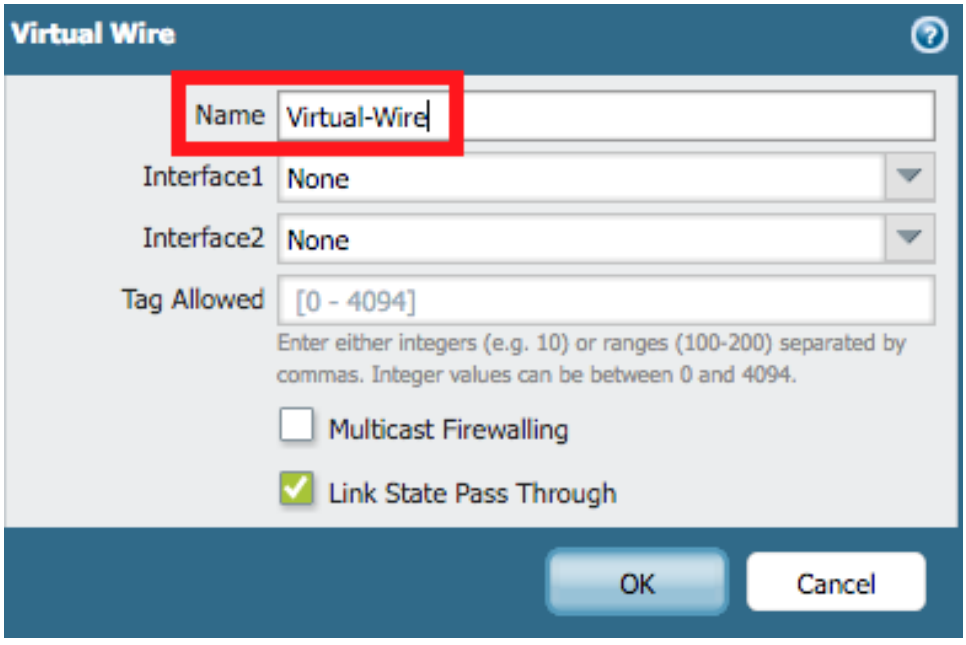


2. On the Config tab next to **Virtual Wire** click the down arrow to the right.

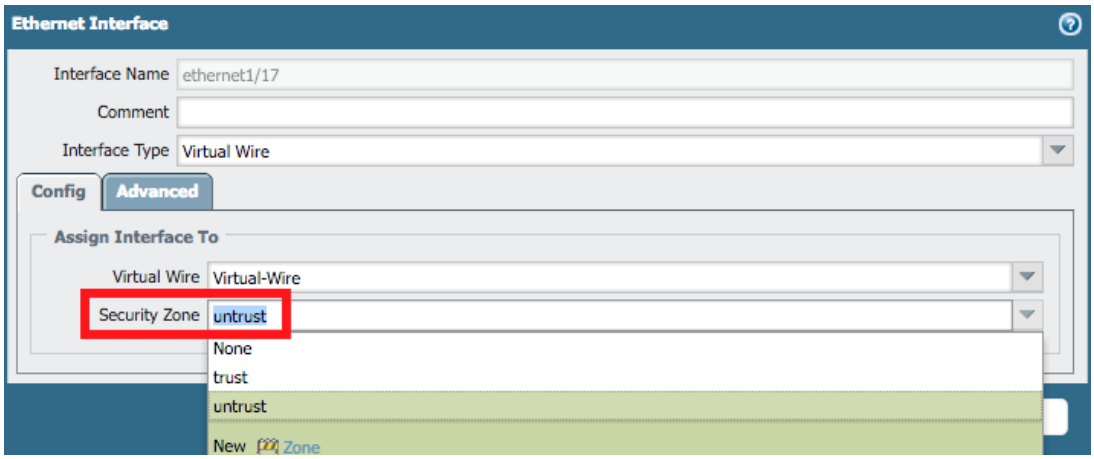
3. Select **New > Virtual Wire**.



4. In the **Name** field, enter a name for the Virtual Wire (Virtual-Wire in this example) and click **OK**.



5. Set the **Security Zone** to untrust and click **OK**.



6. Do the same for the next interface (ethernet1/18 in this example) but set the Security Zone to trust.

7. When done, be sure to click **Commit** (and optionally **Save**) to apply the changes.

8. Repeat these steps on the next Palo Alto Networks 3020 NGFW.

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.

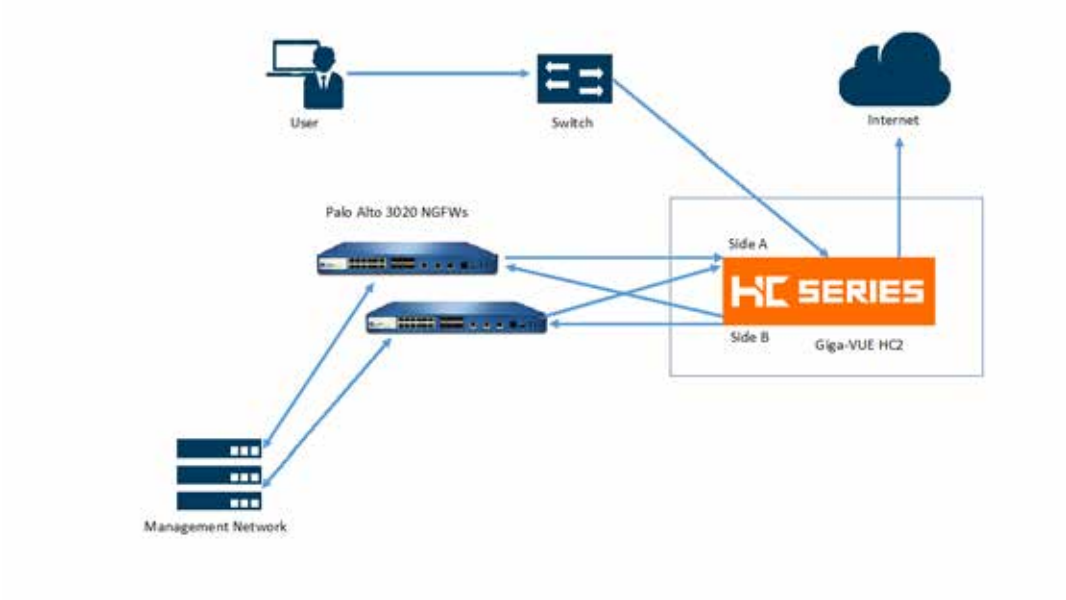


Figure 2-4: Gigamon GigaVUE-HC2 Configurations

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 > 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 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.

Figure 2-5: Inline Networks Page

4. Click New. The Inline Network configuration page displays.
5. On the Inline Network page, do the following, and then click **Save** when you are done.

   - In the **Alias** field, type an alias that will help you remember which network link this Inline Network bypass pair represents. For example, `InLineNet1`.
   - Select the port for **Port A** by using the drop-down list or by typing the port label in the Port A field for the A Side port as it is represented in the network topology diagram shown in Figure 1-1.
   - The value in the Port B field automatically populates once you have selected the port for Port A.

     Important: It is essential Side A and B of the GigaVUE-HC2 match the Side A and B of the Palo Alto Networks 3020 or traffic distribution or the Inline Tool Group will not work correctly.
   - Leave the **Traffic Path** and **Link Failure Propagation** set to the default values.
   - Select **Physical Bypass**. 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.

6. Repeat these steps for all other network links.

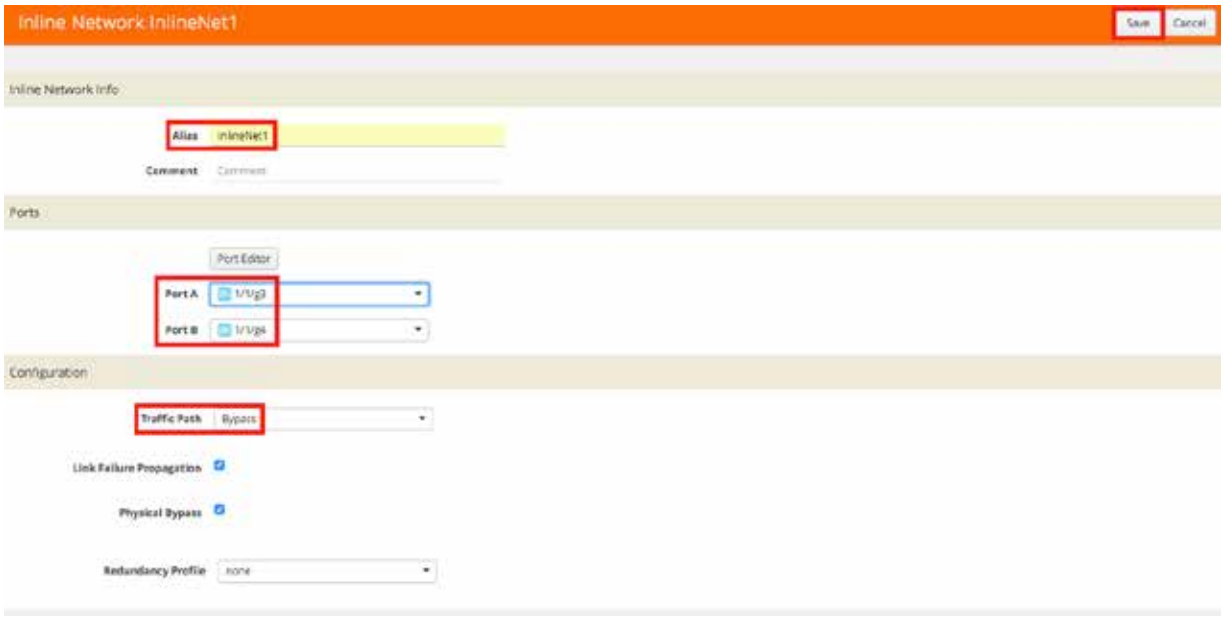


Figure 2-6: Inline Network Pair Configuration

Step 2: Configure the Inline Network Group

To configure the inline network group, do the following:

1. In GigaVUE-FM, select **Inline Bypass > Inline Network Groups**.
2. Click **New**.
3. In the **Alias** field, type an alias that represents the inline network group. For example, `PaloAlto-A_NGroup`.
4. Click the **Inline Network** field and either select from the drop-down list as shown in Figure 2-7 or start typing any portion of the alias associated with Inline Network you want to add to the Inline Network Group.

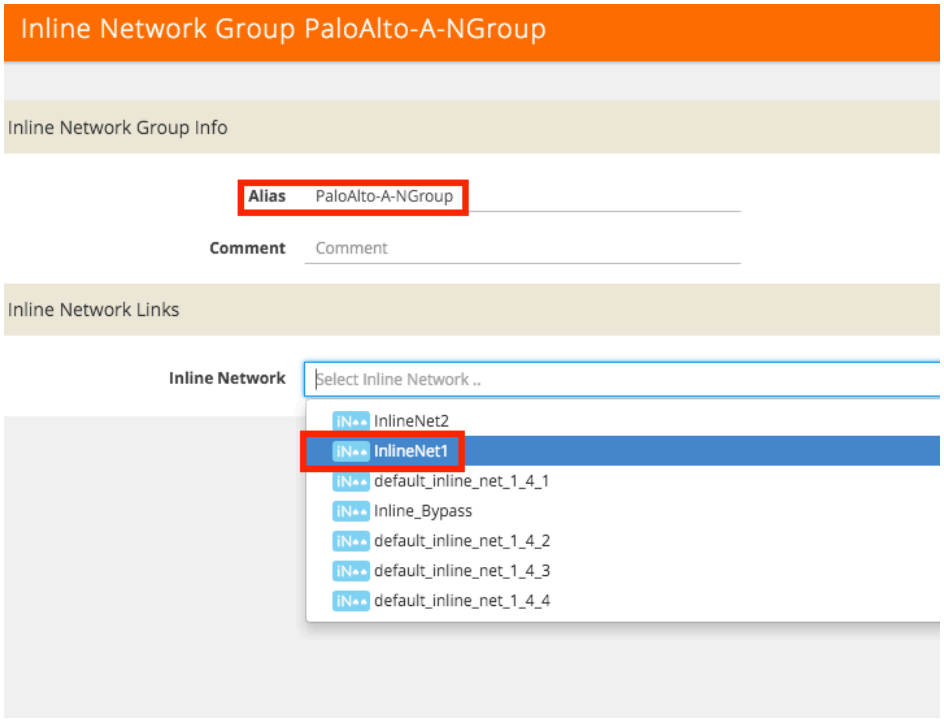


Figure 2-7: Inline Network Selection

5. 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

6. Click **Save** when you are done.

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

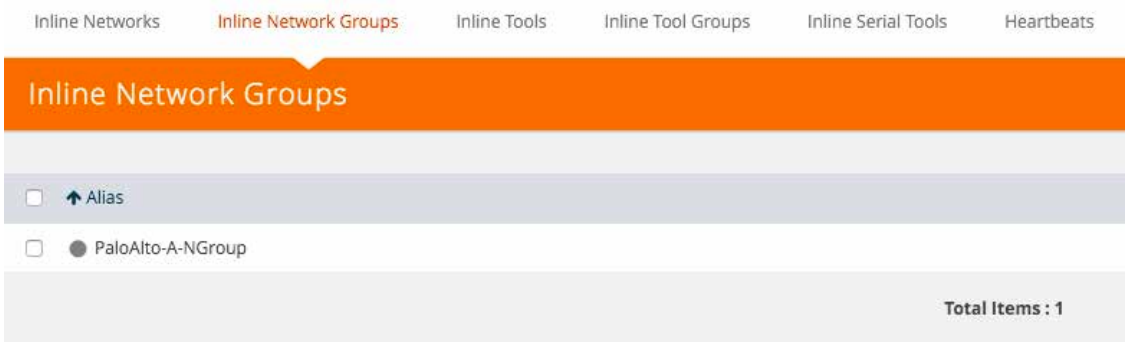


Figure 2-9: Finished list of Inline Network Groups

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

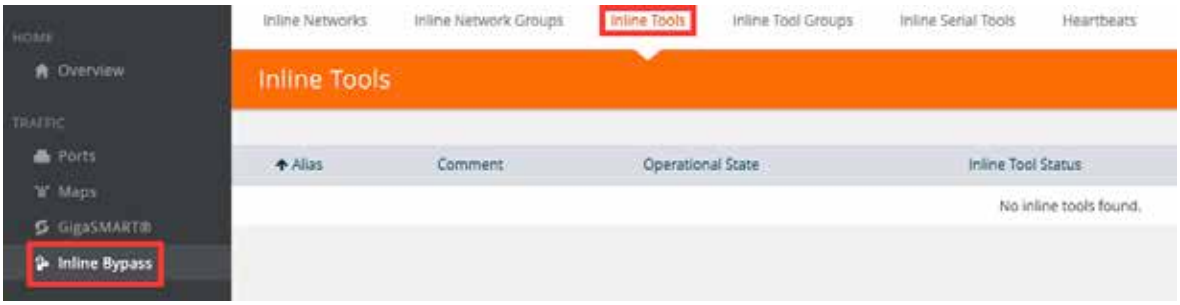


Figure 2-10: Navigating to the Inline Tools page

2. Click **New** to open the configuration page for inline tools.

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:
   - For **Port A**, specify the port that corresponds to Side A in the network diagram.
   - 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. Leave the default setting for the remaining configuration options.

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

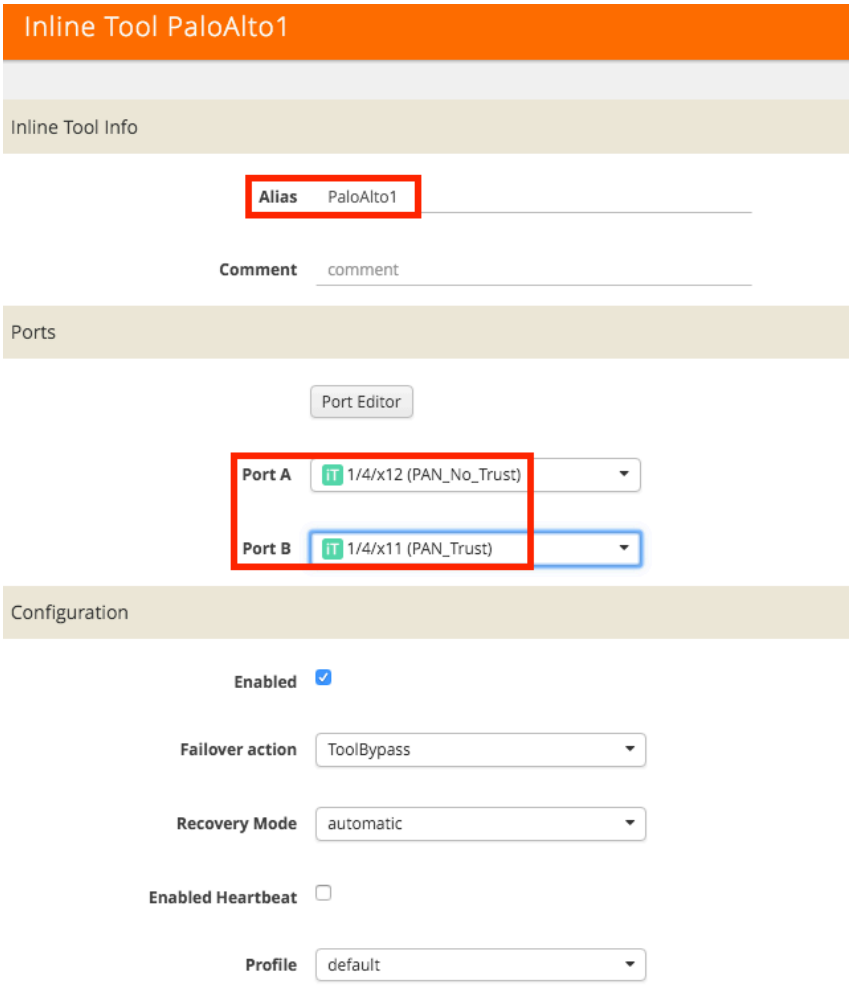


Figure 2-11: Inline Tool Pair Configuration

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. 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 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, `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.

   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:
   - 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-bdstip** for **Hash**.

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

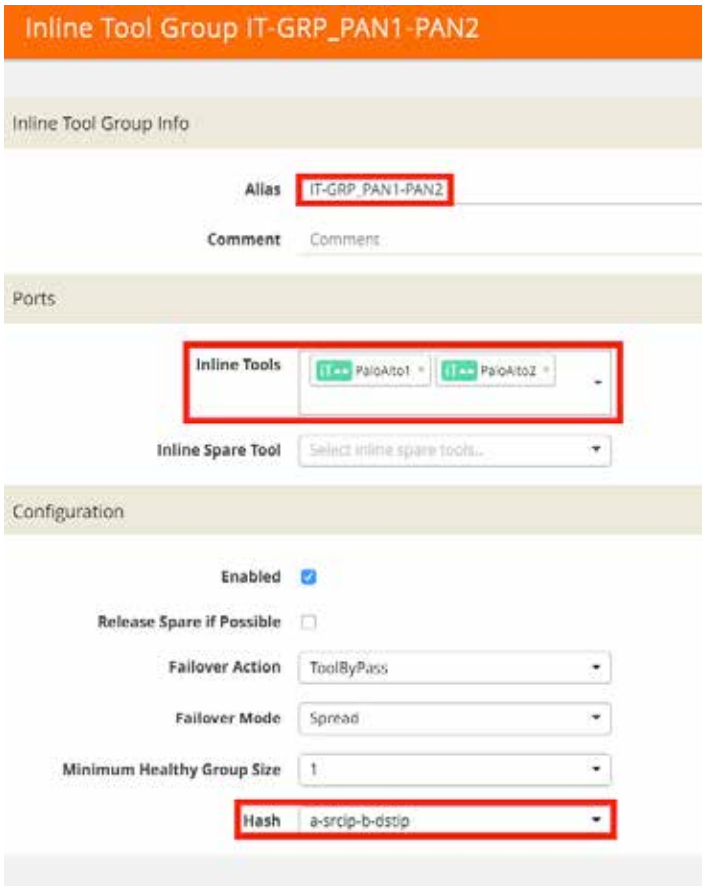


Figure 2-12: Inline Tool Group Configuration

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: 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 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 GigaVUE-FM, navigate 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 Bypass.
4. In the Map, set the **Source** and **Destination** fields as follows:
   - Set **Source** to the inline network group that you created in *Step 2: Configure the Inline Network Group*.
   - Set **Destination** to the inline tool groups that you created in *Step 4: Configure the Inline Tool Group*.
5. In Map Rules, click **Add a Rule**.
6. Specify the following for the rule:
   a. Click in the Condition search field for the rule and select **ip4Proto** from the drop-down list.
   b. Select **Pass**. (This is the default.)
   c. Select **Bi Directional**.
   d. In the **Ipv4 Protocol** drop-down list, select **IGMP**.

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

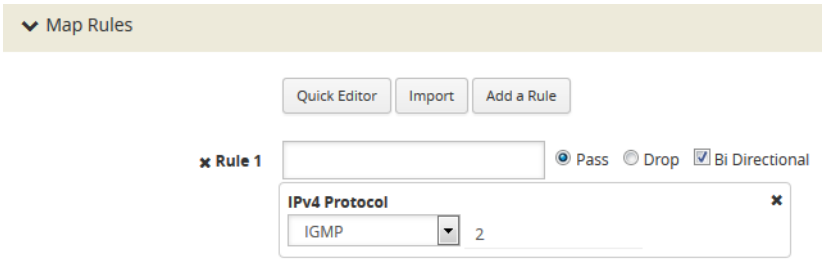


Figure 2-13: Rule for Inline Tool Flow Map

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:

1. In GigaVUE-FM, go 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*. For example, `Collector-ING_ITG`.
   - Set **Type** to Inline.
   - Set **Sub Type** to Collector.
   - Set **Traffic Path** to Normal.
3. In Map Source and Destination, set the **Source** and **Destination** to the same source and destination as the first rule map configured in *Step 1: Configure the Traffic Flow Map with an Inline Bypass Rule*.

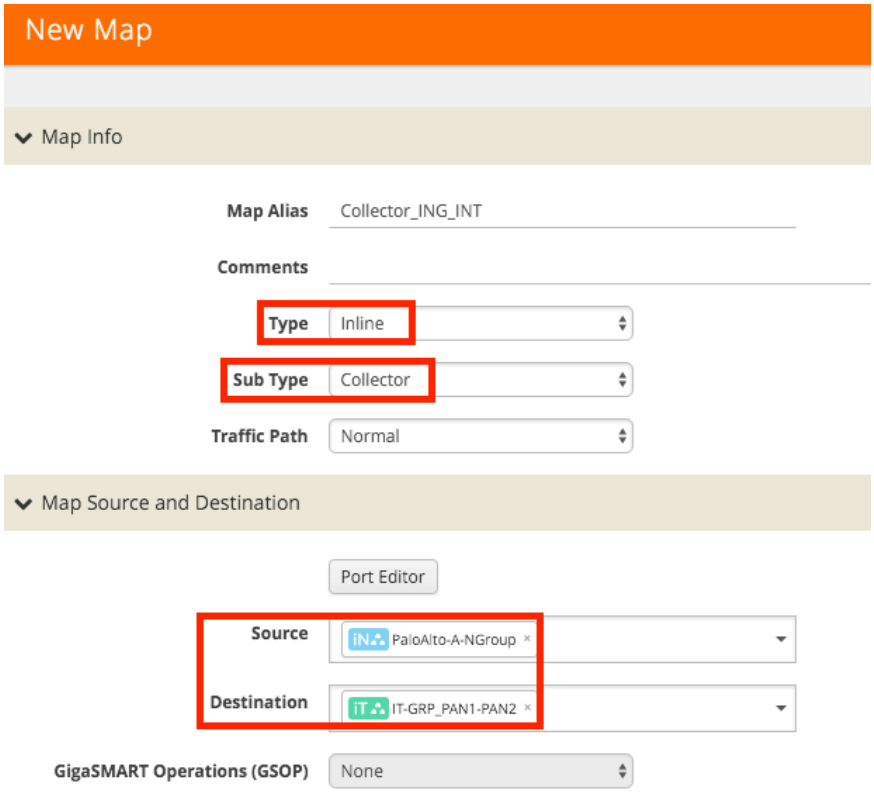


Figure 2-14: Configuration for Collector Map

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 **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**.

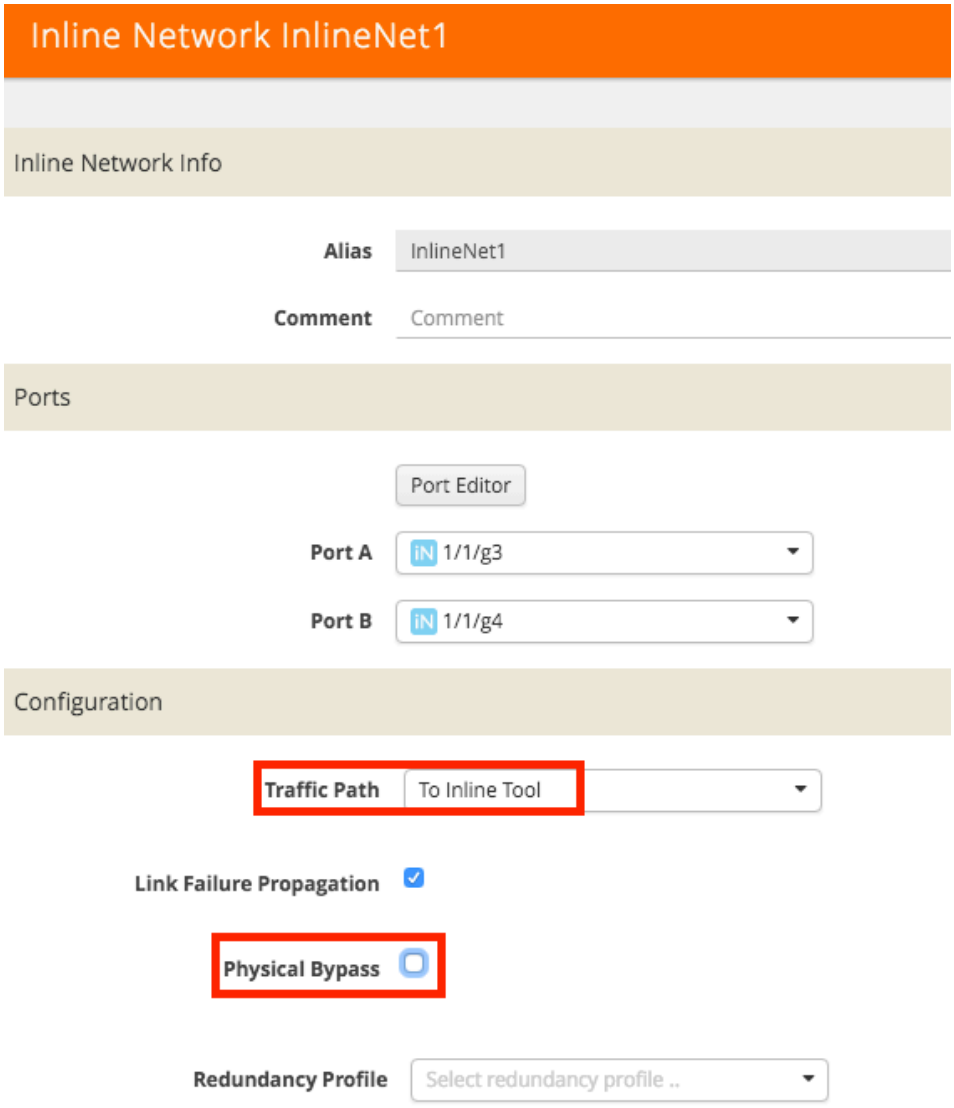


Figure 2-15: Inline Network Traffic Path Changed to Inline Tool, Physical Bypass Unchecked

4. Click **Save**.

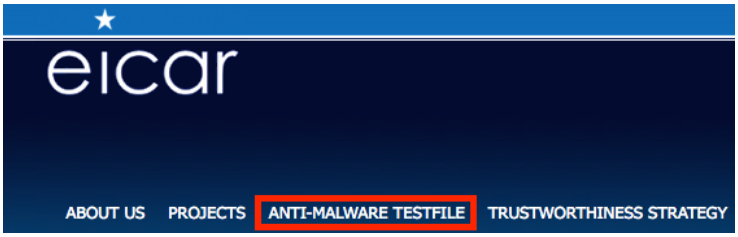
5. Repeat step 3 and step 4 for each inline network in the inline network group.

Testing the Functionality of the Palo Alto Networks NGFW

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.

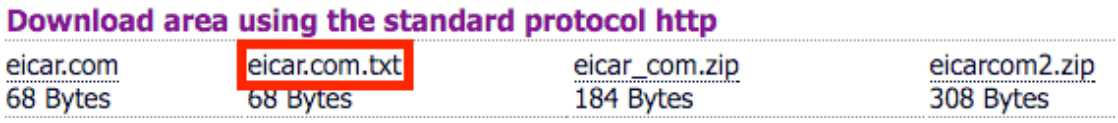
To test the functionality, do the following:

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

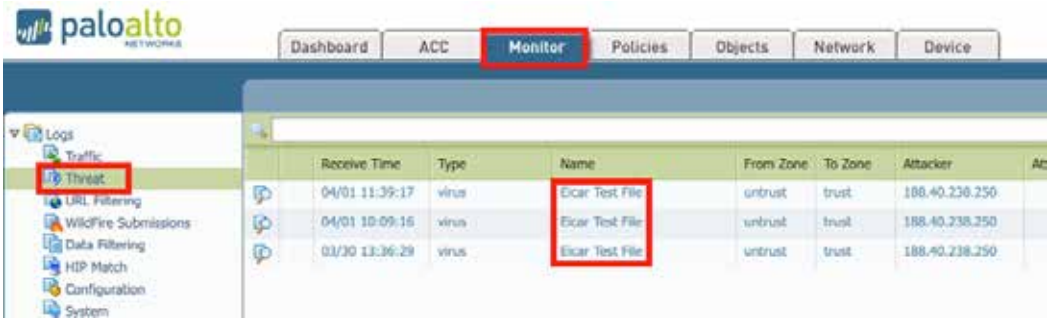
4. Scroll down and click on eicar.com.txt under the standard protocol http.



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

You can also view Threat Log statistics from the Palo Alto Networks GUI to confirm it is blocking.

6. Go to the Monitor tab. Under Logs click Threat. It should look similar to the following figure:



3 Summary and Conclusions

The previous chapters 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 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 Palo Alto Networks 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.

See Inside Your Network™

4063-02
11/16