

TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Gigamon

Contents

Partner Information	3
Use Cases for Integration into Palo Alto Networks Next Generation Security Operating Platform	3
Palo Alto Networks Products for Integration	4
Integration Benefits	4
Integration Diagram	5
Before You Begin	6
Overview	6
Palo Alto Networks Configuration	6
Palo Alto Networks NGFW Configuration: Virtual Wire	6
Partner Product Configuration	9
GigaVUE-HC2 Configuration: Inline Network and Inline Tool Groups	9
Configuring the GigaVUE-HC2 Inline Network and Inline Tools	10
Configuring the Inline Traffic Flow Maps	18
Troubleshooting	22
Summary and Conclusions	23
How To Get Help	23

Partner Information

	Partner information
Date	June 28 th , 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.

	0
hernet1/17	
ap	×
ap :	
rtual Wire	
ayer2	
ayer3 ggregate Ethernet	
	OK Cancel
	themet1/17 ap iA Artual Wire ayer2 ayer3 kggregate Ethernet

- 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.

Zone	0
Name trust	User Identification ACL
Log Setting None	Enable User Identification
Type Virtual Wire	Include List 🔺
Interfaces A	Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
	Add Delete Users from these addresses/subnets will be identified. Exclude List
+ Add Delete	Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Zone Protection	
Zone Protection Profile None	
Enable Packet Buffer Protection	Add Delete
	Users from these addresses/subnets will not be identified.
	OK Cancel

- 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.

Virtual	Wire		0
	Name	PAN-Inline	
	Interface1	ethernet1/1	-
	Interface2	ethernet1/2	-
	Tag Allowed	0-4094	
		Enter either Integers (e.g. 10) or ranges (100-200) separated	by
		Multicast Firewalling	
		Link State Pass Through	
		OK Cancel	

- 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

Security Policy Rule							0
General Source	User	Destination	Application	Service/URL Category	Actions	Usage	
Name Rule Type	all-traffic						
Description							
Tags							~
Group Rules By Tag	None						~
Audit Comment							
	Audit Com	ment Archive					
					(ОК	Cancel

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

٩											3 ite	ms 🔿 🗙
				Source								
	Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	all-traffic	none	interzone	any	any	any	any	any	any	any	any	Allow
2	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
3	interzone-default	none	interzone	any	any	any	any	any	any	any	any	🛇 Deny

- 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.

🧐 GigaVUE-FM	HC2-1-F08-33 (H Series) Last synced at 2	2019-04-17 14:43:52					Q	C	H ad	min • ?
номе	Inline Flows Inline Networks	Inline Network Groups Inline Too	ls Inline Tool Groups	Inline Serial Tools	Heartbeats	Redundancies				
✿ Overview Norkflows	Inline Flows							1 Resub	mit All Ne	w Edit
🚓 Node Topology	Search Device	STATUS STATISTICS								
House Hopology	 ► HC2-1-F08-33 ► Inline Network Bundle ■ Inline Network LAG ■ Inline Network ■ default_inline_net_1_3_4 									
Get started About										+

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.

- Inline Network
 default_inline_net_1_3_1
 default_inline_net_1_3_2
 default_inline_net_1_3_3
 default_inline_net_1_3_4
- 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**.

Elevible Inline Canva	Quick Port Ec		ОК	Close	Properties	OK	Cancal	
Flexible mine canva						Froperties	UK	cancer
NEW	Quick search					Configuration		
Flex Map								
ООВ Сору	1/1/x15	port alias	Network 🗘	Enable		Alias		
Search Device	1/1/x16	port alias	Network \$	Enable				
▼ HC2-1-F08-33	1/2/×1		. A Network	Enable		Comment		
Inline Network Bundle	172781	port alias	Tool					
	1/2/x2	port alias	Hybrid Stack	Enable		Port Editor		
Inline Network	1/2/x3	port alias	Circuit	Enable		Port A		
default_inline_net_1_3_1	1/2/x4	port aliar	Inline Tool	Enable		Select inline Network		*
<pre>default_inline_net_1_3_2</pre>		porcailas				Port B		
default_inline_net_1_3_3	1/2/x5	port alias	Network 🗘	Enable		Select inline Network		
Toline SSL APP	1/2/x6	port alias	Network \$	🔲 Enable		Traffic Path		
* Inline Tool	1/2/x7	port alias	Network \$	Enable		Bypass		
Tool1	1/2/29		Naturark	Enable	- 1	Link Failure Propagation		
Tool2	1/2/x8	port alias	Network	Enable				
Tool3	1/2/x9	port alias	Network \$	🔲 Enable				
Tool4	1/2/x10	port alias	Network 0	Enable				
Tool5 Tool5	1/2/x11	port alias	Network	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**.

HOME	Flexible Inline Canvas		Delete Solution Deploy Cancel
🕈 Overview	NEW	Delete P Clear Canvas Autofill other direction VLAN Table Settings	
Norkflows	Flex Map OOB Copy		
TRAFFIC	Search Device		
E Ports	▼ HC1-F08-19		
₩ Maps	▼ Inline Network Bundle	Create an Inline Network	
GigaSMART®	• Inline Network LAG	Start with your existing inline network or create	
App Intelligence	- Inline Network		
Inline Bypass	default_inline_net_1_2_1		
Active Visibility	default_inline_net_1_2_2		
	• Inline SSL APP		
SYSTEM	• Inline Tool	Add a map	
III Chassis	• Inline Tool Group	Build your traffic flows with maps.	
Roles and Users	- Heartbeat		
♣ - Health	default		
Settings	• Negative Heartbeat		
SUPPORT	• Redundancy		
IE Logs	• IB Pathway	Choose a tool	
@ Debug	- GigaStream™ 🔂	Complete and deploy by choosing tools which you	
Get Started	• Ports		
About	Network		
O NOOde	▶ Tool		+
	 Hybrid 		-
**	 Stack 		

- 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.
- Continue adding inline networks until all port pairs are in the Inline Network field as shown in Figure 2-8.

HOME	Flexible Inline Canvas		Properties OK Cancel
A Overview	NEW	Delete Clear Canvas Autofill other direction VLAN Table Settings	Configuration
Node Topology	Flex Map OOB Copy		PaloAlto-A_NGroup
TRAFFIC	Search Device		Inline Networks
Ports Y Maps GigaSMART® App Intelligence inline Bypass Cative Visibility System Chassis Active System Reference	HC1-F08-19 Inline Network Bundle Inline Network LAG Inline Network LAG Inline Network default_inline_net_1_2_1 default_inline_net_1_2_2 Inline SSL APP Inline Tool Inline Tool Inline Tool Inline Tool Inline Tool	1 Create an Inline Network Start with your existing inline network or create a new inline network. 2 Add a map Build your traffic flows with maps.	default_inline_net_1.2_1
Ar Health Constant Constant Constant Constant Constant Constant Constant Constant About	real robat default · Negative Heartbeat · Redundancy · IB Pathway · GigaStream ^{***} · Ports · Network · Tool · Hybrid	Choose a tool Complete and deploy by choosing tools which you want to send your traffic to.	3

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.

НОМЕ	Flexible Inline Canvas					
f Overview	NEW	🛍 Delete	🖉 Clear Canvas	Autofill other direct	ion VLAN Table	Settings
🎀 Workflows	Flex Map					
🛔 Node Topology	ООВ Сору					
	Search Device					
📕 Ports	▼ HC1-F08-19					
\Iſ Maps	✓ Inline Network Bundle			4	reate an Inline	e Network
	▼ PaloAlto-A_NGroup			s	art with your exist	ing inline netw
	default_inline_net_1_2_2			a	new inline networ	к.
App Intelligence	default_inline_net_1_2_1					
🏠 Inline Bypass						

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**.

🛞 GigaVUE-FM		t 2019-04-17 15:13:51				Q 📣 C' 🗄 admin• 0
	Flexible Inline Canva	Quick Port	Editor		OK Close	Properties OK Cancel
	NEW	Ouick search				Configuration
	Flex Map					
	OOB Copy	1/1/x10	from_HC2_F08-06	Network 0	🗷 Enable	Alias
	Search Device	1/1/x11	PAN-1	Inline Tool 🔹	🗷 Enable	7//05
	 default_inline_net_1_2 default_inline_net_1_2 	1/1/x12	PAN-2	V Network	🗷 Enable	Comment
	- Inline Network LAG	1/2/x1	port alias	Tool Hybrid	Enable	Port Editor
	- Inline Network	1/2/x2	port alias	Stack Circuit	Enable	Port A
	Inline SSL APP Joline Tool	1/2/x3	port alias	Inline Network Inline Tool	Enable	No available inline tool ports +
	Inline Tool Group	1/2/x4	port alias	(Network 0)	Enable	Port B
	- Heartbeat	1/2/x5	port alias	Inline Network \$	Enable	No available inline tool ports
	default	1/2/x6	port alias	Inline Network \$	Enable	C Enabled
	Redundancy	1/2/x7	port alias	Inline Network \$	Enable	Failour action
	- IB Pathway	1/2/x8	port alias	Inline Network \$	Enable	Tool Burass
	 GigaStream™ 	1/3/g1	port alias	Inline Network	🗷 Enable	1000 59 100
	Ports Network	1/3/g2	port alias	Inline Network	🕏 Enable	Recovery Mode
	> Tool	1/3/g3	port alias	Network 0	Enable	automatic
	Hybrid	1/3/04	port allas	Network 1	Enable	Enable (Additional tags on the tool side)
	Stack Inline Network	1/2/45	port allas	Nictured A	C Crable	Flex Traffic Path
	Inline Tool	1/3/go	port alias		w enable	To Inline Tool

- 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.

oigaVUE-FM	HC1-F08-19 (H Series) Last synced at 201	9-04-17 15:13:51				Q 🦉	G	B	admin 👻	0
	Flexible Inline Canvas					Properties			ок с	Cancel
Overview Workflows Node Topology	NEW Flex Map OOB Copy	🛢 Delete 🖉 Clear Ca	invas 🗷 Autofill other di	rection VLAN Table • Settings		Alias PaloAlto1 Comment				-1
TRAFFIC Ports W Maps GigaSMART® App Intelligence Inline Bypass Active Visibility	Search Device • HC1-F08-19 • Inline Network Bundle • PaloAlto-A_NGroup • default_inline_net_1_2_2 • default_inline_net_1_2_1 • Inline Network LAG • Inline Network LAG		1	Create an Inline Network Start with your existing inline network or create a new inline network.		Comment Port Editor Port A IT 1/1/x11 Port B IT 1/1/x12				•
SYSTEM Chassis Roles and Users Health Settings	Inline SSL APP Inline SSL APP Inline Tool Inline Tool Inline Tool default Meantbeat		2	Add a map Build your traffic flows with maps.	-	Enabled Failover action Tool Bypass Recovery Mode automatic				•
support I Logs	Redundancy Redundancy IB Pathway GigaStream ¹⁰⁰ Ports Network Tool K Hybrid		3	Choose a tool Complete and deploy by choosing tools which you want to send your traffic to.	-	Inline tool sharing mode	s on the tool :	side)		•

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:

oigaVUE-FM	HC1-F08-19 (H Series) Last synced at 20	19-04-17 15:13:51				Q 🔎	G	B	admin 🕶	0
	Flexible Inline Canvas								ОК	Cancel
🔒 Overview	NEW	🗈 Delete 🛛 🝠 Clear Can	was 🗷 Autofill other d	irection VLAN Table Settings						1
ℵ Workflows ▲ Node Topology	Flex Map OOB Copy					Alias IT-GRP_PAN1-PAN2				
	Search Device	,			Π	Comment				
🚔 Ports	default_inline_net_1_2_1		4	Create an Inline Network		Inline Tools				
	- Inline Network LAG			Start with your existing inline network or create		select inline tools				-
	• Inline Network			a new inline network.	•	Tee PaloAlto1				
	- Inline SSL APP					Equal	•			
	- Inline Tool					Inline Spare Tool				
	PaloAlto1					select inline tools				
	• Inline Tool Group		2	Add a map		Enabled				
	Heartbeat default		2	Build your traffic flows with maps.	0	Release Spare if P	ossible			
Roles and Users	- Negative Heartbeat					Failover Action				
	- Redundancy					Tool Bypass				•
Settings	• IB Pathway					Failover Mode				
	 GigaStream™ 					Spread				•
	▼ Ports		3	Choose a tool		Minimum Healthy Grou	p Size			
	Network		5	Complete and deploy by choosing tools which you want to send your traffic to.		1				•
	▶ Tool					Harb				
	 Hybrid 					advanced				•
	Stack					the Real to Bash				_
	Inline Recoork					To Inline Tool				•

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.

🞯 GigaVUE-FM	HC1-F08-19 (H Series) Last synced at 201	9-04-17 15:13:51									Q	٩	C	B	admin	• 0
	Flexible Inline Canvas														ОК	Cancel
🔒 Overview	NEW	1 Delete	Clear Canvas	s 🗷 Autofill oth	her direction	VLAN Table	Settings				Aller					
Norkflows ▲ Node Topology	Flex Map OOB Copy										IT-GRP_PAN1-	PAN2				
	Search Device										Comment Comment					
📥 Ports	default_inline_net_1_2_1				Cr	eate an Inline	Network				Inline Teels					
	- Inline Network LAG			1	Sta	rt with your existing with your existing the second s	ng inline network	or create		B	PaloAlto1	×				•
	• Inline Network										Weighting					
	• Inline SSL APP										Equal		•			
Inline Bypass Active Visibility	Inline Tool PaloAlto1										Inline Spare To	ol				
	Inline Tool Group									_	select inline to	ols				_
	- Heartbeat			2	Ad	ld a map				3	Enabled					
🛄 Chassis	default			_	Bu	ild your traffic flow	vs with maps.		-		Release	Spare if Po	ssible			
Roles and Users	Negative Heartbeat									-	Failover Action					
	- Redundancy										Tool Bypass					•
Settings	IB Pathway									-	Eailouar Mada					
	 GigaStream™ 										Spread					•
	• Ports			2	Ch	ioose a tool										
	▶ Network			5	Co	mplete and deploy	y by choosing tool	s which you			Minimum Heal	thy Group	Size			•
	+ Tool				110	nic to send your en	onn. co.									
	▶ Hybrid										Advanced					•
	Stack															
	 Inline Network 										Flex Traffic Pat	:h				
~	Inline Tool										to mine tool					•

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.

oigaVUE-FM	HC1-F08-19 (H Series) Last synced at 201	9041715:13:51	Q	P	C	B	admin 🕶	0
	Flexible Inline Canvas				Delete S	olution	Deploy (Cancel
🔒 Overview	NEW	Delete / Clear Canvas & Autofil other direction VLAN Table & Settings						
🏞 Workflows	Flex Map	PaloAlto-A NGroup						
	OOB Copy	RX		Tx				
	Search Device							
international Ports	▼ HC1-F08-19							
	 Inline Network Bundle 							
	PaloAlto-A_NGroup							
	<pre>default_inline_net_1_2_2 default_inline_net_1_2_1</pre>							
	Inline Network LAG							
	Inline Network	Collector_1555542928						
	Inline SSL APP			┥				
	• Inline Tool	A			в			
Roles and Users	PaloAlto1			- 11				
A → Health	Inline Tool Group							
Settings	• Heartbeat							
	default							
	Negative Heartbeat							
	Redundancy							
	• IB Pathway							
About	• GigaStream™ 🔂							
	✓ Ports	Collector 1555	5542928					
	Network	TX COLLECTOR MA		Rx				
	▶ Tool			104	_			+

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.

Rules	
Add a Rule	
× Rule 1	← ● Pass ● Drop ■ Bi-directional
Rule Comment	
Comment	
IP Version	×
Version v4	

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.

oigaVUE-FM	HC1-F08-19 (H Series) Last synced at 201	+0417 15:13:51	Q 😃 (C 💾 admin- ?
	Flexible Inline Canvas			OK Cancel
🔒 Overview	NEW	Delete Clear Canvas Autofill other direction VLAN Table Settings	Configuration	
Node Topology	Flex Map OOB Copy	PaloAlto-A_NGroup	Alias	
	Search Device		Traffic-to-PAN	
Ports	HC1-F08-19 Inline Network Bundle		Comment Comment	
GigaSMART®	▼ PaloAlto-A_NGroup	Map_1555543270	Inline Network	Tool Side VLAN Tag
	 default_inline_net_1_2_2 default_inline_net_1_2_1 		default_inline_net_1_2_2	1-4000 (Default is set to auto)
Inline Bypass	Inline Network LAG		default_inline_net_1_2_1	1-4000 (Default is set to auto)
	- Inline Network	Collector 1555543113		
	• Inline SSL APP		Rules	
	• Inline Tool		Add a Rule	
▲ Roles and Users ♣ Health	Inline Tool Group IT-GRP_PAN1-PAN2		× Rule 1	
Settings	• Heartbeat		Rule Comment	
	default		Comment	
	Negative Heartbeat	Map	IP Version	×
	• Redundancy	(Version V4 +	
	• IB Pathway			
About	• GigaStream™ 🚺			
	✓ Ports	Collec		
	Network	TX		
	▶ Tool			

- 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.

ar		
PROJECTS	ANTI-MALWARE TESTFILE	TRUSTWORTHINESS STRATEGY
	PROJECTS	PROJECTS ANTI-MALWARE TESTFILE

3. Click the Download link

ABOUT US	PROJECTS	ANTI-MALWARE TESTFILE	TRUSTWO	RTHINESS ST
INTEN	IDED USE	YOU	ARE HERE	ANTI-MALV
DOWN	LOAD	IN	TENDE	D USE

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

Download area using the standard protocol http

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

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

Virus/Spyware Download Blocked

Download of the virus/spyware has been blocked in accordance

File name: eicar.com.txt

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.