

DEPLOYMENT GUIDE

Fortinet NGFW With Gigamon Inline



Table of Contents

Overview
Solution Overview
Use Case 1: Inline Bypass (Virtual Wire Pair) Mode
Deployment Requirements 5
Architecture Overview
Access Credentials
Use Case 2: Inline SSL Solution With FortiGate
Architecture Overview
Configurations
Configuring FortiGate NGFW: Virtual Wire Pair
Configuring FortiGate Virtual Wire Pair
The Following Steps Apply Only for Inline SSL Deployment 8
Configure Web-filter Profile
Configure Virtual Wire Policy
Configure Interfaces for Inside and Outside Zone
Configure Static Default Mode 10
Configure IPv4 Policy 11
Configuring GigaVUE-HC2: Inline Network and Inline Tool Groups 12
Configuring GigaVUE-HC2 Inline Network and Inline Tools 12
Configuring the Inline SSL App (Only for Inline SSL deployment)

Table of Contents (contd.)

	Configuring the Inline Traffic Flow Maps	21
	Changing Inline Network Traffic Path to Inline Tool	22
	Testing the Functionality of the FortiGate NGFWs	23
Su	Immary and Conclusions	25
Av	ailable Documentation	25
Dc	ocumentation Feedback	25
Сс	ontacting Gigamon Support	25
Сс	ontacting Fortinet Support	25

Overview

Fortinet's award-winning next-generation firewalls (NGFWs) provide highperformance, consolidated security for end-to-end protection across the entire network. Through awareness of applications, users, and content within network traffic, FortiGate NGFWs offer comprehensive protection against known and unknown threats (e.g., ransomware, malicious botnets, zero-day, and encrypted malware). They offer scalable throughput of advanced security services, flexible network interfaces, and performance based on Fortinet's powerful security processors. The FortiOS operating system ensures superior price, performance, and security efficacy.

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 Fortinet 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 FortiGate and Gigamon together has the following benefits:

Traffic distribution for load sharing

Improves the scalability of inline security by distributing the traffic across multiple FortiGate NGFW appliances, allowing them to share the load and inspect more traffic.

Agile deployment

Adds, removes, and/or upgrades FortiGate NGFW appliances without disrupting network traffic; converting FortiGate NGFW appliances from out-of-band monitoring to inline inspection on the fly without rewiring.

Offload SSL Decryption

Offloading SSL decryption to the Gigamon solution has proven to be high performance and increased overall efficiency of the tools.

Use Case 1: Inline Bypass (Virtual Wire Pair) Mode

Customers may need multiple FortiGate NGFW appliances to scale to the volume of traffic generated on their network. When the aggregate traffic exceeds the capacity of any single FortiGate 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 among the remaining members, thereby ensuring availability of the security functions provided by the Fortinet 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.

Solution Overview

The solution tested and described in this guide is based on a standard active inline network and tool deployment where two or more Fortinet 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 a FortiGate appliance.

This section covers the following:

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



Deployment Requirements

The Gigamon plus Fortinet NGFW solution consists of the following:

- GigaVUE-HC2 chassis with GigaVUE-OS 5.7.00 software, one PRT-HC0-X24, and one TAP-HC0-G100C0 (a BPS-HC0 line card can also be used). One SMT-HC0 Gigasmart card with inline SSL License (for Inline SSL only).
- GigaVUE-FM version 5.7 software for GigaVUE-HC2 GUI configuration.
- Two FortiGate NGFW appliances. This includes the following:
 - FortiOS version 5.4.5

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 a FortiGate NGFW appliance. 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. This section presents the combined solution.



Figure 1-1: Gigamon Inline Bypass with FortiGate NGFW.

Notice in **Figure 1-1** that there is a sidedness to the architecture because data flows to and from Side A, where 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 Fortinet devices of the inline tool group.

Access Credentials

The default access credentials for the Gigamon GigaVUE-FM and FortiGate NGFW are as follows. Gigamon GigaVUE-FM access defaults:

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

FortiGate NGFW access defaults:

- Username: admin
- Password: leaveblank
- Default management IP address: 192.168.1.99

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 GigaVUE-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 GigaVUE-OS 5.0 release.

Use Case 2: Inline SSL Solution With FortiGate

Secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic introduces security blind spots and hides advanced threats leading to a surge in threat. Enabling SSL inspection on the security tools leads to degradation in performance and consumption of intensive CPU. GigaSECURE Inline SSL solution can be deployed to offload processor-intensive decryption functions from security tools such as an NGFW to increase threat inspection effectiveness. The underlaying solution is a validated design that allows for integrating TLS decryption/encryption services and performs the inline deep packet inspection and remediation on the decrypted traffic using the FortiGate NGFW.

Gigamon Inline SSL solution requires the connected inline tools to preserve the Layer 2 information. This allows to switch the traffic back to the appropriate inline network pair on which the traffic was received. When a firewall/Layer 3 router that performs NAT/PAT or an explicit proxy is connected as an inline tool, the MAC/IP/Layer 4 information gets swapped based on the policy configured on the inline tool. This traffic, when received back at Gigamon with swapped layer information, is not correlated and the sessions are not established to process further.

The solution outlined here mitigates the above limitation. After performing SSL/TLS decryption, the decrypted traffic from Gigamon hits Fortinet's virtual wire interfaces for deep packet inspection. FortiGate preserves the Layer 2 information in the virtual wire mode, once deep packet inspection is performed, the traffic loops back from the virtual wire interfaces and is reencrypted. The encrypted traffic is now forwarded back on the appropriate inline network pair to the connected FortiGate's routed interface to perform firewall, routing, and/or VPN functionality.

Architecture Overview

This use case illustrates deploying GigaVUE-HC2 device for SSL decryption and FortiGate firewall in virtual wire pair for inspection and in NAT/Route mode for routing the user's traffic to the internet, as illustrated in **Figure 2-1**.



Figure 2-1: Gigamon Inline Solution with FortiGate NGFW.

The topology shows two separate instances of FortiGate: one as an inline tool and the other as a firewall. However, in the validation process, both of these modes are configured on a single NGFW hardware. A pair of interfaces are configured for virtual wire mode and are connected to GigaVUE-HC2 as an inline tool. FortiGate's Layer3 interface, which is configured in NAT/Route mode to route traffic, is connected to Gigamon on the inline network pair.

Configurations

This chapter describes the configuration procedures for the GigaVUE-HC2 and FortiGate NGFW as an inline tool group solution through Gigamon's GigaVUE-FM. The procedures are organized as follows:

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

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

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

NOTE: This chapter assumes that you have connected the Fortinet appliances directly to GigaVUE-HC2 as shown in **Figure 1-1**. You should configure all GigaVUE-HC2 ports that connect the Fortinet 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 <u>Customer Portal</u>.

NOTE: This chapter describes how to configure the FortiGate NGFW in NAT Mode using Virtual Wire Pairs. The FortiGate NGFW could instead be configured in Transparent Mode if needed.

Configuring FortiGate NGFW: Virtual Wire Pair

The procedures described in this section apply to the highlighted area in the reference architecture diagram shown in Figure 3-1.





Configuring FortiGate Virtual Wire Pair

To configure the FortiGate NGFW Virtual Wire Pair, perform the following steps for each FortiGate appliance. You can skip these steps if the Virtual Wire Pairs you wish to use are already configured.

- 1. In the FortiGate GUI, go to **Network > Interfaces**.
- 2. Click Create New and choose Virtual Wire Pair from the drop-down list. Refer to Figure 2-2.

+ Network	~	246
Interfaces		A Edit
DNS	Interface	ew eut
Packet Capture	Zone	Y Name
SD-WAN	Virtual Wire	Pair ort1
SD-WAN Status Check	0	port2

Figure 2-2: Navigation to Virtual Wire Pair.

3. In the Name field, enter a name for the Virtual Wire Pair. Refer to Figure 2-3.

	Virtualivvire		
nterface Members	🖸 port3	×	
	o port4	×	
-	+		
/ildcard VLAN 🔘			

Figure 2-3: Creating the Virtual Wire Pair.

- 4. In the Interface Members box, click the plus (+) sign and choose the 2 ports you want to use.
- 5. Enable the **Wildcard VLAN** option if you are passing the traffic that is VLAN tagged. Click **OK**.
- 6. Repeat these steps on the next FortiGate NGFW.

The Following Steps Apply Only for Inline SSL Deployment

Configure Web-filter Profile

To configure web-filter profile, perform the following steps:

- 1. In the FortiGate GUI, Security Profiles > Web Filter Profile.
- 2. Click the plus (+) sign to create a new web-filter profile.
- 3. Enter web-filter profile alias name UTM-profile.
- 4. Block social media and networking category.
- 5. Click OK to create new web-filter profile.

 root New Web Filter Profile FortiView Name UTM-Profile Write a comment	FortiGate 500E FG5H0E3	917900061	20	?
FortiView Pottoverk Name UTM-Profile Write a comment Policy & Objects Security Profiles Security Profiles Proxy Options SSL/SSH Inspection Web Rating Overrides Web Profile Overrides Web Profile Overrides	🎝 root 💌	New Web Filter Profile		
ICAP Servers Image: Allow tyles User & Device Image: Block WiFi & Switch Controller Image: Block Image: Block tyles Image: Block tyles	 ▲ FortView > ♦ FortView > ♦ Network > ♦ Solicy & Objects > ■ Security Profiles ♥ Web Filter ↑ ♥ Method Profile ♥ Web Filter ♥ Method Profile ♥ Web Rating Overrides ₩ Web Profile Overrides ₩ User & Device > ♥ WiFi & Switch Controller > 	New Web Filter Profile Name UTM-Profile Comments Write a comment		

Configure Virtual Wire Policy

To configure virtual wire policy, perform the following steps:

- 1. In the FortiGate GUI, go to Policy & Objects > IPv4 Virtual Wire Policy.
- 2. Click create new and select the direction (port5 \rightarrow port6).
- 3. Enter policy name Alias Policy1.
- 4. Click + to filter the source IP address.
- 5. Click + to filter the destination IP address.
- 6. Click + to filter the traffic with destined TCP ports.
- 7. Click on web filter and select web-filter profile UTM-Profile.
- 8. Click OK to create the policy.

← → C 🔺 Not se	ecure http	₩.//10.115.89.160/ng/firev	all/policy/policy/virtual-wire/edi	t/?vdom=root				☆	
FortiGate 500E	FG5H0E3	917900061						1	
👌 root	•	New Policy							
FortiView	> ^	N. COLOR							
🕂 Network	>	Name	Vwire-Policy1						
System	>	Virtual Wire Pair	port5						
Policy & Objects	~	Source	I all	×					
IPv4 Policy		Destination Address	🕒 all	×					
IPv4 Virtual Wire Pair	*	Schedule	always	•					
Policy		Service	ALL	×					
Explicit Proxy Policy		Action	✓ ACCEPT Ø DENY ₽	LEARN					
IPv4 Access Control Li	st	C IL D CL							
IPv4 DoS Policy		Security Profiles							
Addresses		Web Filter	UTM-Profile	•					
Internet Service Datab	oase	ICAP C	Q Search	+					
Services		Proxy Options	WEB UTM-Profile						
Schedules		SSL/SSH Inspection C	MEB default						
Virtual IPs		Logging Options	web monitor-all						
IP Pools		Log Allowed Traffic	O Security Events All Session	ons					

Configure Interfaces for Inside and Outside Zone

To configure the interfaces for inside and outside zone, perform the following steps:

1. In the FortiGate GUI, go to **Network > Interfaces**.

- 2. Select **port3 → Edit**, configure Interface alias name as Inside_zone.
- 3. Configure IP address as 172.16.6.1 and subnet mask as 255.255.255.0.

FortiGate 500E FG5	HOE39	17900061	?1	?
💩 root	•	Edit Interface		
FortiView Vetwork Interfaces Explicit Proxy WAN LLB WAN Status Check WAN LLB Profes	> ☆	Interface Nameport3 (70:4C:A5:45:C0:98)Alias		
Static Routes Policy Routes RIP OSPF BGP Multicast		Address Addressing mode Manual DHCP Dedicated to FortiSwitch IP/Network Mask. 172.16.6.1/255.255.255.0 Restrict Access Administrative Access MITTPS PING FMG-Access CAPWAP SSH SNMP RADIUS Accounting		
System Solary & Objects Solary Profiles User & Device WiFi & Switch Controller Int Log & Report Monitor	> > > > > >	C DHCP Server Networked Devices Device Detection Admission Control Security Mode None Miscellaneous Sen Outgoing Compactings to Botted Sites Dirable Dir		
0		Scan Outgoing Connections to Bother Sites Disable Block Monitor OK Cancel Untitled - Paint		

- 4. Select **port9 → Edit**, configure Interface alias name as outside_zone.
- 5. Configure IP address as 192.168.50.3 and subnet mask as 255.255.255.0.

👌 root	•	Edit Interface	
FortiView	>		
+ Network	~	Interface Name porty (70:4C-35:45:C0:9E)	
Interfaces	습	Allas Outside_zone	
Explicit Proxy		Lins Status Up o	
WAN LLB		Yerual Domain root	
WAN Status Check		Role 🚯 LAN 👻	
WAN LLB Rules			
Static Routes		Address	
Policy Routes		Addressing mode Manual DHCP Dedicated to FortiSwitch	
RIP		IP/Network Mask 192.168.50.3/255.255.255.0	
OSPF		Restrict Access	
BGP		Administrative Access @ HTTPS @ PING EMG-Access CAPWAP SSH	
Multicast		SNMP RADIUS Accounting	
System	>	DHCPServer	
Policy & Objects	>	Networked Devices	
Security Profiles	>		
Luser & Device	>		
TWIFI & Switch Controller	>	Admission Control	
Log & Report	>	Security Mode	
C Monitor	>	Miscellaneous	
		Scan Outgoing Connections to Botnet Sites Disable Block Monitor	
0		OK	

Configure Static Default Route

To configure the static default route, perform the following steps:

- 1. In the FortiGate GUI, go to **Network > Static Routes**.
- 2. Create new, enter destination address as 0.0.0.0 and subnet mask as 0.0.0.0.
- 3. Select the device as port9 (Outside_zone).
- 4. Enter gateway IP as 192.168.50.2 and click OK to create default route.

a root	•	New Static Route	
FortiView	>		
+ Network Interfaces	~	Destination U	Submet Named Address Internet Service 0.0.0.0/0.0.0 Image: Construct Service Image: Construct Service
Explicit Proxy		Gateway	192.168.50.2
WAN LLB		Administrative Distance ()	10
WAN Status Check		Comments	// 0/255
WAN LLB Rules		Status	C Enabled O Disabled
Static Routes	☆	Advanced Options	
Policy Routes		-	
RIP			OK Cancel
OSPF			
BGP			
Multicast			
System	>		
Policy & Objects	>		
Security Profiles	>		
🚨 User & Device	>		
奈 WiFi & Switch Controller	>		
Log & Report	>		
C Monitor	>		

Configure IPv4 Policy

To configure IPv4 policy, perform the following steps:

- 1. In the FortiGate GUI, go to **Policy & Objects > IPv4 Policy**.
- 2. Click New \rightarrow enter policy Alias as IPv4-Policy.
- 3. Select **port3** as Incoming interface from the drop-down menu.
- 4. Select **port9** as outgoing interface from the drop-down menu.
- 5. Click + to filter the source IP address.
- 6. Click + to filter the destination IP address.
- 7. Click + to filter the traffic with destined TCP ports.
- 8. Select Action as Accept and click OK to create the policy.

FortiGate 500E FG5H0	3917900061	11 ? [] admin
👌 root	New Policy	
FortiView FortiView FortiView FortiView System Policy & Objects FortiPolicy Explicit Proxy Policy Explicit Proxy Policy IPv4 Access Control List Ibv6 Policy	Name IPV4-Policy Incoming Interface	
Addresses Internet Service Database Services Schedules Virtual IPs IP Pools	NAT O Security Profiles Web Filter ICAP SSL/SSH Inspection	
Traffic Shapers Traffic Shaping Policy ▲ Security Profiles > ▲ User & Device > ❤ WiFi & Switch Controller >	Logging Options Log Allowed Traffic Security Events All Sessions Comments Write a comment Enable this policy C	
Log & Report >	• OK Cancel	

Configuring GigaVUE-HC2: 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:

- 1. Configuring the GigaVUE-HC2 Inline Network and Inline Tools
- 2. Configuring the Inline Traffic Flow Maps
- 3. Testing the Functionality of the FortiGate 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 GigaVUE-HC2 Inline Network and Inline Tools

This section describes 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 (if applicable)

Step 3: Configure the Inline Tools

NOTE: This section assumes all the ports to which the network devices are connected 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.

Step 1: Configuring the Inline Network Bypass Pair

- 1. Select the GigaVUE-HC2 from the list of physical nodes that GigaVUE-FM is managing.
- 2. Select Inline Bypass > Configuration Canvas.

oigaVUE-FM	HC2-F08-11 (H Series) Last synce	d at 2019-08-19 12:46:16			Q		3 8	admin - 🌣 🚱
HOME A Overview Workflows	Inline Flows Inline Netwo	rks Inline Network Groups	Inline Tools	Inline Tool Groups	Inline Serial Tools	Heartbeats	Redundancies	Configuration Canvas
🚓 Node Topology	Search Device	STATUS STATISTICS						TROUBLESHOOT
TRAFFIC Ports W Maps GigaSMART® Physical Intelligence	 +HC2-F08-11 Tinline Network Bundle Tinline Network LAG Tinline Network 							
🗭 Inline Bypass								
Active Visibility								
🛄 Chassis								
🚨 Roles and Users								
A → Health								
Settings								

Figure 2-5a: Inline Networks page.

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 2-5b**. 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, perform the following steps.

🚳 GigaVUE-FM	HC2-1 F08-33 (H Series) Last syr	nced at 2019-08-19 12:51:15		۵		C	💾 admin- 🌣 😯
номе	Flexible Inline Can						Delete Solution Deploy Cancel
🔒 🔒 Overview	NEW	🛱 Delete 🥒 Clear Canvas	↓ Import ①	◆ Export ① ☑ Autofill other direction VLAN Table	Settings		
₩ Workflows ▲ Node Topology	Flex Map OOB Copy						
TRAFFIC	Search Device						
 ➡ Ports ₩ Maps ☑ GigaSMART® ④ App Intelligence 	+ HC2-1-F08-33 Inline Network Bundle Inline Network LAG		1	Create an Inline Network Start with your actioning inline network or create a new inline network.		7	-
 Inline Bypass Active Visibility SYSTEM Chassic 	Inline Network default_inline_net default_inline_net default_inline_net default_inline_net		2	Add a map Build your traffic flows with maps.	5]	
Roles and Users	Inline Tool PAN1 Tool2 Tool3		3	Choose a tool Complete and deploy by choosing tools which you		8	1-

Figure 2-5b: Inline Network port pairs.

3. Click the plus (+) sign next to Inline Network. Refer to Figure 2-5b.



Figure 2-5b: Inline Networks sub default inline list.

- 4. On the new Properties 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.
 - Click **Port Editor** and choose desired network ports and make them **Inline Network** and check **Enable**.

				_		
	Quick Po	rt Editor		OK Close	Properties	OK Cancel
NEW	Quick search				Configuration	
Flex Map						
ООВ Сору	1/1/x15	port alias	Network \$	Enable	Allas	
	1/1/x16	port alias	Network +	Enable	mineveri	
- HC2-1-F08-33	1014			10 F	Comment	
Inline Network Bundle	1/2/x1	port alias	Tool	U Enable	Comment	
▼ Inline Network LAG	1/2/x2	port alias	Hybrid Stack	Enable	Port Editor	
	1/2/x3	port alias	Circuit	Enable	Port A	
default_inline_net_1_3_1		porcunos	Inline Network		Select inline Network	
default_inline_net_1_3_2	1/2/x4	port alias		Enable		
default_inline_net_1_3_3	1/2/x5	port alias	(Network 🗘	Enable	Select inline Network	
default_inline_net_1_3_4						
- Inline SSL APP	172730	port alias	Network ¥	Chable	Traffic Path	
- Inline Tool	1/2/x7	port alias	Network 🕴	Enable	Bypass	
Tool1	1/2/x8	port alias	Network +	Enable	Link Failure Propagation	
Tool2						
• Tool3	1/2/x9	port alias	Network \$	U Enable		
Tool4	1/2/x10	port alias	Network 0	🔲 Enable		
Tool5	1/2/x11	port alias	Network \$	Enable		
		ge and a second				

Figure 2-6a: Inline Network option under Quick Port Editor.

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 the B side as it is represented in the network topology diagram shown in **Figure 1-1**.

Important: It is essential for Side A and Side B of the GigaVUE-HC2 to match with Side A and Side B of the FortiGate NGFW. If they don't match, the traffic distribution or the Inline Tool Group will not work correctly. Retain the default selection in Traffic Path and Link Failure Propagation.

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

- Select **Physical Bypass** (if available). This minimizes packet loss during traffic map changes.
- 5. Leave Redundancy Profile to None.
- 6. Repeat these steps for all other network links.
- 7. Click Save.

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

8. Repeat these steps for all other network links (if applicable).

	Flexible Inline Canvas		Properties OK Cancel
	NEW	Delete	Configuration
N Workflows	Flex Map OOB Copy		Alias
	Search Device		InlineNet1
l Ports f Maps 5 GigaSMART®	HC1-F08-19 Inline Network Bundle Inline Network LAG Inline Network	1 Create an inline Network Start with your existing inline network or create a new inline network.	Comment Comment Port Editor
 App Intelligence Inline Bypass Active Visibility 	default_inline_net_1_2_1 default_inline_net_1_2_2		Port A
STEM Chassis Roles and Users	Inline SSL APP Inline Tool Inline Tool Group Heartbeat	2 Add a map Build your traffic flows with maps.	Traffic Path Byposs
Health Settings	default • Negative Heartbeat • Redundancy		Link Failure Propagation Physical Dypass Redundancy Profile none
≣ Logs ® Debug 9 Get Started	TIB Pathway GigaStream™ Orts	3 Choose a tool Complete and deploy by choosing tools which you want to send your traffic to.	
O About	Network Tool Hybrid Stark		

Figure 2-6b: Flexible Inline Canvas.

Step 2: Configuring the Inline Network Group

To configure the inline network group (if applicable), do the following:

1. In Flexible Inline Canvas, click the plus sign next to Inline Network Bundle.

	Flexible Inline Canvas		Delete Solution Deploy Cancel
	NEW	B Delete de Clear Canvas de Autofili other direction VLAN Table O Settings	
N Workflows & Node Topology	Flex Map OOB Copy		
	Search Device	>	
Ports	▼ HC1-F08-19		
W Maps	• Inline Network Bundle	Create an Inline Network	
GIPASMART®	Inline Network LAG	Start with your existing inline network or create	
	- Inline Network		
	default_inline_net_1_2_1		
	default_inline_net_1_2_2		
	• Inline SSL APP		
	- Inline Tool	Add a map	
	- Inline Tool Group	Build your traffic flows with maps.	
	• Heartbeat G		
	default		
	• Negative Heartbeat		
	• Redundancy		
	• IB Pathway	Choose a tool	
	- GigaStream™ G	5 Complete and deploy by choosing tools which you	
Get Started	· Ports		
D shout	Network		
	+ Tool		
	Hybrid	•	
	<< > Stack		

Figure 2-6c: Inline Network Bundle selection.

- 2. In the Alias field, type an alias that represents the inline network group. For example, FortiGate-A_NGroup.
- 3. From the Inline Network field, select the inline network 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.

HOME	Flexible Inline Canvas				Properties	OK Cancel
A Overview N Workflows	NEW Flex Map DDB Conv	🛢 Delete 🖉 Clear Canvas 🕏 Autofii	other direction VLAN Table Settings		Configuration	
A Nobe topology TRAFFIC Ports Maps GiggSSMART® App Intelligence Tollog Rynass	Search Device Search Device HC1-F08-19 Inline Network Bundle Inline Network LAG Inline Network Gefault_inline_net_1_2_1	1	Create an Inline Network Start with your outing inline network or create a new inline network.	-	Palokto A, NGroup Infline Networks Infline Gelaut, inline, net, 1, 2, 1	
Active Visibility SYSTEM Chassis Actives and Users Health	default_inline_net_1_2_2 Inline SSL APP Inline Tool Inline Tool Toline Tool Heartbeat default	2	Add a map build your traffic flows with maps.	-		
C settings SUPPORT H≣ Logs C Debug O Get Started O About	Negative Heartbaat Redundancy Redundancy GigaStream ¹¹⁴ Ports Network Note Yord Yord	3	Choose a tool Complete and depty by theorem to which you want to send your staffs to.			
javascript:void(0)					1	

Figure 2-7: Inline Network selection.

- 4. Continue adding inline networks until all port pairs are in the Inline Networks Field.
- 5. Click **OK** when done.

HOME	Flexible Inline Canvas						
🔒 Overview	NEW	🛍 Delete	🖉 Clear Canvas	Autofill other d	lirection	VLAN Table	Settings
🎦 Workflows	Flex Map						
🚓 Node Topology	ООВ Сору						
TRAFFIC	Search Device						
Ports	▼ HC1-F08-19						
\I ſ Maps	- Inline Network Bundle			4	Creat	te an Inline	Network
5 GigaSMART®	 PaloAlto-A_NGroup default_inline_net_1_2_2 				Start v a new	vith your existi inline network	ing inline netw <.
App Intelligence	default_inline_net_1_2_1						

Figure 2-8: Finished list of Inline Network groups.

Step 3: Configuring the Inline Tools

This section describes 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 **Configuring the Traffic Flow Map with a Pass All Rule**.

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

🞯 GigaVUE-FM	HC1-F08-19 (H Series) Last synced at 20	119-04-17 15:13:51			Q 🌓 C 🗒	admin • ?
HOME	Flexible Inline Canvas				Properties	OK Cancel
A Overview	NEW	🛢 Delete 🛷 Clear Canvas 🗹 Autofil oth	er direction VLAN Table 🔷 Settings		Configuration	
ド Workflows	Flex Map OOB Copy				Alias	
TRACCIC	Search Device				Alias	
Ports	 default_inline_net_1_2_2 default_inline_net_1_2_1 		Create an Inline Network	I	Comment	
GigaSMART®	Inline Network LAG Inline Network		Start with your existing inline network or create a new inline network.	. 8	Port Editor	
 Inline Bypass Active Visibility 	Inline SSL APP Inline Tool				No available inline tool ports	•
SYSTEM	Inline Tool Group Heartbeat default	2	Add a map Build your traffic flows with maps.	8	Port B No available inline tool ports	•
Roles and Users	Negative Heartbeat Redundancy				Enabled Failover action	
SUPPORT	GigaStream™		Channestan		Tool Bypass	•
i≣ Logs ® Debug	Ports Network Tool	3	Complete and deploy by choosing tools which you want to send your traffic to.	-	automatic	*
Get Started About	Hybrid Stack				Inline tool sharing mode Enable (Additional tags on the tool side)	
	Inline Network Inline Tool				Flex Traffic Path To Inline Tool	-

Figure 2-9: Inline Tool creation.

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

🛞 GigaVUE-FM		at 2019-04-17 15:13:5	1 E dia a			Q 🥂 C 💾 admin- 0
номе		QUICK POP	tEditor		OK Close	Properties OK Cancel
A Overview	NEW	Quick search				Configuration
🏷 Workflows	Flex Map	1				
👍 Node Topology	ООВ Сору	1/1/x10	from_HC2_F08-06	Network 0	Enable	Alias
TRAFFIC	Search Device	1/1/x11	PAN.1	Inline Tool		A035
🚔 Ports	default_inline_net_1_2	1/1/+12		A Naturck	@ Eastele	Comment
`₩ Maps	Ucraul_Initie_fiet_1_2	0.0412	PAN-2	Tool	er chable	
💋 GigaSMART®	Inline Network LAG	1/2/x1	port alias	Hybrid Stack	Enable	Port Editor
App Intelligence	* Inline SSL APP	1/2/x2	port alias	Circuit Inline Network	🗎 Enable	Port A
Inline Bypass	▼ Inline Tool	1/2/x3	port alias	Inline Tool	Cnable	No available inline tool ports +
	✓ Inline Tool Group	1/2/x4	port alias	Network 0	Enable	Port B
Chassis	+ Heartbeat	1/2/x5	port alias	Inline Network \$	💷 Enable	No available inline tool ports *
Roles and Users	default	1/2/x6	port alias	Inline Network \$	Enable	
Ar Health	* Redundancy	1/2/x7	port alias	Inline Network 0	Enable	Failover action
Settings	▼ IB Pathway	1/2/x8	port allas	[Inline Network \$	Enable	Tool Bypass •
SUPPORT	▼ GigaStream™	1/3/g1	port alias	Inline Network	🗷 Enable	Recovery Mode
i≣ Logs	Ports Network	1/3/g2	port alias	Inline Network \$	🗷 Enable	automatic
G Get Stagrad	+ Tool	1/3/g3	nort allar	Network 🗘 🕄	Enable	
About	+ Hybrid	10141	houranas		C Cashia	Enable (Additional tags on the tool side)
	Stack	173/g4	port alias	Network 🗘 🛛	w Enable	Flex Traffic Path
	Inline Network	1/3/g5	port alias	Network 0	Enable	To Inline Tool ·
<	runne rool	1000 C				

- 3. In the Alias field, type an alias that will help you remember which inline tool this inline tool pair represents. For example, FortiGate.
- 4. In the Ports section, specify the ports as follows:
 - vSide B in the network diagram

For the network diagram, refer to **Figure 1-1**.

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

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

	Flexible Inline Canvas				Properties	OK Cancel
	NEW	🛢 Delete 🥒 Clear Canvas 🗟 Autofill other	direction VLAN Table Settings		Allas	
N Workflows	Flex Map OOB Copy				Comment	
	Search Device	0			Comment	
	- HC1-F08-19		Create an Inline Network		Port Editor	
	• Inline Network Bundle	1	Start with your existing inline network or create	2	Port A	
S GigaSMART®	PaloAlto-A_NGroup		a new inline network.	• •	1/1/1/1	
	default_inline_net_1_2_2					
	Contraction Contraction				Port B	
	Inline Network LAG				1/1/x12	*
	• Inline Network				G. Fuchled	
	- Inline SSL APP	2	Add a map	8	2 Enabled	
	Inline Tool		build your trainic nows with maps.		Failover action	
	- Inline Tool Group				Tool Bypass	•
	• Heartbeat C				Bermery Mode	
🗘 Settings	derault					
	• Negative Heartbeat				automatic	•
	• Redundancy	3	Choose a tool		Inline tool sharing mode	
	- IB Pathway		Complete and deploy by choosing tools which you want to send your traffic to.		Enable (Additional tags on the tool side)	
	▼ GigaStream™				Flex Traffic Path	
	- Ports	0			To Inline Tool	•
	 Network Teal 				Regular Heartbeat	
	1001				Ø Enable	

Figure 2-10: Inline Tool Pair configuration.

- 7. Click Save.
- 8. Repeat steps 2 through 6 for all additional FortiGate NGFWs.

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 the 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 inline tool port links goes down.

Step 4: Configuring the Inline Tool Group

To configure the inline tool group, do the following:

1. In Flexible Inline Canvas, click the plus (+) sign next to Inline Tool Group. Refer to Figure 2-11.

🎯 GigaVUE-FM	HC1-F08-19 (H Series) Last synced at 20	19-04-17 15:13:51			Q 🧔	св	admin• ?
HOME	Flexible Inline Canvas						OK Cancel
Overview Workflows A Node Topology	NEW Flex Map OOB Copy	Delete Clear Canvas Autofill other	direction VLAN Table Ø Settings		Alias IT-GRP_PAN1-PAN2		
TRAFFIC Ports W Maps GigaSMART® App Intelligence Intelligence	Searth Device default_inline_net_1_2_1 Inline Network LAG Inline Network Inline SSL APP Inline Tool	1	Create an Inline Network Start with your oxisting inline network or create a new inline network.		Comment Comment Inline Tools Jelect inline tools Tree PaloAtto1 Equal	•	-
 Active Visibility System Chassis Roles and Users Health 	PaloAlto1 Inline Tool Group Heartbeat default Negative Heartbeat	2	Add a map Build your traffic flows with maps.	-	Inline Spare Tool Select Inline tools Enabled Release Spare If Possi Failover Action	ble	
 Settings SUPPORT i≣ Logs Debug 	Redundancy ID Pathway GigaStream ^(m) Ports Network	3	Choose a tool Complete and deploy by choosing tools which you want to send your traffic to.		Failover Mode Spread Minimum Healthy Group Siz	0	•
Get Started About	Tool Hybrid Stack Inline Network Inline Tool				Hash advanced Flex Traffic Path To Inline Tool		•

Figure 2-11: Inline Tool Group configuration.

- 2. In the Alias field, type an alias that describes the inline tool groups. For example, IT-GRP_FGT1-FGT2.
- 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.

- 4. In the Configuration section, do the following:
 - Select Enable.
 - Select Release Spare If Possible if applicable.
 - Retain the defaults for Failover Action, Failover Mode, and Minimum Healthy Group Size.
 - Select Advanced for Hash.
- 5. Click OK.

Configuring the Inline SSL App (Only for Inline SSL deployment)

The following steps are required starting 5.7 to configure Inline SSL App.

1. Under Configuration Canvas, click the plus (+) sign next to Inline SSL.



2. From the new pop-up window on the left, choose your SSL-app options.

	Flexible Inline Canvas						OK Cancel
	NEW	B Delete	# Clear Canwas	♦ Import ④ ♦ Export ④ 🛛 Autofill othe			
	Flex Map OOB Copy				Alias *	Alias	
narric 🏝 Ports	Search Device	3			03 engines	Select GS engines.	
	default_inline_net_1_3_1			Create an Inline Network	33L Monitor Mode	Disable - O	
GigaSMART®	inline_network_q5_q6			Start with your existing inline network or create a new inline network.	➤ Deployment Type		
Active Visibility	PAN-2				Deployment Type	Keychain Password Add new keys Inbound Outbound Hybrid	
	Inline Tool Group Inline SSL APP		2	Add a map Build your traffic frees with mans	✓ Advanced		
Roles and Users	• Key Store				> Configurations		
In Health In Settings	FmAuto-key-ssl-decrypt-app-df93 FmAuto-key-ssl-decrypt-app-Sa7f				> Traffic Path		
	Heartbeat default	·	3	Choose a tool	> Security Exceptions		
≣ Logs ⊪ Debug	• Negative Meartbeat			want to send your traffic to.	> Whitelist/Blacklist		
	Redundancy IB Pathway				> Policy Rules		
	• GigaStream***				> Network Access		
	Ports Network				> Decryption Port Mapping		
	• Tool				> Trust Store		
	Stack Inline Network				> TCP Settings		
	// Inline Tool				N		

- 3. Here are the options that can be chosen for basic setup.
 - Alias > Pick Any Name SSL-app.
 - From the **GS Engines** drop-down, choose the one available.
 - Leave SSL Monitor Mode to Disable.

- Click Keychain Password and add a password and select Auto login. Press OK.
- Choose **Deployment Type** to **Outbound**.
- Click Add New Keys.
 - Either Generate Certificate or Copy and Paste Private Key and Certificate.
- Under Advanced, open each option one by one and choose desired config.
- For Configurations, choose **Default Action** as **Decrypt** and other options as desired.
- Under Traffic Path, leave options at default.
- Under Security Exceptions, choose desired option. In this case, we choose Self Signed certificate to Decrypt.
- Add Whitelist/BlackList if needed.
- Under Policy Rules, click Add a Rule.
 - Pick Category > financial_services.
 - Add another rule Pick Category > health_and_medicine.
- Under Network Access, choose DHCP or IP Address.
- Under **Decryption Port Mapping**, click **Add Port Map** if you need to change port 443 to port 80 after decryption.
- For Trust Store, either choose to Append or Replace.
- Choose desired **TCP Settings** or leave them default.
- Under Miscellaneous (Global Settings), choose Min and Max SSL/TLS version and Connection Reset Action.
- Click OK.

The multiple screenshots below only highlight the options we selected for this scenario. These can vary based on different deployment requirements.

		ок	Cancel
Alias *	ssl-ann		
GS engines	an opp		
do engines			
SSL Monitor Mode	Disable 🗸		
✓ Deployment Type			
	Keychain Password Add new keys		
Deployment Type	🗋 Inbound 🧿 Outbound 🔿 Hybrid		
Certificate Authority			
	SigningFor Key Pair Alias Delete		
	Finality Fmauto-key-ssi-decrypt-app-dr93		
	secondary FmAuto-key-ssl-decrypt-app-5a7f		
✓ Advanced			
✓ Configurations			
Comgutations			
Default Action	O Decrypt ○ No Decrypt		
URL cache miss action	O Decrypt ○ No Decrypt ○ Defer		
Tool Fail Action	Bypass Tool O Drop Connection		
Tool bypass	Decrypted SSL Traffic 👔		
	No Decrypted SSL Trattic Non-SSL TCP Taffic		
	~		

Figure 2-12a: SSL app configuration.

	ок	Cancel
> Traffic Path		
✓ Security Exceptions		
Self signed certificate O Decrypt O Drop		
Invalid certificate O Decrypt O Drop		
Expired certificate O Decrypt O Drop		
Revocation CRL		
Revocation OCSP		
> Whitelist/Blacklist		
✓ Policy Rules		
Add a Rule		
Category X		
Value Interfaces * Rule 2 Decrypt No Decrypt 		
Category × Value health_and_medicine		
✓ Network Access		
Network access is used for getting URL categorization updates. Default mode uses a local DB.		

Figure 2-12b: SSL app configuration.

	ок	Cancel
Category A Value financial_services × Rule 2 Obcrypt No Decrypt Value kealth_and_medicine Category X 		
✓ Network Access		
Network access is used for getting URL categorization updates. Default mode uses a local DB. GigaSMART 1/4/e1 Network Access Configuration O None O DHCP O IP Address		
Decryption Port Mapping		
Priority User-defined Port Maps Add Port Map Delete All ID 1 X In Port 443 Out Port 80 Default Out Port Default Out Port		
> Trust Store		
> TCP Settings		

Figure 2-12c: SSL app 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 FortiGate tool group, allowing you to test the deployment functionality of the Fortinet appliances within the group. Perform the following steps:

Step 1: Configure the Traffic Flow Map with a Pass All 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 FortiGate appliances. Refer to **Testing the Functionality of the FortiGate NGFWs**, which describes the test procedure.

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

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

- 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 Inline Network group that was created earlier.



Figure 2-13: Configuration for Pass All Map.

2. If you want to send all traffic to IT-GRP_FGT1-FGT2, just **Drag and Drop** IT-GRP_FGT1-FGT2 Tool Group in the path of the Collector Map. The map can be renamed by clicking on it.

oigaVUE-FM	HC1-F08-19 (H Series) Last synced at 201	404-17 15:13:51	Q	4	C	в	admin 👻	8
	Flexible Inline Canvas				Delete S	olution	Deploy (Cancel
	NEW	Delete						
ℵ Workflows	Flex Map OOB Copy	Palolito-A_NGroup		Tx	1			
TRAFFIC Ports Ports GigaStAART® GigaStAART® GigaStAART® A drive Visibility SYSTEM Chassis A ctive Visibility SYSTEM Chassis A close and Users A close starts SUFFORT E Logs D Debug G Get Started A About	Search Device	A Collector:155563113 IT.GBP:PMN1:PM22 COLLCTOR:MMP COLLCTOR:MMP INAL TOO: GOOP ICGBP:PMN1:PM22 COLLCTOR:MMP	55543113	Tx	В			
	Network Tool		MAP	Rx				

NOTE: This example uses a Pass All rule so any traffic going through the Inline Network(s) will be sent to the FortiGate(s) for inspection. If you want to selectively send traffic to the FortiGate(s), then use Flex Map; refer to the User Guides and Technical Documentation in the Customer Portal.

3. Click **Deploy**. Leave Default option **Logical Bypass**.

Deploy	
Traffic Path during Deployment	
 Logical Bypass I C Keep As-is 	
	OK Cancel

For Inline SSL decryption, just drag and drop Inline SSL map on the canvas and make sure the Inline Tool/Tool Group fall within the Inline SSL app. Make sure to **click Deploy** after placing the inline SSL App.

	Flexible Inline Canvas			OK Cancel
	NEW	Delete	Configuration	
	Flex Map OOB Copy		Alias	
	Search Device	default_inline_net_1_3_2	default_inline_net_1_3_2	
	HC2-F08-11 Inline Network Bundle		Comment Comment	
W Maps GigaSMART®	Inline Network LAG		Port Editor	
App Intelligence Inline Bypass	Inline Network default_inline_net_1_3_1		Port A	
	default_inline_net_1_3_2 inline_network_q5_q6		Port B	
	Inline Tool PAN-2	Collection J359391065 353400 744-2 503400 Collection Jack Collection Jack Col	Traffic Path	
	Sutter_IT		To Inline Tool	
♣ Health ♦ Settings	Inline Tool Group Inline SSL APP		Link Failure Propagation Physical Bypass	
	ssi-app		Redundancy Profile	
	PmAuto-key-ssi-decrypt-app-df93	1//gt		
	FmAuto-key-ssl-decrypt-app-Sa7f	008 COV		
	default			
	Negative Heartbeat			
	Redundancy IB Pathway			
	• GigaStream'"			
	✓ Ports ♦ Network			

Changing 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).
- 3. In the Configuration section, make the following changes:
 - Set Traffic Path to Inline Tool.
 - Uncheck Physical Bypass.

НОМЕ	Flexible Inline Canvas			Properties ок	Cancel
🔒 Overview	NEW	🛢 Delete 🖉 Clear Canvas 🗹 Autofill o	ther direction VLAN Table • Settings	Configuration	
Node Topology	Flex Map OOB Copy			Alias	
TRAFFIC	Search Device	>		default_inline_net_1_2_2	
➡ Ports ₩ Maps SigaSMART®	HC1-F08-19 Inline Network Bundle PoloAlto-A_NGroup default_inline_net_1_2_2	1	Create an Inline Network Start with your existing inline network or create a new inline network.	Comment Comment Port Editor	
Active Visibility	default_inline_net_1_2_1 Inline Network LAG Inline Network			Port B	
SYSTEM Chassis Roles and Users Health	Inline SSL APP Inline Tool Inline Tool Group Inline Tool Group IT-GRP PAN1-PAN2	2	Add a map Build your traffic flows with maps.	Traffic Path To Inline Tool	
 Settings Support Elogs 	Heartbeat default Negative Heartbeat			Physical Bypass Redundancy Profile none	÷
 Debug Get Started About 	Kedundancy Kedundancy IB Pathway GigaStream™ O Ports Network	3	Choose a tool Complete and deploy by choosing tools which you want to send your traffic to.	-	

Figure 2-14: Inline Network traffic path changed to Inline tool, Physical Bypass unchecked.

- 4. Click OK.
- 5. Repeat step 3 and step 4 for each inline network in the inline network group (if applicable).

Testing the Functionality of the FortiGate NGFWs

One of the easiest ways to determine if the FortiGate NGFW is working properly is by attempting to access a website that should be blocked. In the example below, policy has been created to block access to the website foo.com.

- 1. From Policy & Objects, select IPv4 Virtual Wire Pair Policy.
- 2. Click **New** and create a policy as shown in **Figure 2-15**.

*	Favorites >	New Policy		
-	Dashboard >			
	FortiView >	Name ()	BlockFoo	
+	Network >	Virtual Wire Pair	port1 → port2	
0	System >		← →	
	Policy & Objects ~ IPv4 Policy	Source	all ×	
	Pv4 Virtual Wire Pair Policy 😭	Destination	⊒ all ×	
	IPv4 Access Control List IPv4 DoS Policy	Schedule	🐻 always 👻	
	Addresses	Service	₽ ALL ¥ +	
	Internet Service Database Services	Action	✓ ACCEPT Ø DENY ₱ LEARN	
	Schedules	Security Profiles		
	Virtual IPs	AntiVirus	•	
	IP Pools	Web Filter	C web default	- #
	Traffic Shapers	DNS Filter	0	
	Traffic Shaping Policy	Application Control		
۵	Security Profiles >	IPS	0	

Figure 2-15: Creating a new policy.

Edit Web Filter Profile					
Nama	default				
Name	Name deraut				
Comments	Write a co	mment	/ 0/255		
Inspection Mode	Flow-base	d			
C FortiGuard category	asced filter				
· Fortiguard category i	aseumter				
Static URL Filter					
URL Filter 💽					
	A				
+ Create / Edit	U Delete				
URL Type	Action	Status			
foo.com Simple	Ø Block	🗢 Enable			
Block malicious URLs discov	vered by FortiSa	andbox 🕥			
Web Content Filter		•			
Rating Options					
Allow websites when a ratin	g error occurs				
Rate URLs by domain and IP	Address				
			Apply		

Figure 2-16: Editing the web filter profile.

To test the functionality, go to a client computer that connects to the internet through the Gigamon HC2. Open a web browser and go to <u>http://.foo.com/</u>. You should get a block page similar to the following:



Figure 2-17: Block page.

Summary and Conclusions

The previous chapters described how to deploy Gigamon GigaVUE-HC2 bypass protection with FortiGate 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 FortiGate 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 offline due to an outage or planned maintenance.
- Traffic distribution to multiple FortiGate 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.

Available Documentation

Document	Summary		
GigaVUE-FM and GigaVUE-VM User's Guide	Provides an overview of the GigaVUE Fabric Manager, including initial configuration, upgrade instructions, setting up accounts, and configuring the GigaVUE nodes.		
GigaVUE-OS CLI User's Guide	Describes how to configure and operate the GigaVUE-OS software from the command line interface.		
GigaVUE-OS H-VUE™ User's Guide	Describes how to use the web-based H-VUE interface to configure and operate the GigaVUE H Series software.		

Documentation Feedback

To send feedback and report issues in our documentation, complete the short survey at the following link:

https://www.surveymonkey.com/r/gigamondocumentationfeedback

Contacting Gigamon Support

For issues with Gigamon products, refer to http://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information. You can also email Technical Support at support@gigamon.com. Refer also to the customer portal at https://gigamoncp.force.com/gigamoncp/.

Contacting Fortinet Support

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



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet*, FortiGate*, FortiCare* and FortiGare*, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results. Mohine metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and ther results may vary. Network variables, different network environments and other results. Mohine registered trademarks of their respective owners. Berformance and other results and internal by testing commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortine enternes a binding written contract; spinght by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version in shall be applicable.

April 20, 2021 4:05 AM

D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\April\957118 - Joint Value Prop\dg-FA-fortinet-ngfw-with-gigamon-inline-4202021\dg-FA-fortinet-ngfw-with-gigam