DEPLOYMENT GUIDE

Fortinet NGFW With Gigamon Inline

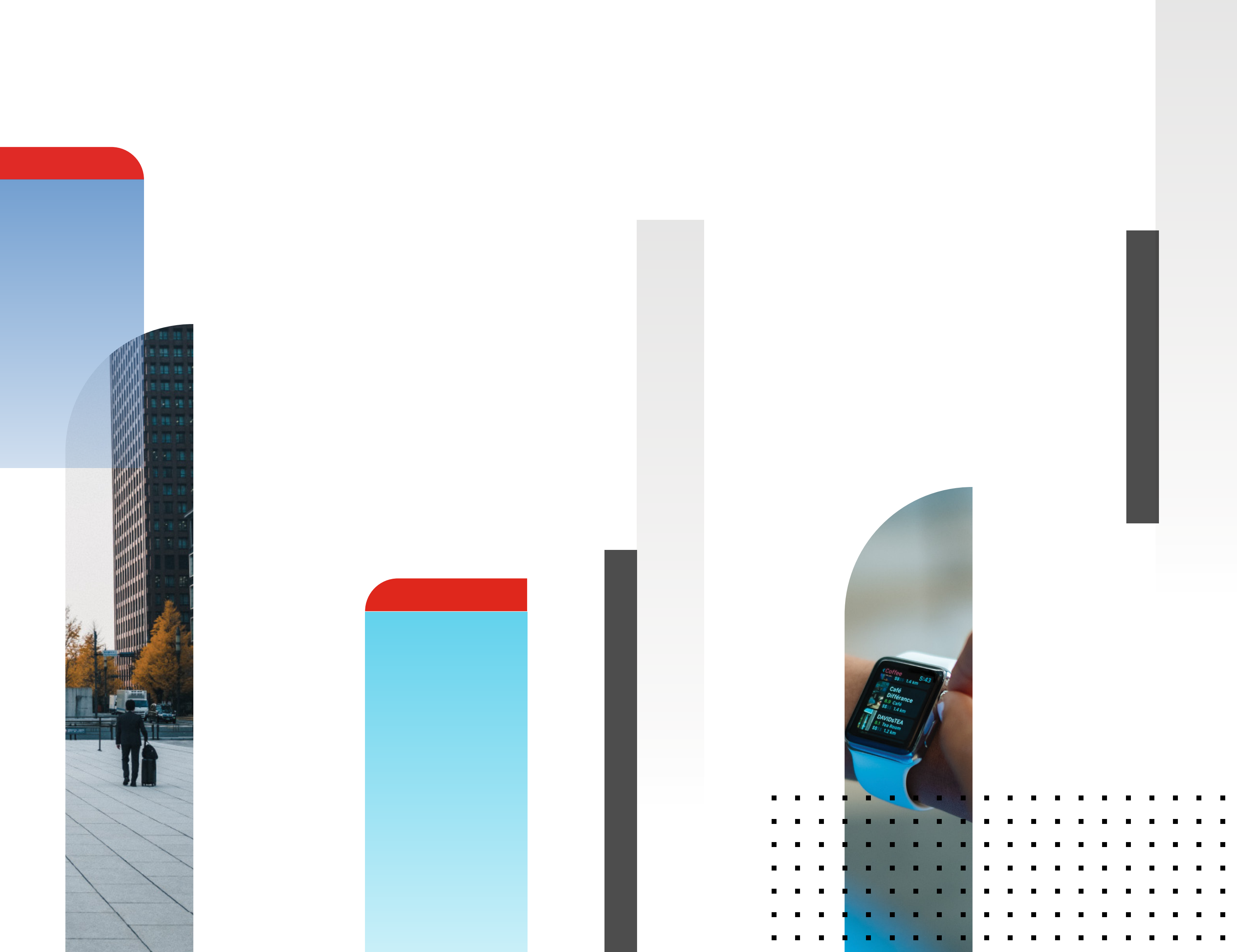


Table of Contents

Table of Contents (contd.)

Overview

Fortinet's award-winning next-generation firewalls (NGFWs) provide high-performance, 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.

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

FORTINET FABRIC-READY

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.

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.

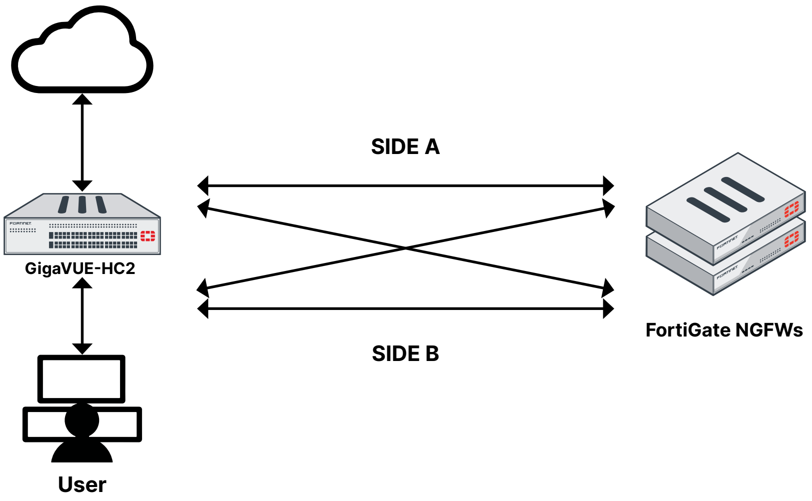


Figure 1-1: Gigamon Inline Bypass with FortiGate NGFW.

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.**

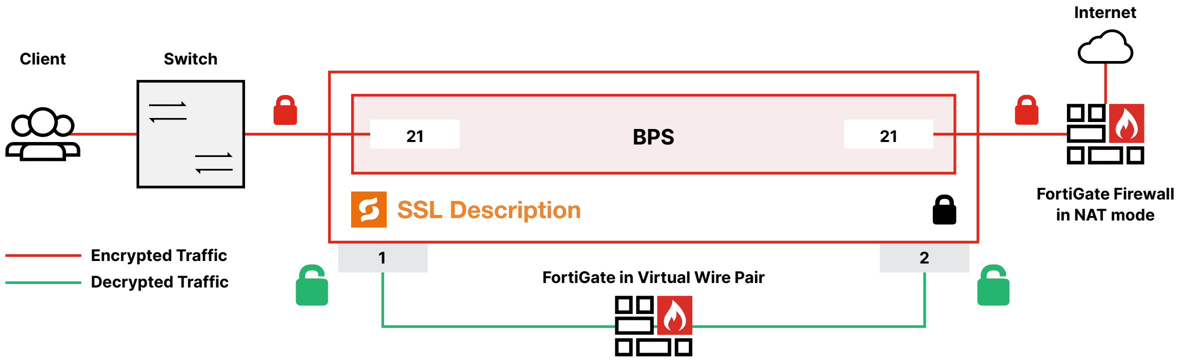


Figure 2-1: Gigamon Inline Solution with FortiGate NGFW.

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 Customer Portal.

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.**

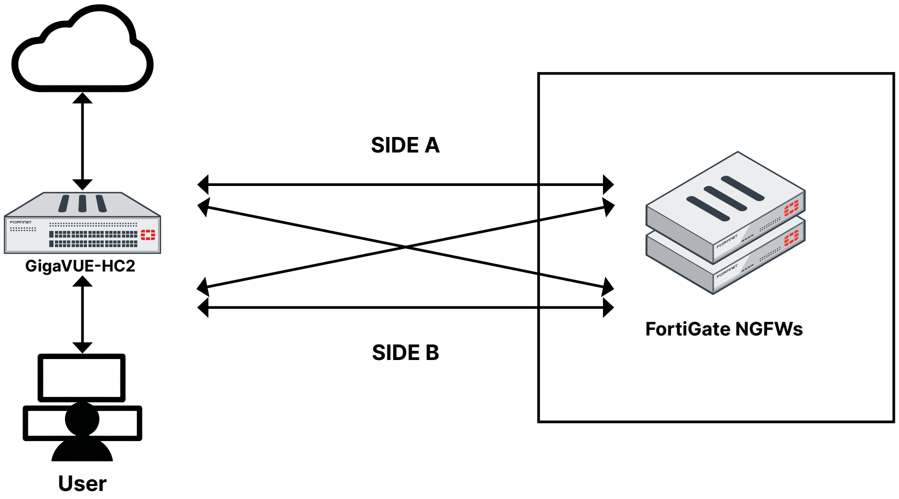


Figure 3-1: FortiGate NGFW.

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**.

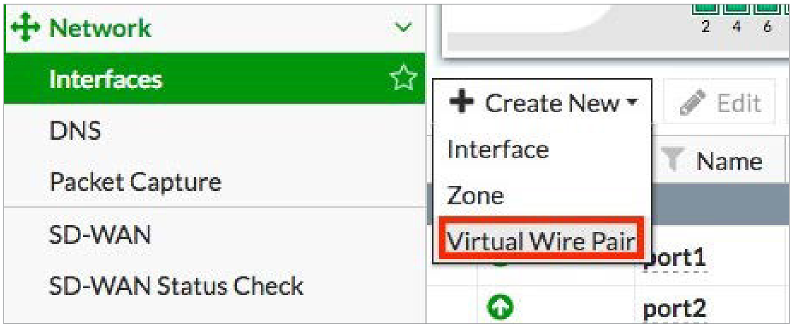
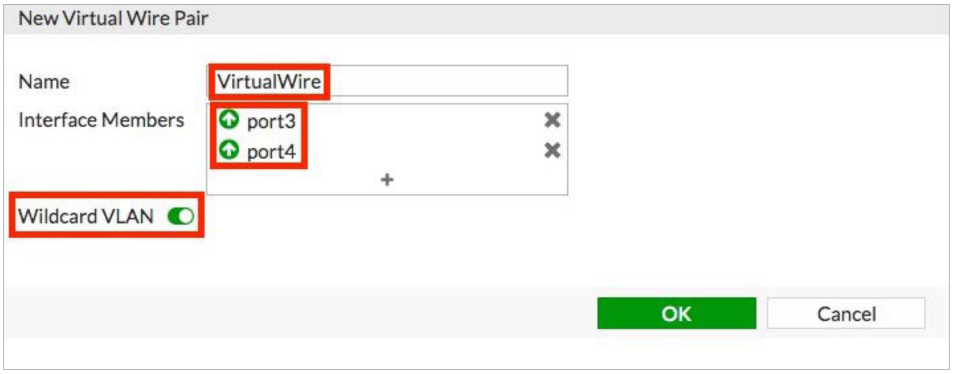


Figure 2-2: Navigation to Virtual Wire Pair.

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



New Virtual Wire Pair

Name VirtualWire

Interface Members port3, port4

Wildcard VLAN ●

Figure 2-3: Creating the Virtual Wire Pair.

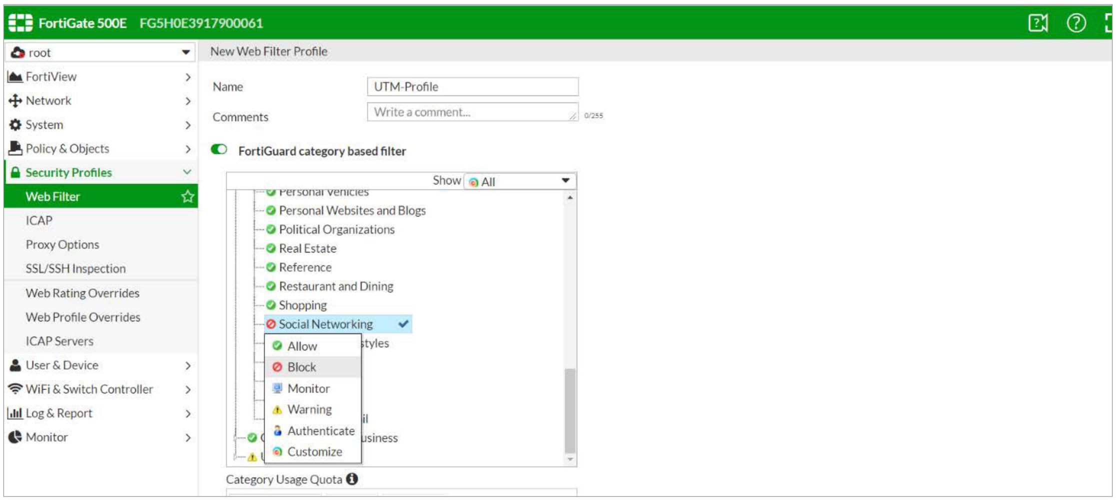
4. In the **Interface Members** box, click the plus (+) sign and choose the 2 ports you want to use.
5. Enable the **Wildcard VLAN** option if you are passing the traffic that is VLAN tagged. Click **OK**.
6. Repeat these steps on the next FortiGate NGFW.

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.



New Web Filter Profile

Name: UTM-Profile

Comments: Write a comment... 0/255

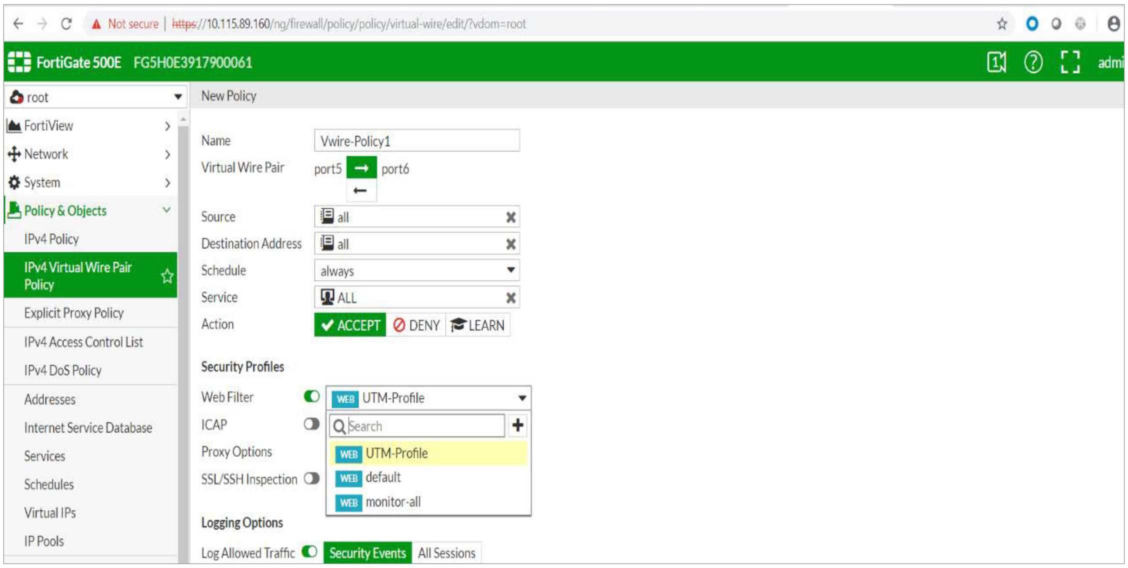
FortiGuard category based filter

Social Networking: Block

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 → 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.



New Policy

Name: Vwire-Policy1

Virtual Wire Pair: port5 → port6

Source: all

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Security Profiles

Web Filter: UTM-Profile

ICAP

Proxy Options

SSL/SSH Inspection

Logging Options

Log Allowed Traffic: Security Events

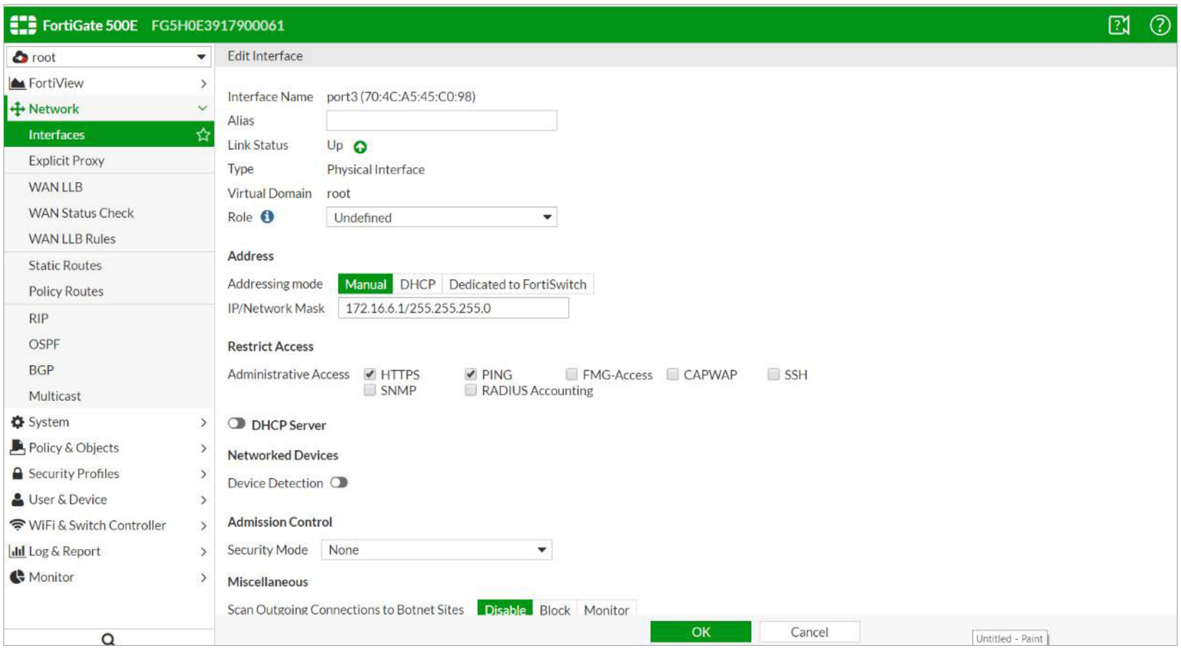
Configure Interfaces for Inside and Outside Zone

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.



Edit Interface

Interface Name port3 (70:4C:A5:45:C0:98)
Alias
Link Status Up
Type Physical Interface
Virtual Domain root
Role Undefined

Address

Addressing mode Manual DHCP Dedicated to FortiSwitch
IP/Network Mask 172.16.6.1/255.255.255.0

Restrict Access

Administrative Access ☑ HTTPS ☑ PING □ FMG-Access □ CAPWAP □ SSH □ SNMP □ RADIUS Accounting

DHCP Server

Networked Devices

Device Detection

Admission Control

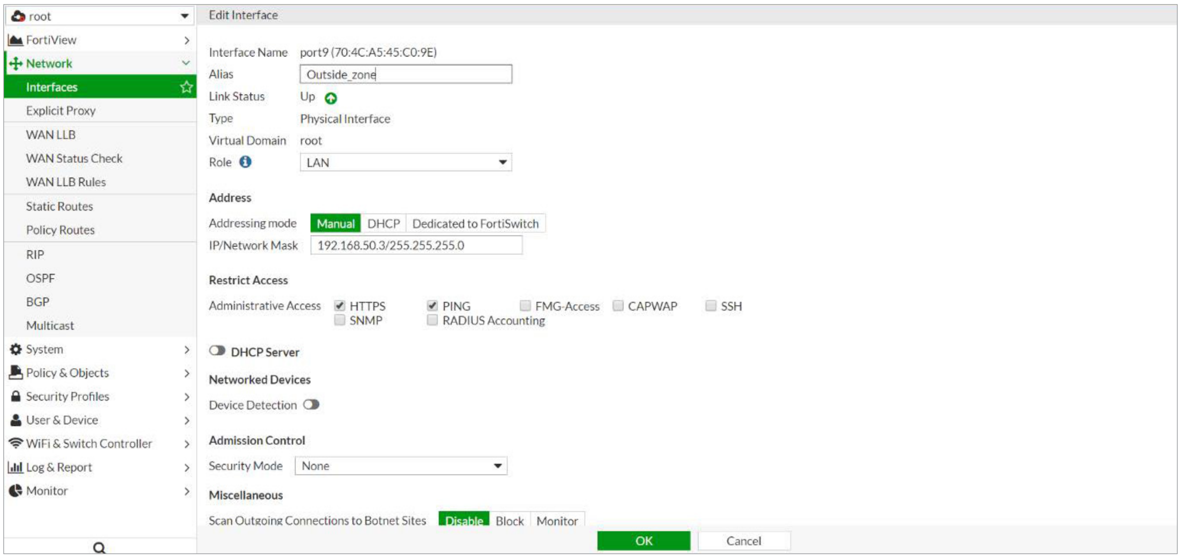
Security Mode None

Miscellaneous

Scan Outgoing Connections to Botnet Sites Disable Block Monitor

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.



Edit Interface

Interface Name port9 (70:4C:A5:45:C0:9E)
Alias Outside_zone
Link Status Up
Type Physical Interface
Virtual Domain root
Role LAN

Address

Addressing mode Manual DHCP Dedicated to FortiSwitch
IP/Network Mask 192.168.50.3/255.255.255.0

Restrict Access

Administrative Access ☑ HTTPS ☑ PING □ FMG-Access □ CAPWAP □ SSH □ SNMP □ RADIUS Accounting

DHCP Server

Networked Devices

Device Detection

Admission Control

Security Mode None

Miscellaneous

Scan Outgoing Connections to Botnet Sites Disable Block Monitor

Configure Static Default Route

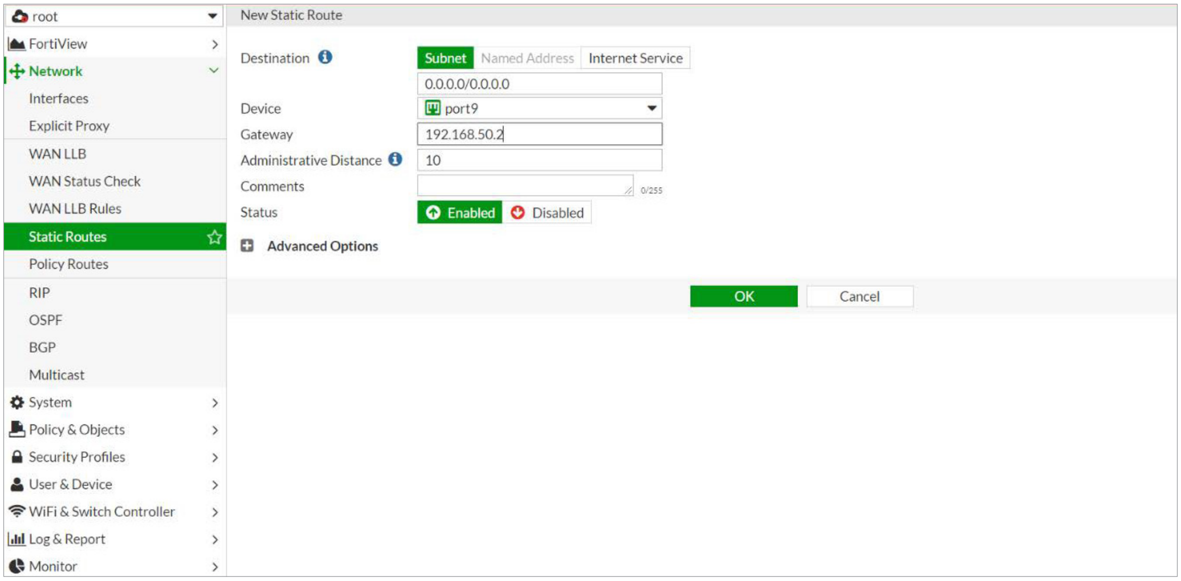
To configure the static default route, perform the following steps:

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.



New Static Route

Destination: Subnet

0.0.0.0/0.0.0.0

Device: port9

Gateway: 192.168.50.2

Administrative Distance: 10

Comments: 0/255

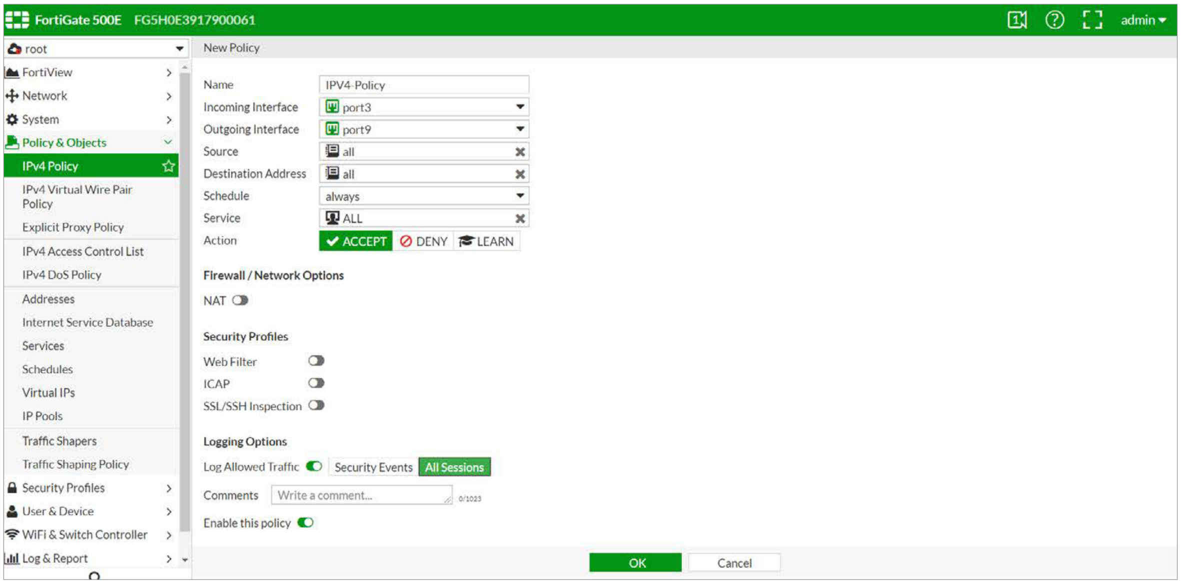
Status: Enabled

Advanced Options

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 → 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.



New Policy

Name: IPV4-Policy

Incoming Interface: port3

Outgoing Interface: port9

Source: all

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Firewall / Network Options

NAT

Security Profiles

Web Filter

ICAP

SSL/SSH Inspection

Logging Options

Log Allowed Traffic: All Sessions

Comments: Write a comment... 0/1023

Enable this policy

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**.

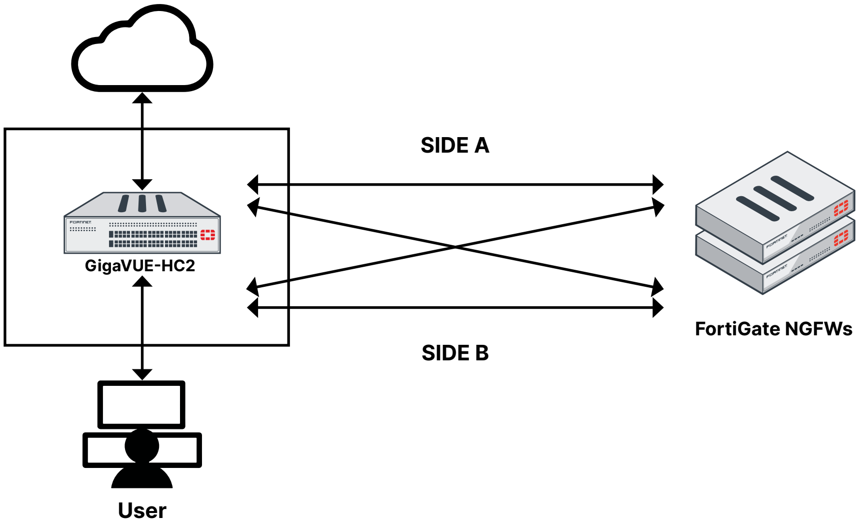


Figure 2-4: Gigamon GigaVUE-HC2 configurations.

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**.

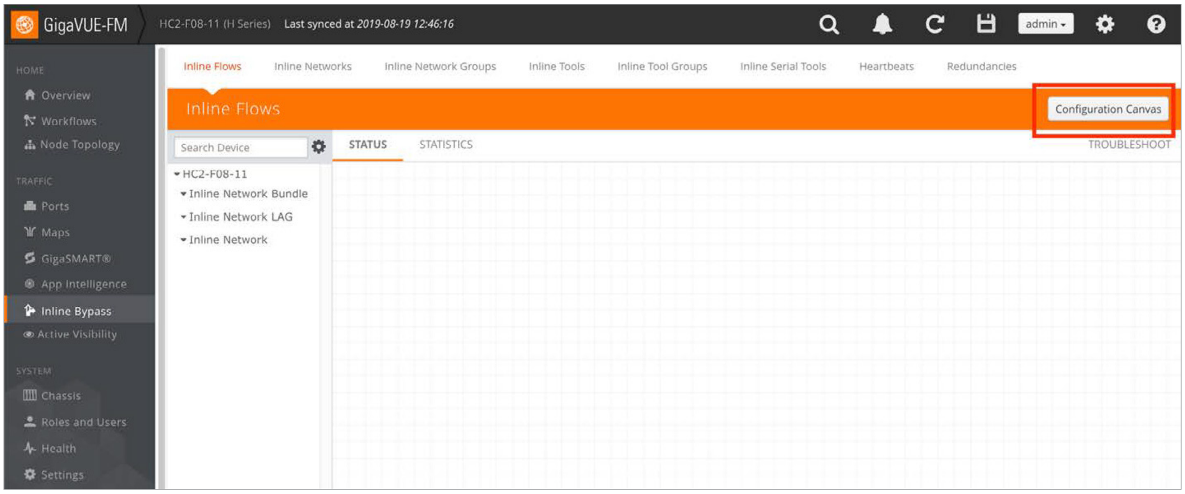


Figure 2-5a: Inline Networks page.

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.

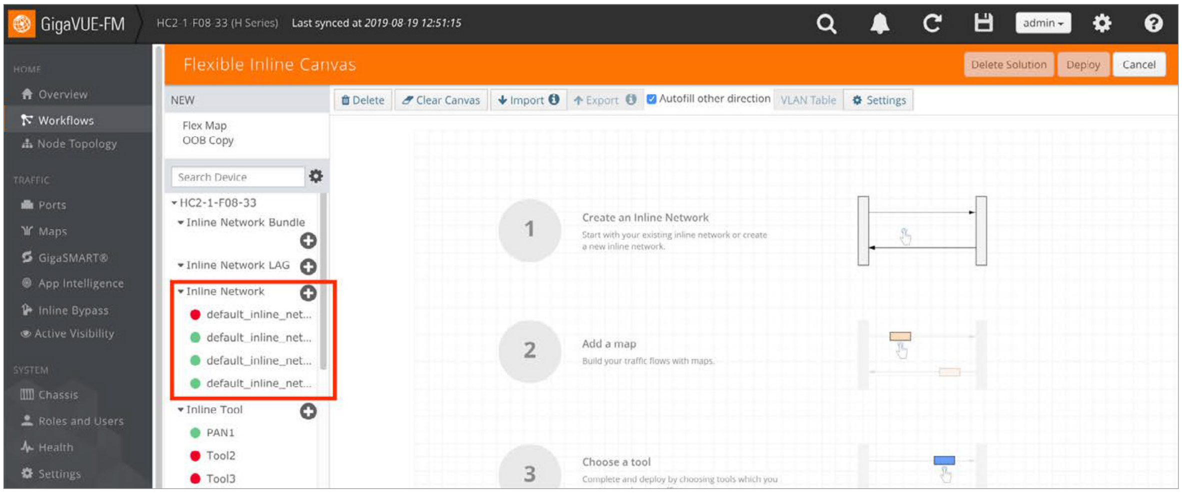


Figure 2-5b: Inline Network port pairs.

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

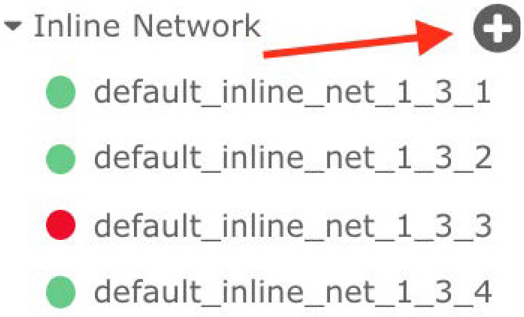
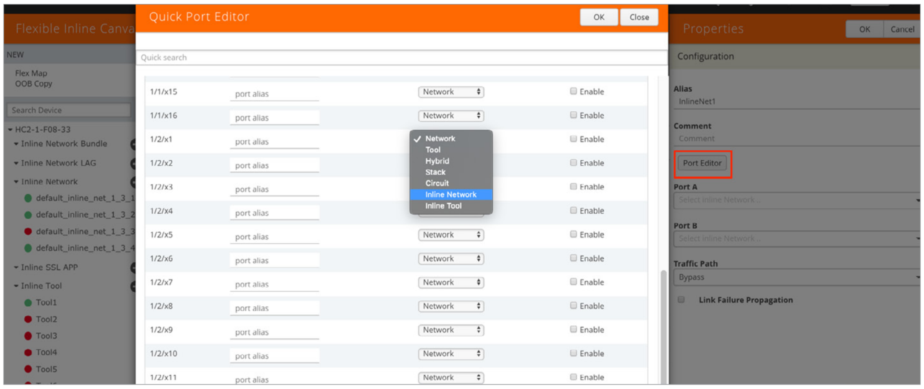


Figure 2-5b: Inline Networks sub default inline list.

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**.



1/1/x15	port alias	Network	□ Enable
1/1/x16	port alias	Network	□ Enable
1/2/x1	port alias		□ Enable
1/2/x2	port alias		□ Enable
1/2/x3	port alias		□ Enable
1/2/x4	port alias		□ Enable
1/2/x5	port alias	Network	□ Enable
1/2/x6	port alias	Network	□ Enable
1/2/x7	port alias	Network	□ Enable
1/2/x8	port alias	Network	□ Enable
1/2/x9	port alias	Network	□ Enable
1/2/x10	port alias	Network	□ Enable
1/2/x11	port alias	Network	□ Enable

Alias: InlineNet1
Comment: Comment
Port A: Select inline Network ..
Port B: Select inline Network ..
Traffic Path: Bypass
□ Link Failure Propagation

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.

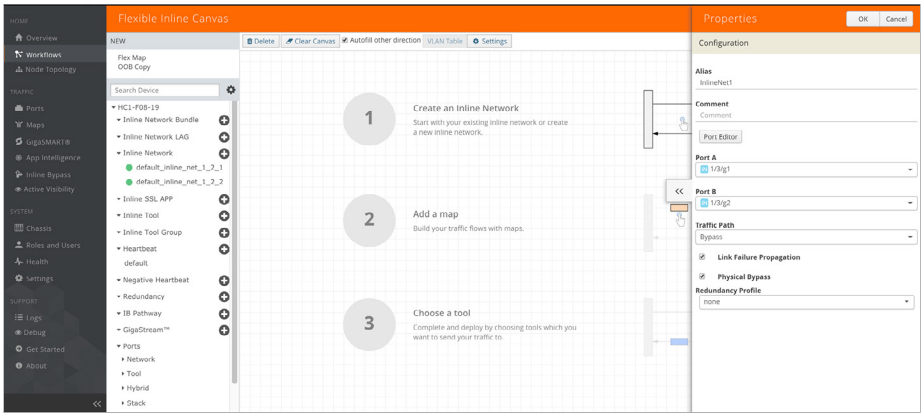
5. Leave **Redundancy Profile** to **None**.

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).



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.

3 Choose a tool
Complete and deploy by choosing tools which you want to send your traffic to.

Alias: InlineNet1
Comment: Comment
Port A: 1/3/g1
Port B: 1/3/g2
Traffic Path: Bypass
☑ Link Failure Propagation
☑ Physical Bypass
Redundancy Profile: none

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.

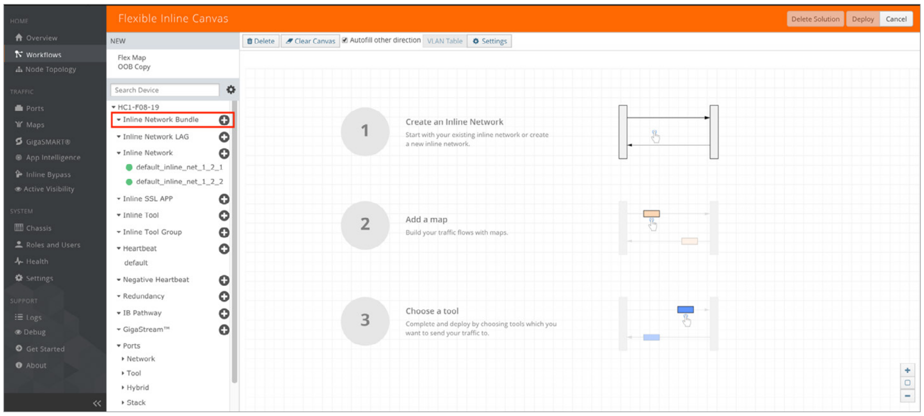


Figure 2-6c: Inline Network Bundle selection.

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.

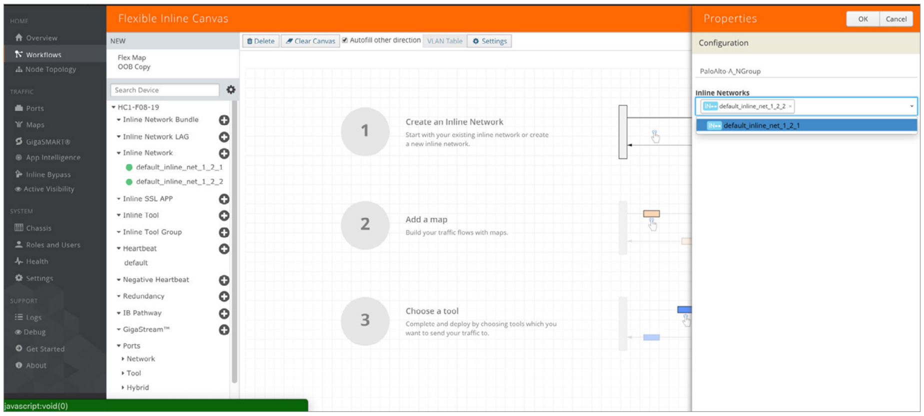


Figure 2-7: Inline Network selection.

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

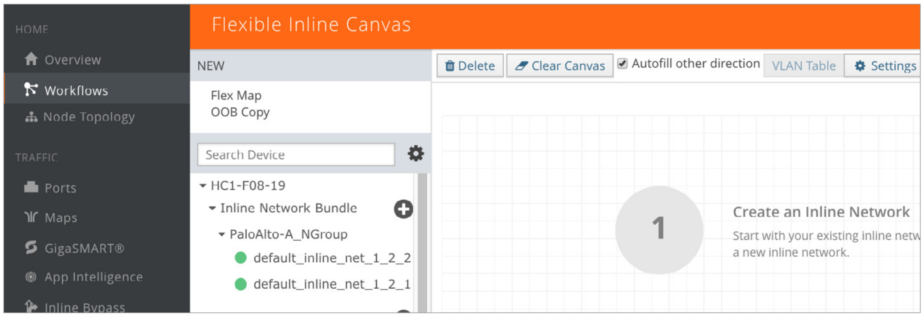


Figure 2-8: Finished list of Inline Network groups.

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**.

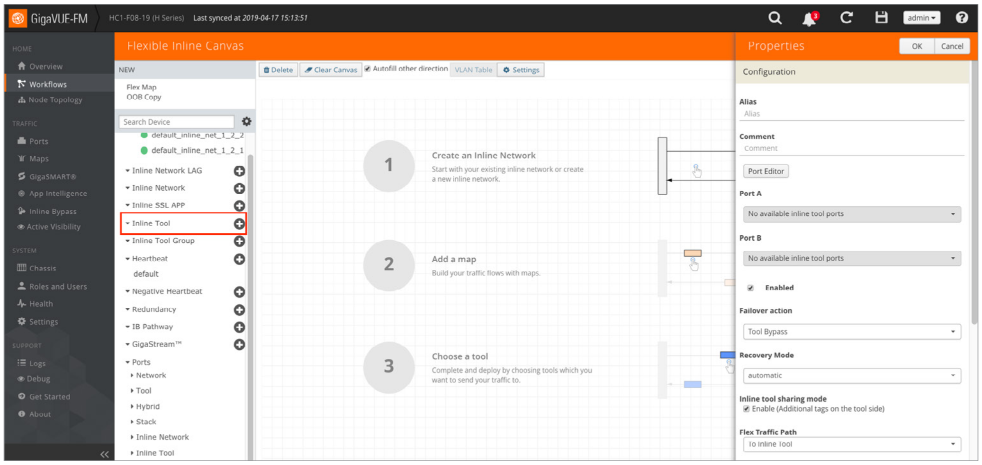
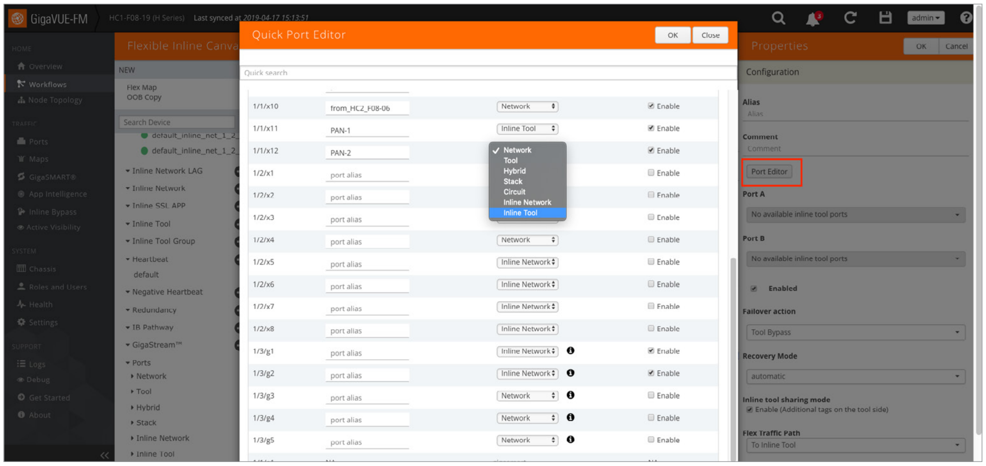


Figure 2-9: Inline Tool creation.

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



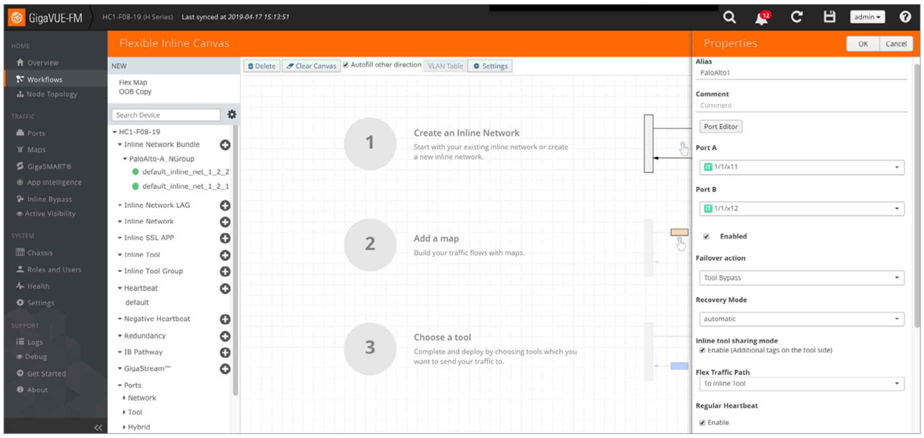
Port	Alias	Type	Enable
1/1/x10	from_HC2_F08-06	Network	☑ Enable
1/1/x11	PAN-1	Inline Tool	☑ Enable
1/1/x12	PAN-2	Network	☑ Enable
1/2/x1	port alias		□ Enable
1/2/x2	port alias		□ Enable
1/2/x3	port alias		□ Enable
1/2/x4	port alias	Network	□ Enable
1/2/x5	port alias	Inline Network	□ Enable
1/2/x6	port alias	Inline Network	□ Enable
1/2/x7	port alias	Inline Network	□ Enable
1/2/x8	port alias	Inline Network	□ Enable
1/3/g1	port alias	Inline Network	☑ Enable
1/3/g2	port alias	Inline Network	☑ Enable
1/3/g3	port alias	Network	□ Enable
1/3/g4	port alias	Network	□ Enable
1/3/g5	port alias	Network	□ Enable

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.



Alias: PaloAlto1

Comment: Comment

Port A: 1/1/x11

Port B: 1/1/x12

☑ Enabled

Failover action: Tool Bypass

Recovery Mode: automatic

Inline tool sharing mode: ☑ Enable (Additional tags on the tool side)

Flex Traffic Path: To Inline Tool

Regular Heartbeat: ☑ Enable

Figure 2-10: Inline Tool Pair configuration.

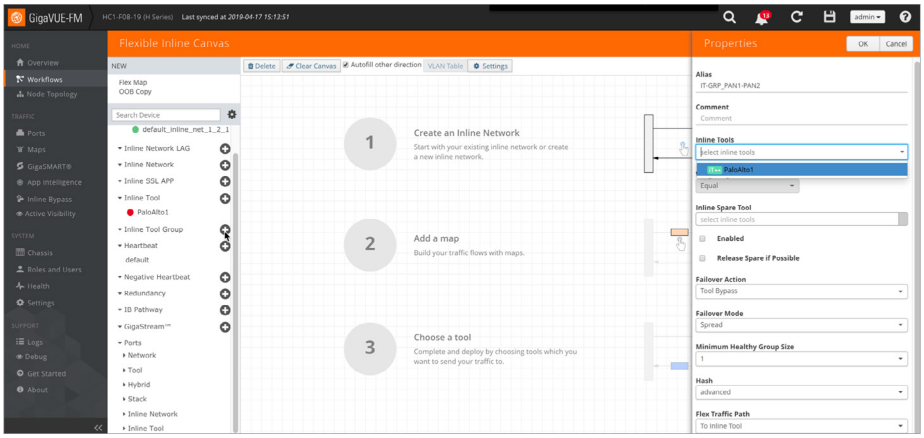
7. Click **Save**.
8. Repeat steps 2 through 6 for all additional FortiGate NGFWs.

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**.



Alias: IT-GRP_PAN1-PAN2

Comment: Comment

Inline Tools: select inline tools
PaloAlto1

Equal

Inline Spare Tool: select inline tools

□ Enabled

□ Release Spare if Possible

Failover Action: Tool Bypass

Failover Mode: Spread

Minimum Healthy Group Size: 1

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.
3. 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.

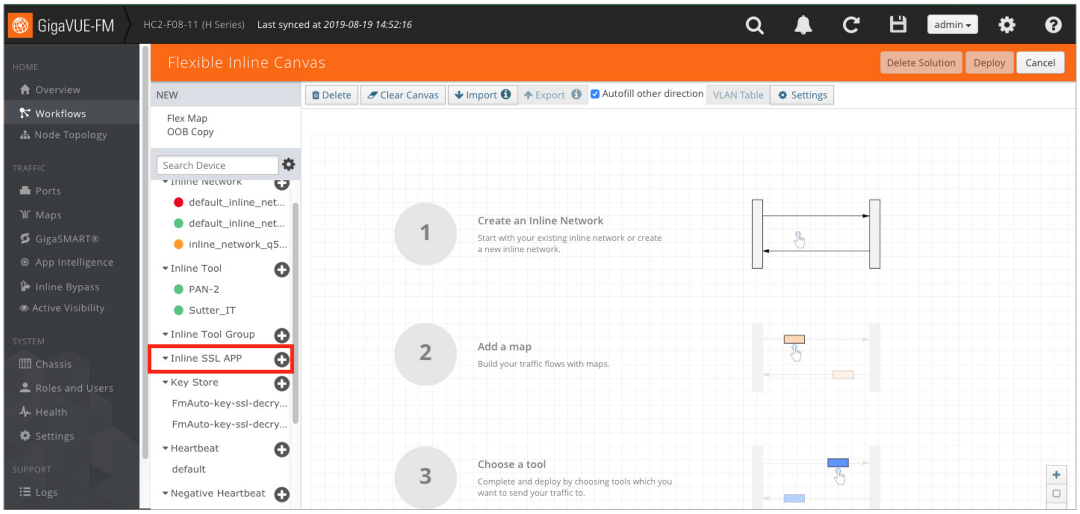
   There is an option to select an Inline spare tool. When you select this option, it becomes the primary failure action for this inline tool group.

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**.

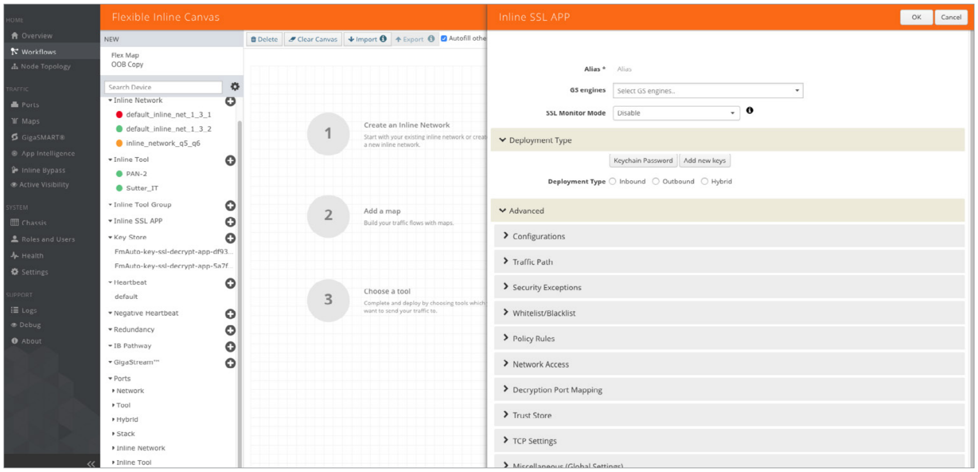
Configuring the Inline SSL App (Only for Inline SSL deployment)

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.

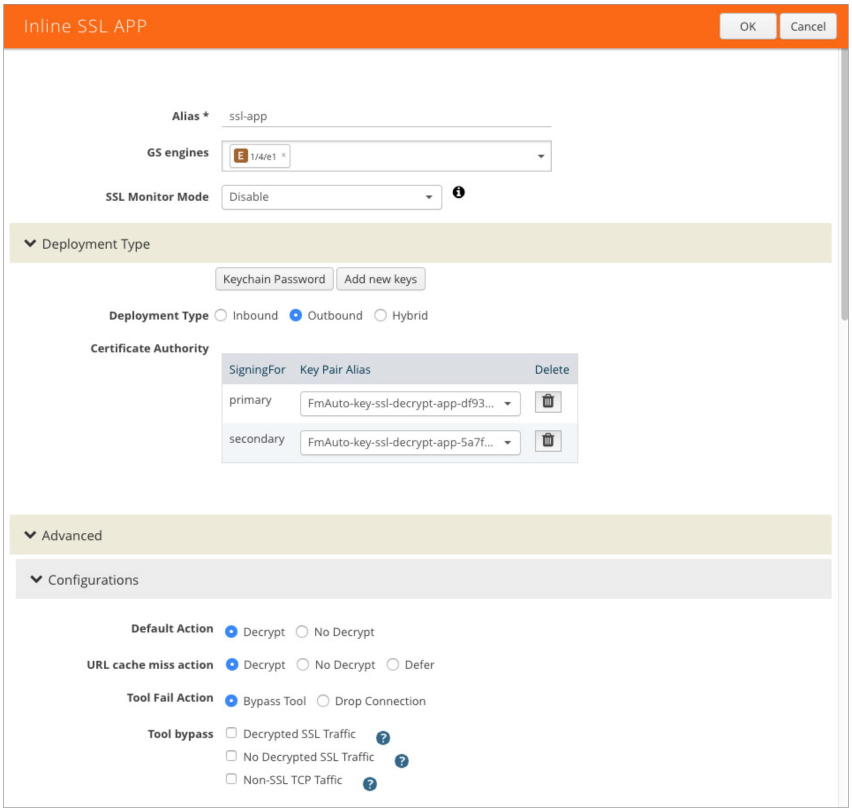


Alias * Alias
GS engines Select GS engines..
SSL Monitor Mode Disable
Deployment Type ○ Inbound ○ Outbound ○ Hybrid

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.



Alias * ssl-app

GS engines 1/4/e1

SSL Monitor Mode Disable

Deployment Type ○ Inbound ● Outbound ○ Hybrid

Certificate Authority

SigningFor	Key Pair Alias	Delete
primary	FmAuto-key-ssl-decrypt-app-df93...	
secondary	FmAuto-key-ssl-decrypt-app-5a7f...	

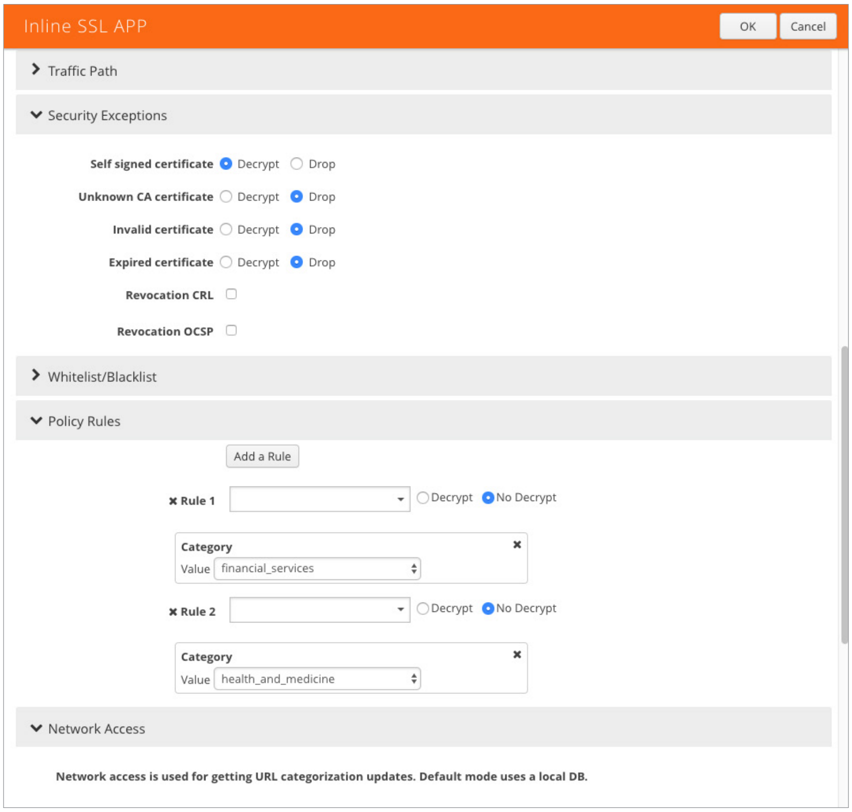
Default Action ● Decrypt ○ No Decrypt

URL cache miss action ● Decrypt ○ No Decrypt ○ Defer

Tool Fail Action ● Bypass Tool ○ Drop Connection

Tool bypass □ Decrypted SSL Traffic
□ No Decrypted SSL Traffic
□ Non-SSL TCP Taffic

Figure 2-12a: SSL app configuration.



Self signed certificate ● Decrypt ○ Drop

Unknown CA certificate ○ Decrypt ● Drop

Invalid certificate ○ Decrypt ● Drop

Expired certificate ○ Decrypt ● Drop

Revocation CRL □

Revocation OCSP □

✖ Rule 1 ○ Decrypt ● No Decrypt

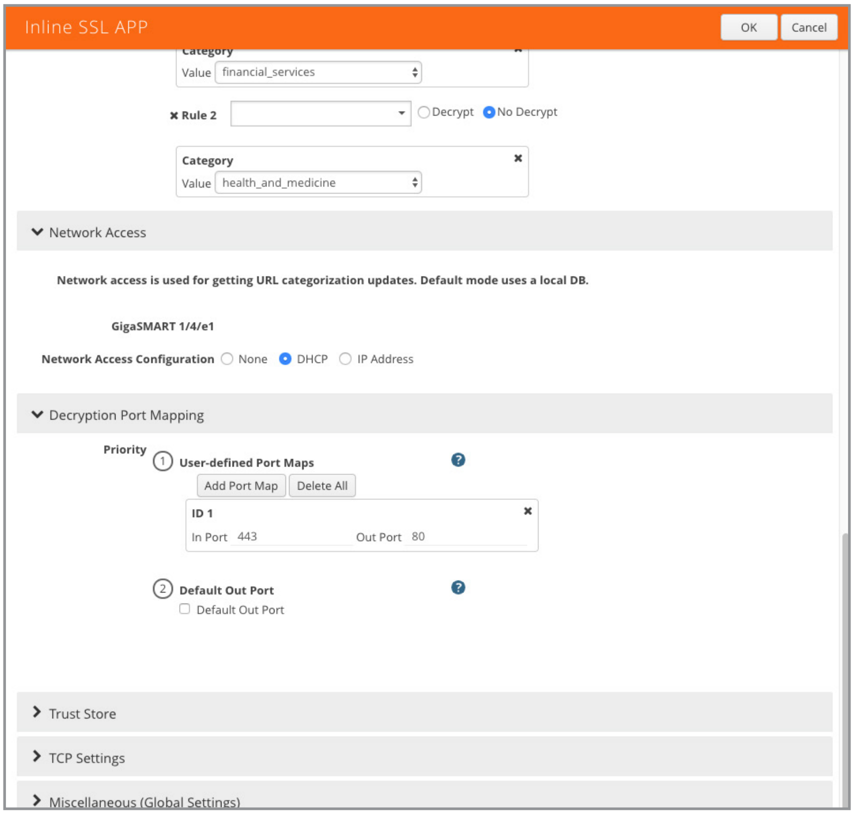
Category ✖
Value financial_services

✖ Rule 2 ○ Decrypt ● No Decrypt

Category ✖
Value health_and_medicine

Network access is used for getting URL categorization updates. Default mode uses a local DB.

Figure 2-12b: SSL app configuration.



Category
Value financial_services

✖ Rule 2 ○ Decrypt ● No Decrypt

Category ✖
Value health_and_medicine

Network access is used for getting URL categorization updates. Default mode uses a local DB.

GigaSMART 1/4/e1

Network Access Configuration ○ None ● DHCP ○ IP Address

Priority
1 User-defined Port Maps

ID 1 ✖
In Port 443 Out Port 80

2 Default Out Port
□ Default Out Port

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.

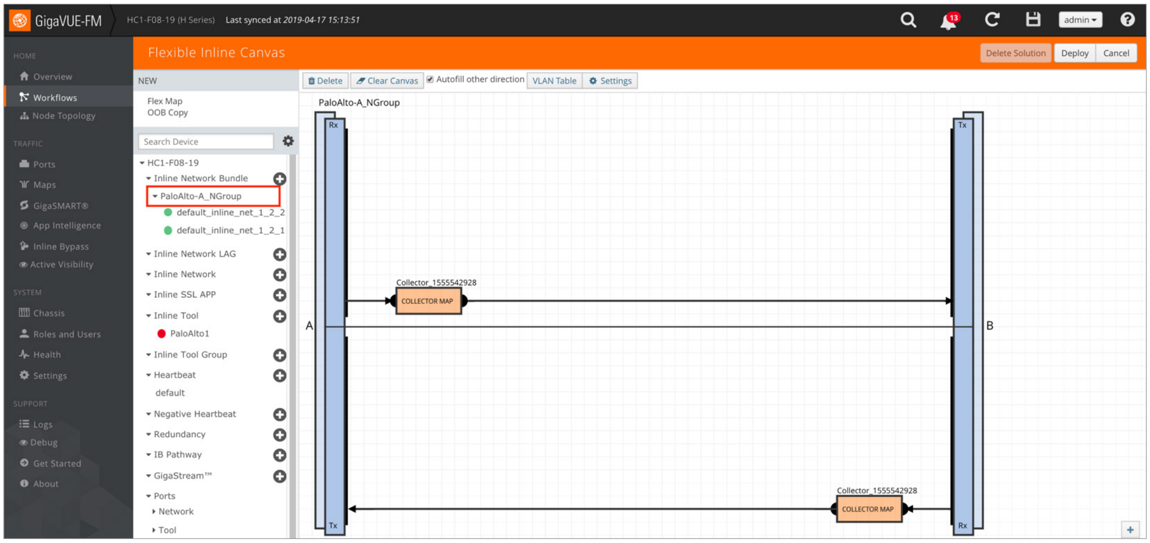
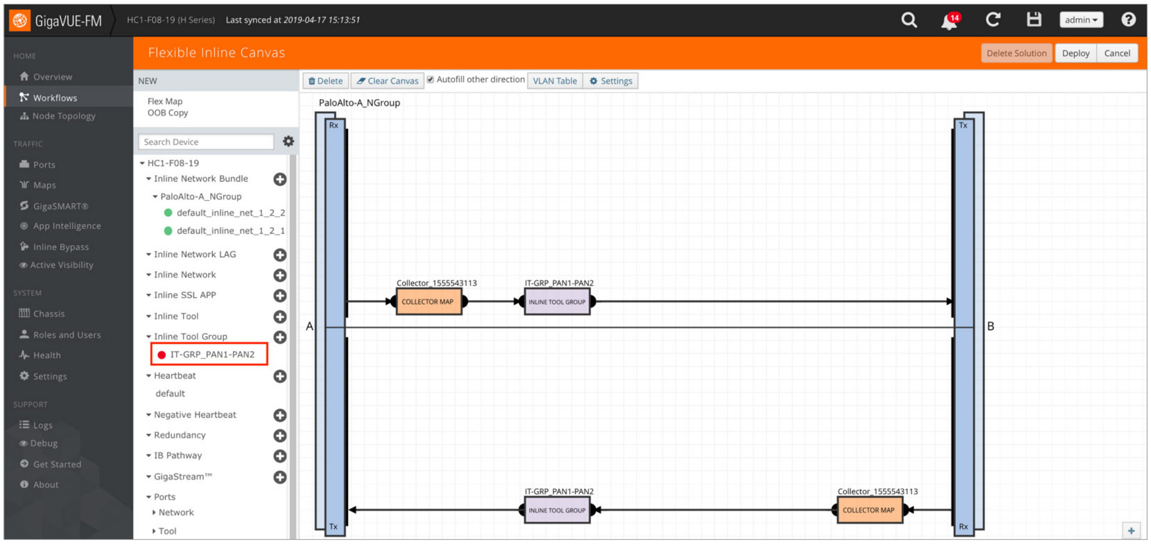


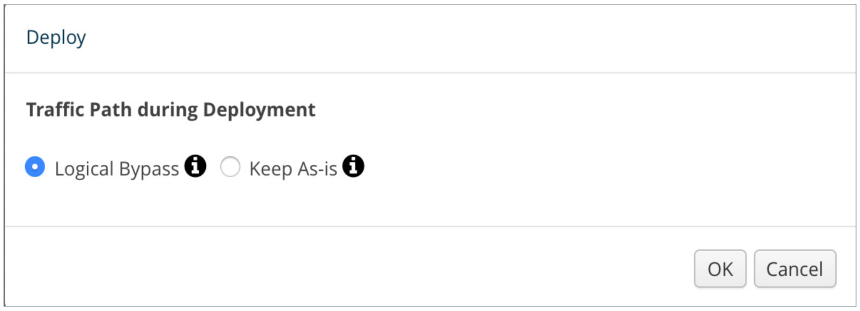
Figure 2-13: Configuration for Pass All Map.

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.



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**.

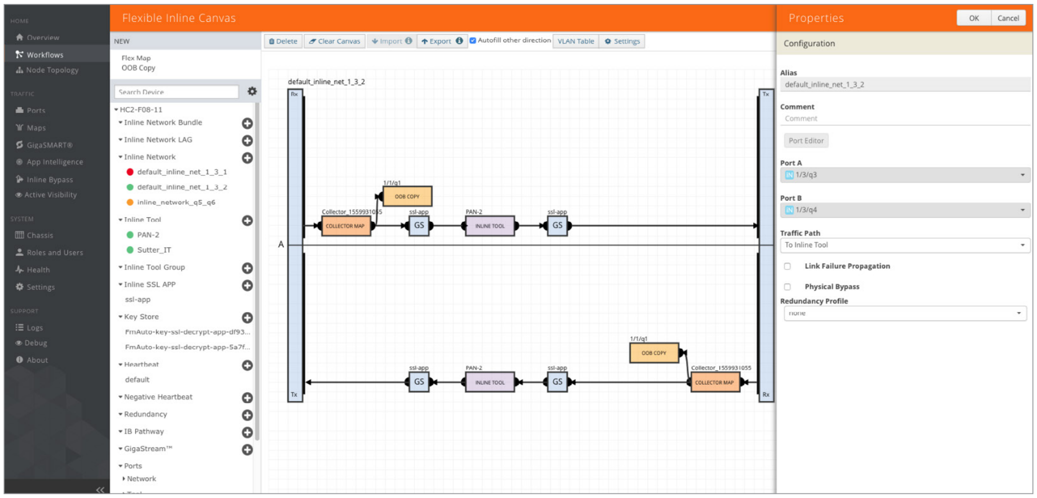


Deploy

Traffic Path during Deployment

● Logical Bypass ○ Keep As-is

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.



Alias: default_inline_net_1_3_2

Comment: Comment

Port Editor

Port A: 1/3/q3

Port B: 1/3/q4

Traffic Path: To Inline Tool

□ Link Failure Propagation

□ Physical Bypass

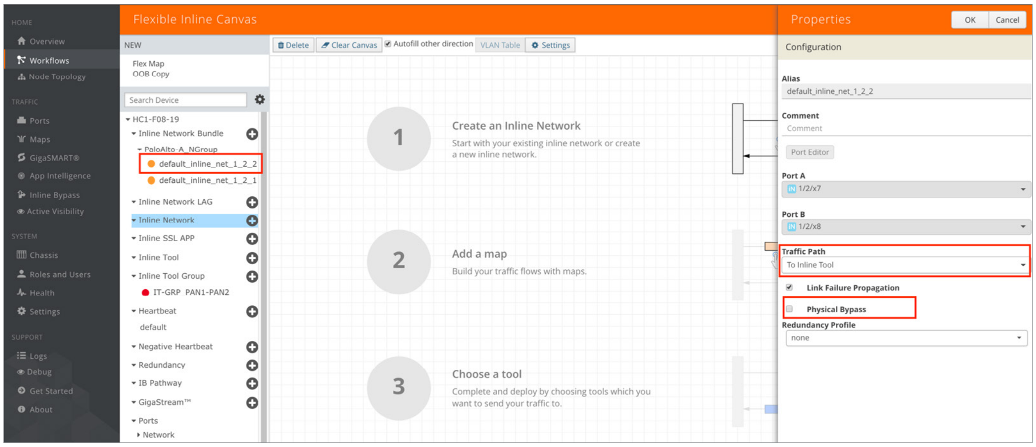
Redundancy Profile: none

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**.



Alias: default_inline_net_1_2_2

Comment: Comment

Port A: 1/2/x7

Port B: 1/2/x8

Traffic Path: To Inline Tool

☑ Link Failure Propagation

☐ Physical Bypass

Redundancy Profile: none

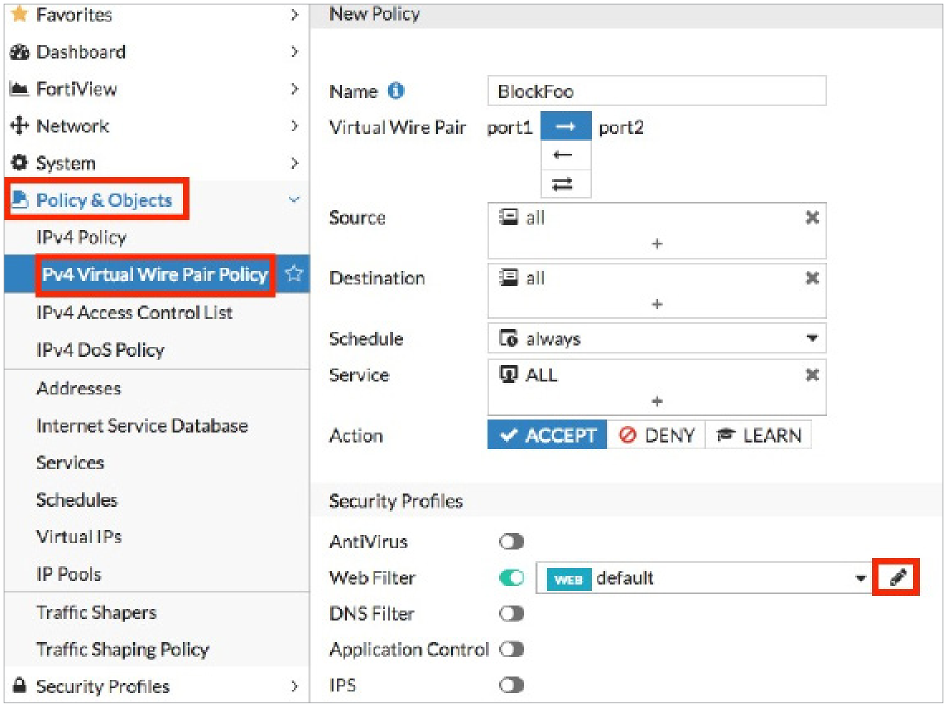
Figure 2-14: Inline Network traffic path changed to Inline tool, Physical Bypass unchecked.

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**.



Name: BlockFoo

Virtual Wire Pair: port1 → port2

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT

AntiVirus: off

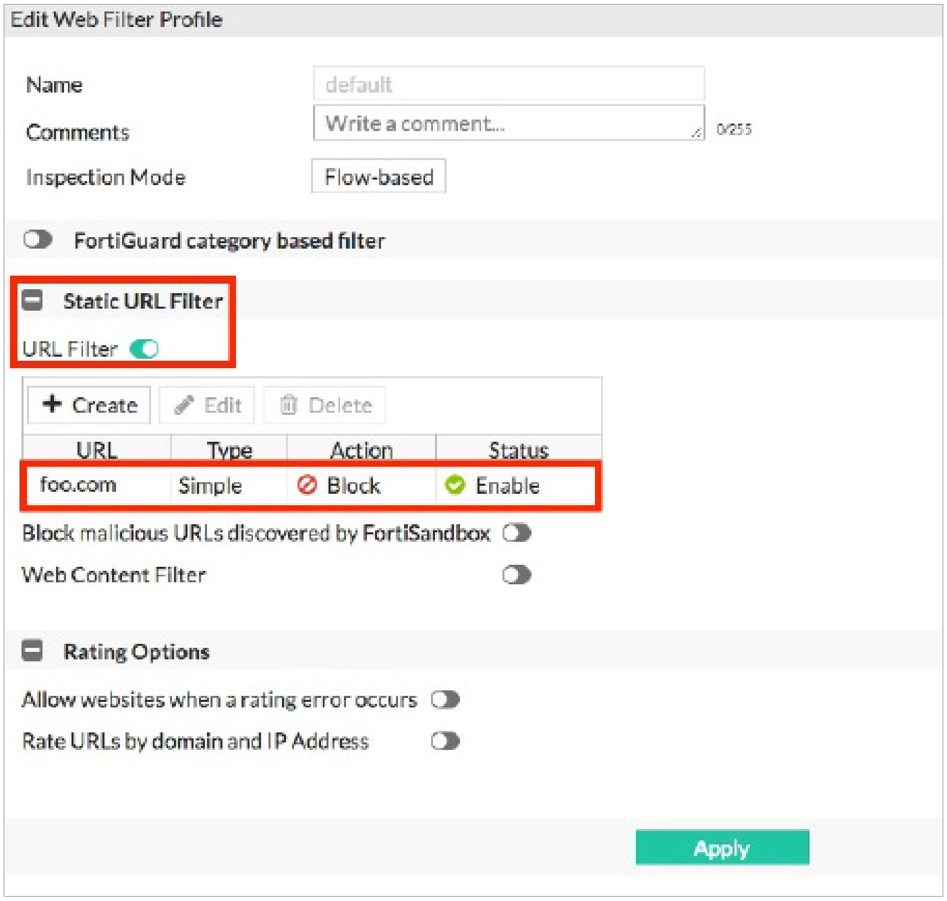
Web Filter: on — WEB default

DNS Filter: off

Application Control: off

IPS: off

Figure 2-15: Creating a new policy.



Edit Web Filter Profile

Name: default

Comments: Write a comment... 0/255

Inspection Mode: Flow-based

FortiGuard category based filter

Static URL Filter

URL Filter

URL	Type	Action	Status
foo.com	Simple	Block	Enable

Block malicious URLs discovered by FortiSandbox

Web Content Filter

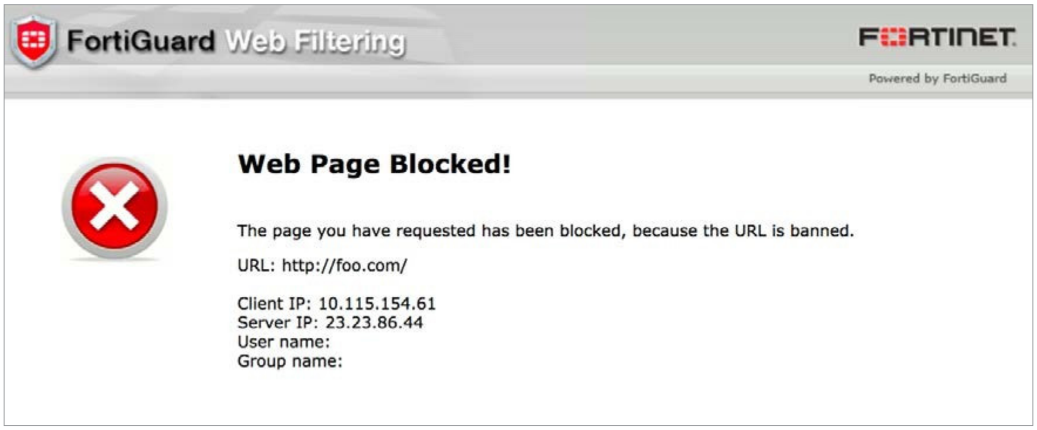
Rating Options

Allow websites when a rating error occurs

Rate URLs by domain and IP Address

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 http://.foo.com/. You should get a block page similar to the following:



Web Page Blocked!

The page you have requested has been blocked, because the URL is banned.

URL: http://foo.com/

Client IP: 10.115.154.61
Server IP: 23.23.86.44
User name:
Group name:

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.

FORTINET®

www.fortinet.com

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-gigamon-inline-4202021

486482-A-0-EN