Check Point 4800 with Gigamon Inline Deployment Guide

Contents

1 Overview

Check Point Next Generation Threat Prevention (NGTP) platforms provide a multi layered line of defense to secure your enterprise from threats. This includes NGTP protection from known, signature-based threats; Antivirus, Anti-Bot and IPS. You also get Next Generation Firewall (NGFW) technologies such as Application Control, URL Filtering and Identity Awareness to enable safe use of the Internet. When combined with Check Point SandBlast, users are protected from zero-day attacks using SandBlast Threat Emulation (sandboxing) and SandBlast Threat Extraction, delivering safe content to the user while the file emulation is done.

Together Gigamon's GigaSECURE® Security Delivery Platform and Check Point Next-Generation Threat Prevention Platforms deliver a robust solution to solve today's security challenges. GigaSECURE capabilities enable physical bypass protection to Check Point inline devices in case of power loss and logical bypass protection in the event of tool failure. Physical bypass helps maintain network traffic continuity by failing to wire in case of a power loss. The bypass capability also facilitates agile deployment by enabling addition, removal and upgrade of Check Point devices without affecting network traffic. This is especially helpful in scenarios where a new inline device needs to be added to gain visibility into the network without disrupting traffic.

The joint Gigamon and Check Point solution also provides the following benefits:

- Full Visibility: Gigamon's GigaSECURE platform provides visibility across the entire network and can deliver traffic from multiple locations, like branch offices and virtualized data center segments back to centrally located Check Point devices.
- Load Sharing: Improves the scalability of inline security by distributing the traffic across multiple security devices, allowing them to share the load and inspect more traffic or aggregate multiple traffic flows into a single flow for efficient port utilization on the firewall.
- Asymmetric Routing Management: GigaSECURE provides an intelligent and efficient way to ensure that the same device inspects all the packets of a given session.
- NetFlow Generation and SSL Decryption: Processing intensive tasks can be offloaded from the Check Point devices by using GigaSECURE functionality for generating unsampled, enhanced metadata (NetFlow/IPFIX) from any selected traffic stream. Similarly, the Security Delivery Platform can be used to decrypt SSL traffic for inspection by Check Point devices.

Use Cases

There are two common use cases where the combined Gigamon and Check Point solution provides intelligent traffic visibility along with continuous security monitoring of traffic. The use cases are discussed in the following sections:

Use Case 1: Inline Bypass with Load Sharing

The raw amount of traffic traversing through networks is increasing as organizations move to higher capacity links to keep up with the increase in information that needs to travel across their networks. To keep up with the increase in traffic volume and maintain a robust security perimeter, organizations may need to scale up and deploy multiple Check Point NGTP appliances in their environments. The primary challenge in deploying multiple Check Point

appliances is ensuring that all packets belonging to the given session go to the same appliance. In addition, for organizations, inline appliances pose a threat to maintaining traffic continuity in case of power failures.

The Gigamon GigaVUE-HC2 visibility node provides intelligent traffic visibility to address complex network visibility requirements. When the GigaVUE-HC2 is placed inline, Check Point appliances are attached directly to it. Firstly, it does intelligent hashing that ensures that all packets in a given session go to the same tool. Secondly, traffic is load shared amongst all Check Point devices to ensure that none of the members is overloaded. If an appliance goes down, the HC2 distributes traffic amongst remaining members thus ensuring continuous security monitoring of traffic.

Use Case 2: Gigamon Resilient Inline Protection

Network and security administrators need to carefully maintain the delicate relationship between network security requirements and network uptime. Both are quintessential to any modern day organization. Maintaining 100% network uptime with a solid security posture is quite challenging especially when new security tools are added or the existing ones are removed or upgraded. As more tools move from out-of-band detection to an inline active protection mode, network resiliency becomes a particular concern. Redundant network architectures provide some level of protection from faults, but they introduce complexity when inline inspection of traffic is required. As part of the GigaSECURE Security Delivery Platform, the GigaVUE-HC2 addresses these challenges with a resilient inline architecture – Gigamon Resilient Inline Protection (GRIP).

Inline security devices pose a high risk to production networks as they represent points of failure in the network. The reason for failure may be power outage, software or hardware failure. The problem worsens when multiple inline security devices are used. These challenges can be overcome using two methods:

- Redundant inline tools– Deploying redundant inline tools increases tool availability by letting the redundant tools take over once the primary tool fails. The failure on the primary tool is detected using heartbeat messages. Apart from having an Active/Standby arrangement, an Active/Active arrangement is also possible such that the visibility node load balances traffic across multiple inline tools.
- Bypass protection– The two types of bypass protection, logical bypass and physical bypass, operate on the principle that traffic continuity must be maintained even if the traffic cannot be inspected. With logical bypass, the traffic is forwarded to the network should the inline tool fail. When deploying redundant inline tools, bypass protection is applied if or when both the active and standby tools are down. Physical bypass protects against problems such as power failure of the visibility node. In the event of a power failure, relays complete the network circuit and keep traffic flowing.

2 Configurations

This chapter covers the deployment prerequisites, architectural overview, topology overview along with the configurations for the two use cases described in the previous chapter. The configurations shown are both for the Gigamon GigaVUE-HC2 and the Check Point 4800 devices.

Use Case 1: Inline Bypass with Load Sharing

The raw amount of traffic traversing through networks is increasing as organizations move to higher capacity links to keep up with the increase in information that needs to travel across their networks. To keep up with the increase in traffic volume and maintain a robust security perimeter, organizations may need to scale up and deploy multiple Check Point NGTP appliances in their environments. The primary challenge in deploying multiple Check Point appliances is ensuring that all packets belonging to the given session go to the same appliance. In addition, for organizations, inline appliances pose a threat to maintaining traffic continuity in case of power failures.

The Gigamon GigaVUE-HC2 visibility node provides intelligent traffic visibility to address complex network visibility requirements. When the GigaVUE-HC2 is placed inline in the network, Check Point appliances are attached directly to it. Firstly, it does intelligent hashing that ensures that all packets in a given session go to the same tool. Secondly, traffic is load shared amongst all Check Point appliances to ensure that none of the members is overloaded. In case an appliance goes down, the HC2 distributes traffic amongst remaining members thus ensuring continuous security monitoring of traffic.

Deployment Prerequisites

The solution tested and described consisted of the following components:

- Gigamon GigaVUE-HC2 (version 4.6) with one inline bypass module
- Connectivity to the outside network (Internet/uplink), and to the inside network using fiber links on the bypass module
- Gigamon GigaVUE-FM Fabric Manager (version 3.3)
- Two Check Point 4800 appliances (version R77.30) connected to HC2 as inline tools
- Check Point Smart Dashboard

The Check Point 4800s are enabled with the following security applications:

- Firewall
- Intrusion Prevention System (IPS)
- URL Filtering
- Anti-Bot and Anti-Virus
- Threat Emulation

Architectural Overview

The joint solution utilizing a Gigamon HC2 with bypass module along with two Check Point 4800 appliances is discussed in this section. The architecture diagram in Figure 1-1 shows where each component in the network is connected. The HC2 with bypass module connected to upstream and downstream links. The two Check Point 4800s connected directly to the HC2 as inline tools.

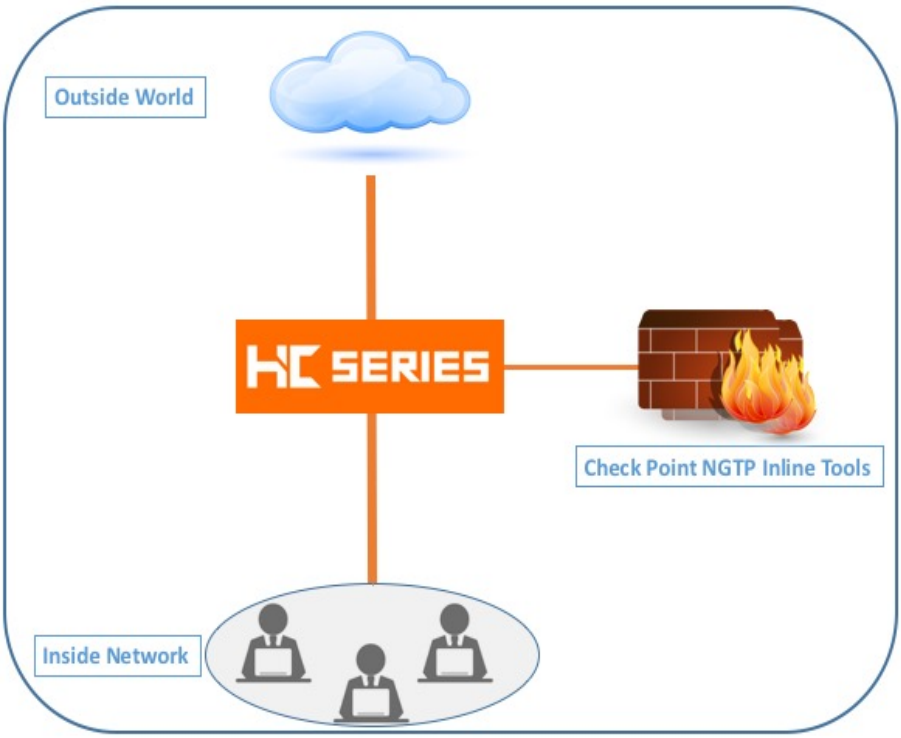

Figure 1-1: Check Point NGTP with Gigamon

Topology Overview and Configuration

The following section discusses in-depth how to configure the Gigamon HC2 and Check Point 4800 as an inline solution. The configuration on Gigamon HC2 is done via FM but can alternatively be done by CLI as well. Traffic is sent in a fashion that is load shared amongst the two inline tool members. Figure 1-2 represents the topology of the solution.

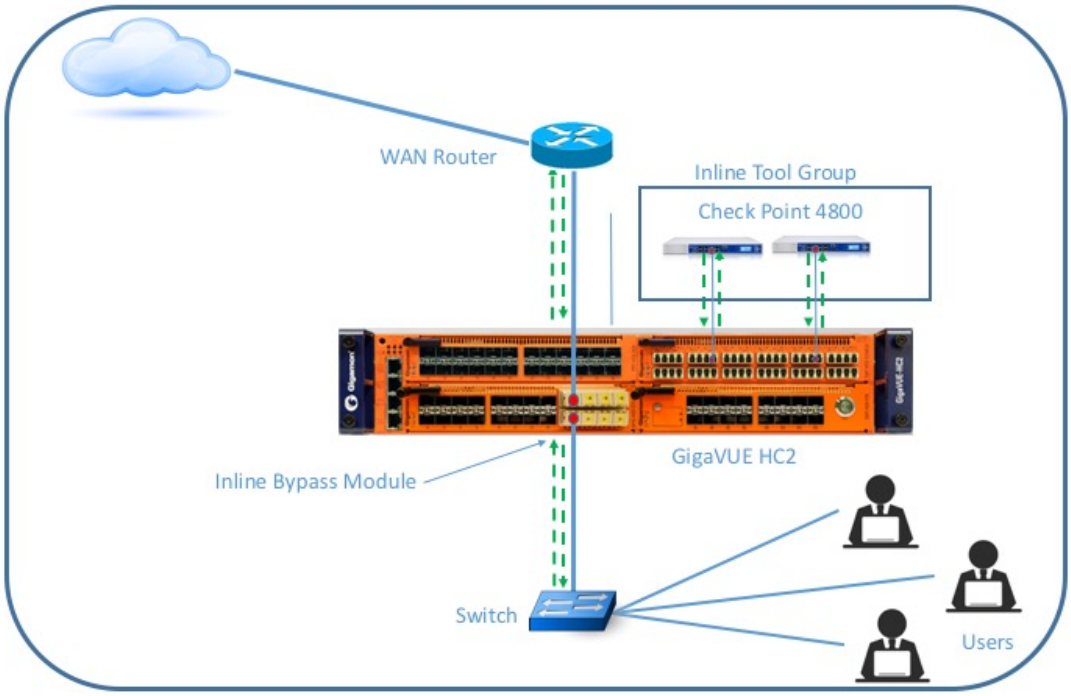

Figure 1-2: Check Point NGTP with Gigamon Topology

Check Point 4800 Configuration

This section covers the configuration steps for the Check Point 4800 devices in detail.

1. Start by logging on to the Check Point Gaia Portal for each 4800 and execute the steps below:

   a. Under **Network Management** click on **Network Interfaces**.

   b. Under **Interfaces**, select **Add**>>**Bridge** as represented in Figure 2-1.

   c. Add the **internal** and **external** interfaces and assign a **Bridge Group number**.

      See Check Point SecureKnowledge sk101371 for more information on Bridge Mode.

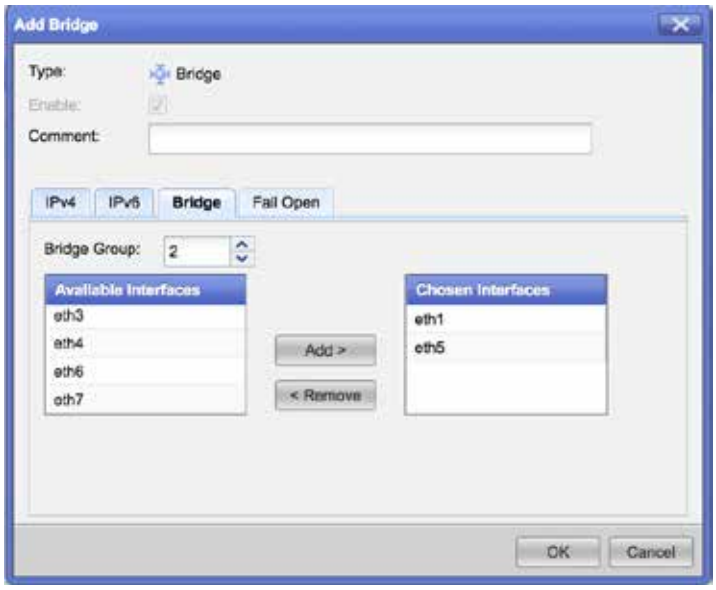

Figure 2-1: Check Point Gaia Interface Configuration Page

2. In Check Point **SmartDashboard** execute the following:

   a. Select the Check Point appliance under **Network Objects**.

   b. Under **General Properties** in the **Network Security** tab select the required security applications that need to be enabled as shown in Figure 2-2.

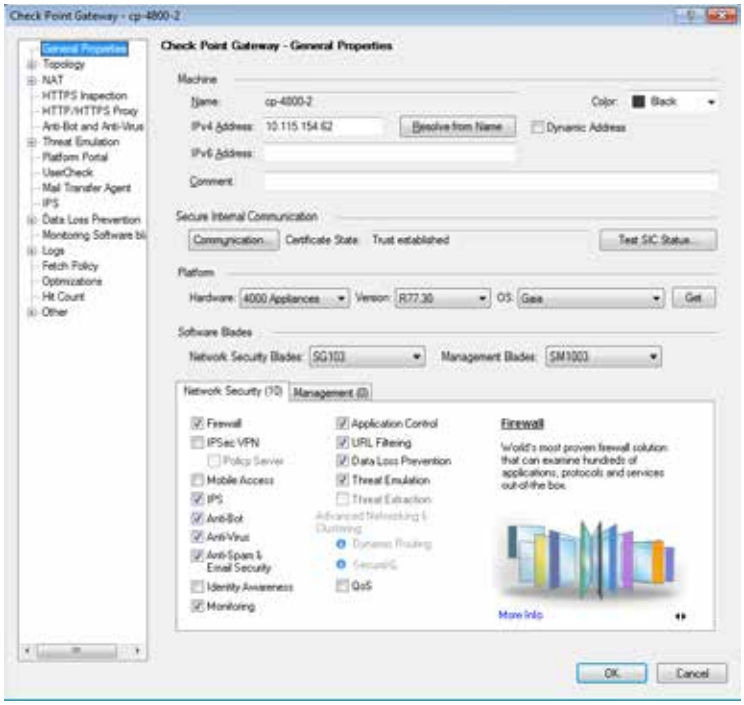

Figure 2-2: Check Point SmartDashboard General Properties

c. Navigate to **Topology** and select **Get > Interfaces with Topology**.

d. Select and assign the appropriate interfaces as internal or external as shown in Figure 2-3.

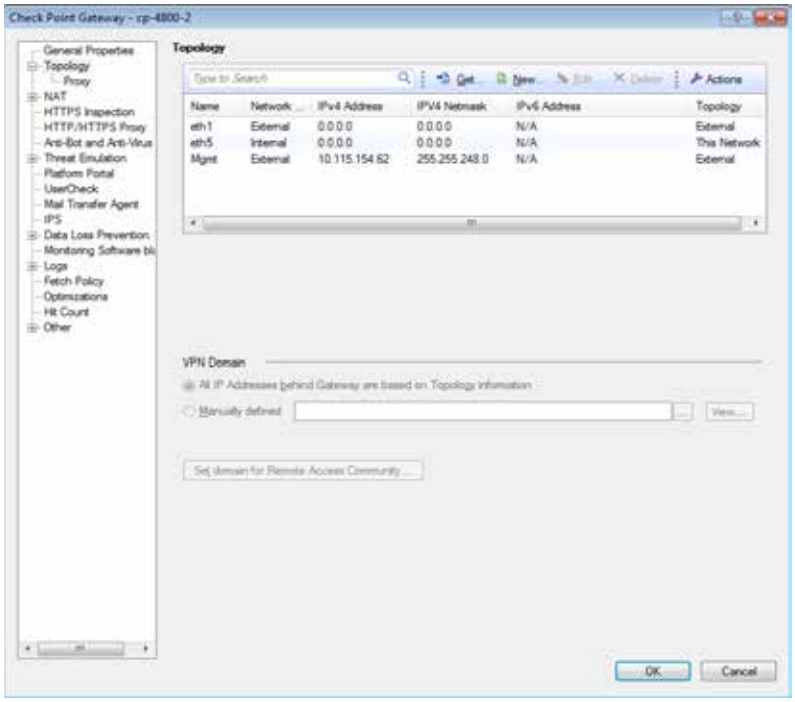

Figure 2-3: Check Point SmartDashboard Topology

e. Navigate to **Policy** check if a valid policy (or policies) exist as shown in Figure 2-4.

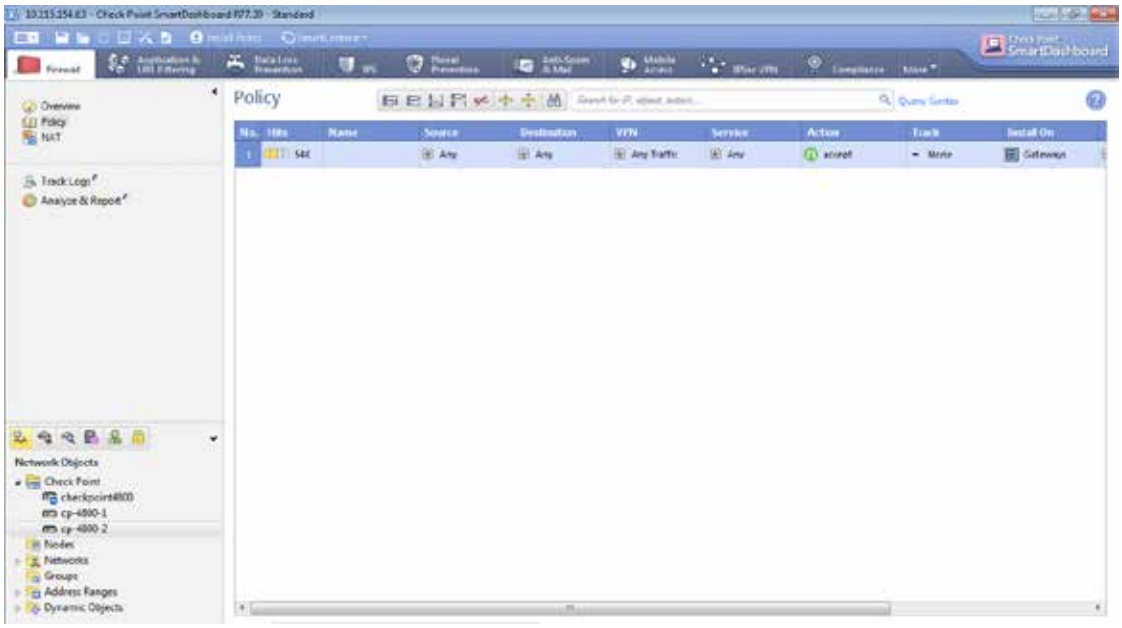

Figure 2-4: Check Point SmartDashboard Policy Page

GigaVUE-HC2 Configuration: Inline Network, Inline Tools and Inline Tool Group

This section provides a step-by-step guide to configuring inline network, inline tools and tool group.

Configuring the GigaVUE-HC2 Inline Network

1. Log into GigaVUE-FM, select **Physical Nodes**.
2. Select the GigaVUE-HC2 from the list of physical nodes that GigaVUE-FM is managing.
3. Select **Inline Bypass > Inline Networks** as shown in Figure 3-1.

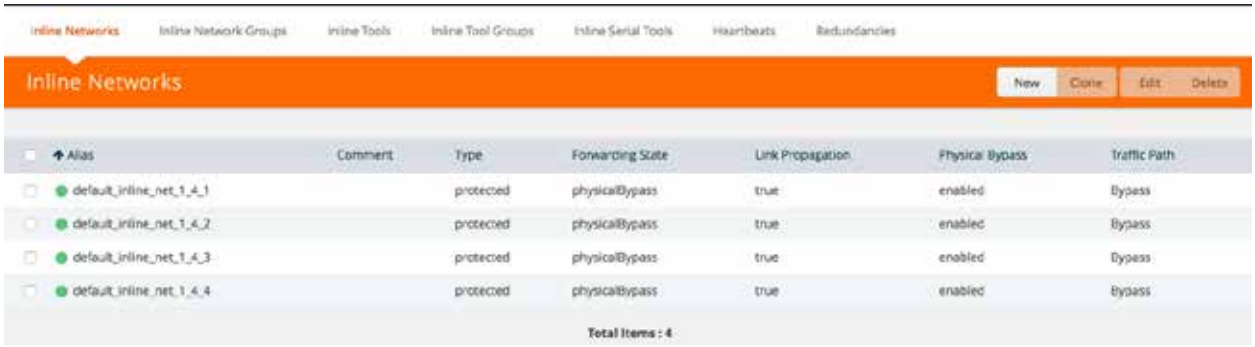

Figure 3-1: Inline Networks Configuration Page

4. Select and click **Edit** on the inline port that's represented in the Figure.
5. In the **Alias** Field, enter an alias and **Comment**.
6. **Port A** and **Port B** are automatically populated, based on earlier port selection.
7. Under **Configuration**, leave **Link Failure Propagation** and **Physical Bypass** to its default value.
8. Change **Traffic Path** > **Inline Tools**.
9. Click **Save** and the configuration looks like as shown in Figure 3-2.

Figure 3-2: Inline Network Configuration

Configuring Inline Tools

Inline tool port pairs and inline tool group configured in this section will be used in the traffic flow map defined in the later steps.

1. In GigaVUE-FM navigate to **Inline Bypass** > **Inline Tools** as shown in Figure 3-3.

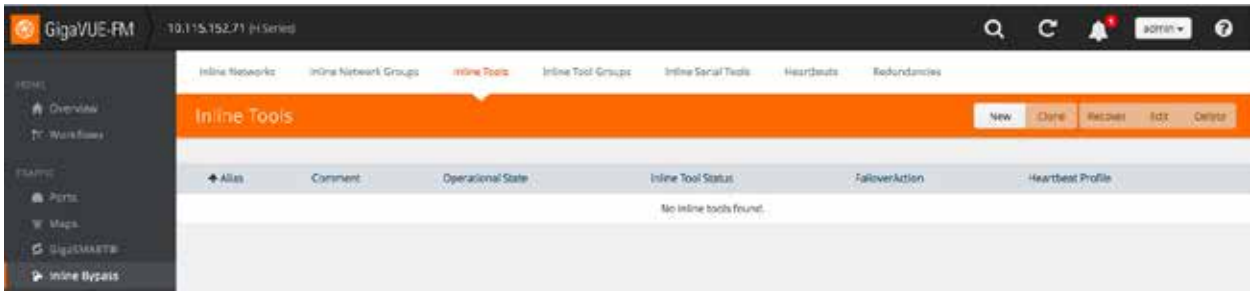

Figure 3-3: Inline Tools Configuration

2. Click **New** to open the configuration page for inline tools.
3. In the **Alias** field, type an alias that's convenient and depicts which inline tool this inline tool pair represents.
4. Under **Ports**, specify the ports as following:
   - For **Port A**, specify the port that corresponds to Side A in the network diagram.
   - For **Port B**, specify the port that corresponds to Side B in the network diagram.

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

5. Under **Configuration**, configure the following:

   - Enabled**: Checked**
   - Failover action**: ToolBypass**

     The failover action for this Inline Tool is ToolBypass. It means that the GigaVUE-HC2 will not send traffic to this inline tool if it is considered to be in a failure mode. The inline help fillt describes other options for inline tool. The other options have very different effects on the overall traffic flow.
   - Recovery Mode**: Automatic**
   - Enabled Heartbeat: **Checked**
   - Profile: **default**
   - HB IP Address A: **Leave Default**
   - HB IP Address **B: Leave Default**

Figure 3-4: Inline Tools Configuration

6. Click **Save** to write the configuration changes to memory as shown in Figure 3-4.
7. Repeat steps 1 through 6 for the second Check Point 4800 appliance. Refer to Figure 3-5 to view the status of inline tools.

Figure 3-5: Inline Tools Status

Configuring the Inline Tool Group

1. In GigaVUE-FM, select **Inline Bypass > Inline Tool Groups**.
2. Click **New** to open the Inline Tool Groups configuration page.
3. In the **Alias** field, enter an alias that represents the inline tool groups.
4. In the **Ports** section, click the Inline Tools field and select all the inline tools for this group from the list of available inline tools. Optionally, the Inline Spare Tool can be selected and an inline tool be selected. In that case, it becomes the primary failure action for this inline tool group.
5. In the Configuration section, configure the following and Save once done:
   - **Enabled: Checked**
   - Keep the defaults for **Release Spare if Possible, Failover Action, Failover Mode, Minimum Healthy Group Size**
   - **Hash**: **advanced**

     The advanced hashing scheme refers to hashing based on source IP, destination IP, L4 source port and L4 destination port. Choosing advanced hash ensures the following:

     - Bi-directional traffic for the same session goes to the same inline tool
     - Traffic is load shared amongst inline tools
6. Click **Save** and the configuration looks like as shown in Figure 3-6.

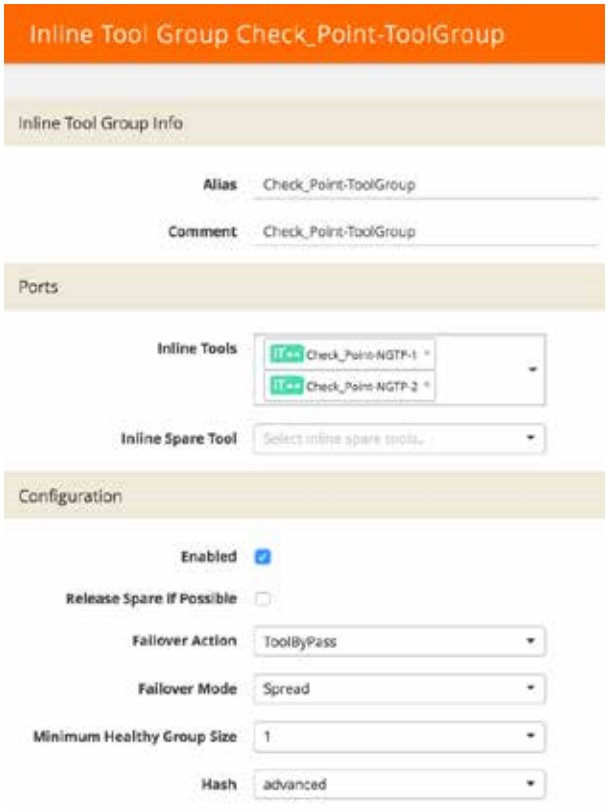

Figure 3-6: Inline Tool Group Configuration

Configuring the Inline Traffic Flow Maps

This section describes in detail how to configure traffic flow from the inline network to the inline Check Point tool group and allowing the reader to test the functionality of the Check Point appliances within the group. It is done in a two-step process:

1. Traffic Flow Map with an Inline Bypass Rule.
2. Change the Inline Network Path to Inline Tool.

After going through the above listed steps, you can test deployment of Check Point appliances.

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

This section describes the configuration steps to allow flow of traffic between the Inline Network and the Inline Tool Group

1. In GigaVUE-FM, navigate to **Maps** and click on **New.**
2. In the **Map Info** section configure the following:
   - **Map Alias**: Enter a map alias that represents the network source and tool destination
   - **Comments**: Enter comments for the map
   - **Type**: **Inline**

- **Sub Type**: **By Rule**
- **Traffic Path**: **Normal**

3. In the **Map Source and Destination** section:
   - Set **Source** to the inline network that was created earlier.
   - Set **Destination** to the inline tool groups that were created earlier.
4. Under **Map Rules:**
   - Click **Add a Rule**
   - In **Rule 1** click **Condition search…** and select **IP Version** > Version **v4** and select **Bi Directional**
   - Leave **Map Order** and **Map Permissions** to default values
   - Click **Save.** Refer to Figure 3-7 for configuration snapshot

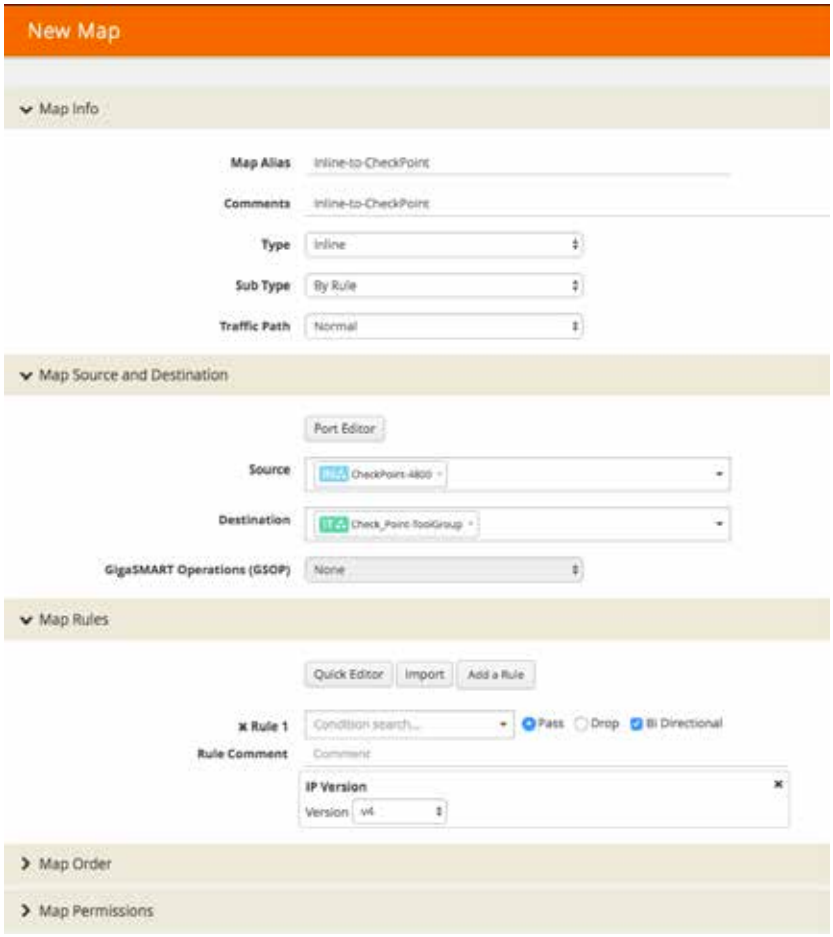

Figure 3-7: New Maps Configuration

Note: Map configuration from CLI: Inline map configuration on CLI differs from GigaVUE-FM map configuration, as Traffic path parameter is not available on CLI. The difference in configuration occurs when destination for map is “bypass” on CLI. GigaVUE-FM does not allow specifying “bypass” for destination but uses traffic path parameter instead to specify bypass.

Step 2: Change the Inline Network Traffic Path to Inline Tool

At this point, the inline tools are connected and configured to inspect traffic from the inline network. The next step after configuring maps is to change the traffic path for the inline networks from Bypass to Inline Tool. Before setting the traffic path to Inline Tool, ensure that the inline tool ports are up.

The steps to change the traffic path from bypass to inline tool are as follows:

1. In GigaVUE-FM, select the inline network defined previously and click **Edit**.
2. Uncheck **Physical Bypass**.

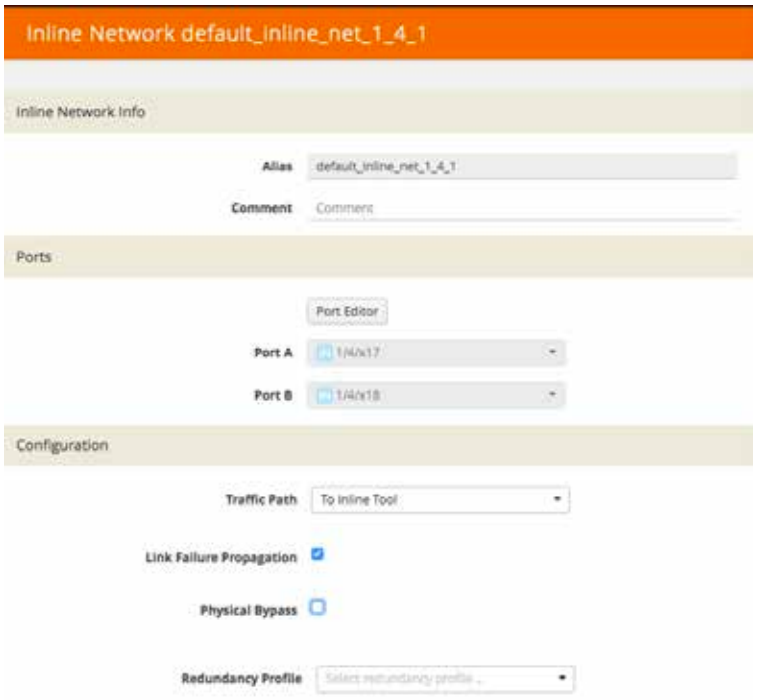

Figure 3-8: Inline Network with Physical Bypass Unchecked

3. Click **Save** as shown in Figure 3-8.

Use Case 2: Gigamon Resilient Inline Protection

Network and security administrators need to carefully maintain the delicate relationship between network security requirements and network uptime, both of which are quintessential to any modern day organization. Maintaining 100% network uptime with a solid security posture all over is quite challenging especially when new security tools are added or the existing ones are removed or upgraded. As more tools move from out-of-band detection mode to an inline active protection mode, network resiliency becomes of particular concern. Redundant network architectures provide some level of protection from faults but they also introduce complexity when inline inspection of traffic is required. As part of Gigamon's GigaSECURE Security Delivery Platform, the GigaVUE-HC2 addresses these challenges with a resilient inline architecture – Gigamon Resilient Inline Protection (GRIP).

Inline security devices pose a high risk to production networks as they represent points of failure in the network. The reason for failure may be power outage, software bug, or hardware failure. The problem worsens when multiple inline security devices are used. These challenges can be overcome using two methods:

- Using redundant inline tools: Deploying redundant inline tools increases tool availability by letting the redundant tools take over once the primary tool fails. The failure on the primary tool is detected using keepalives or heartbeat messages. Apart from having an Active/Standby arrangement, an Active/Active arrangement is also possible such that the visibility node load balances traffic across multiple inline tools.

- Using bypass protection: The two types of bypass protection – logical bypass and physical bypass operate on the principle that traffic continuity must be maintained even if the traffic cannot be inspected. With logical bypass, the traffic is forwarded to the network should the inline tool fail. When deploying redundant inline tools, bypass protection is applied if/when both the active and standby tools are down. Physical bypass protection protects against problems such as power failure of the visibility node itself. In the event of a power failure, relays complete the network circuit and keep traffic flowing.

Deployment Prerequisites

The solution tested and described consisted of the following components:

- Two Gigamon HC2 (version 4.6) with one inline bypass module on each

- Connectivity to the outside network (Internet/uplink), and to the inside network using fiber links on the bypass module

- Gigamon Fabric Manager (FM) (version 3.3)

- Two Check Point 4800 appliances (version R77.30) connected to the HC2s as inline tools

- Check Point Smart Dashboard

The Check Point 4800s had the following security applications enabled:

- Firewall

- Intrusion Prevention System (IPS)

- URL Filtering
- Anti-Bot
- Anti-Virus
- Threat Emulation

Architectural Overview

The Gigamon GRIP solution with two Check Point 4800 appliances and Gigamon GigaVUE-HC2 is discussed in this section. The architecture diagram in Figure 4-1 shows where each component in the network is connected. The HC2 with bypass module connected to upstream and downstream links. The two Check Point 4800s are connected directly to the HC2 as inline tools.

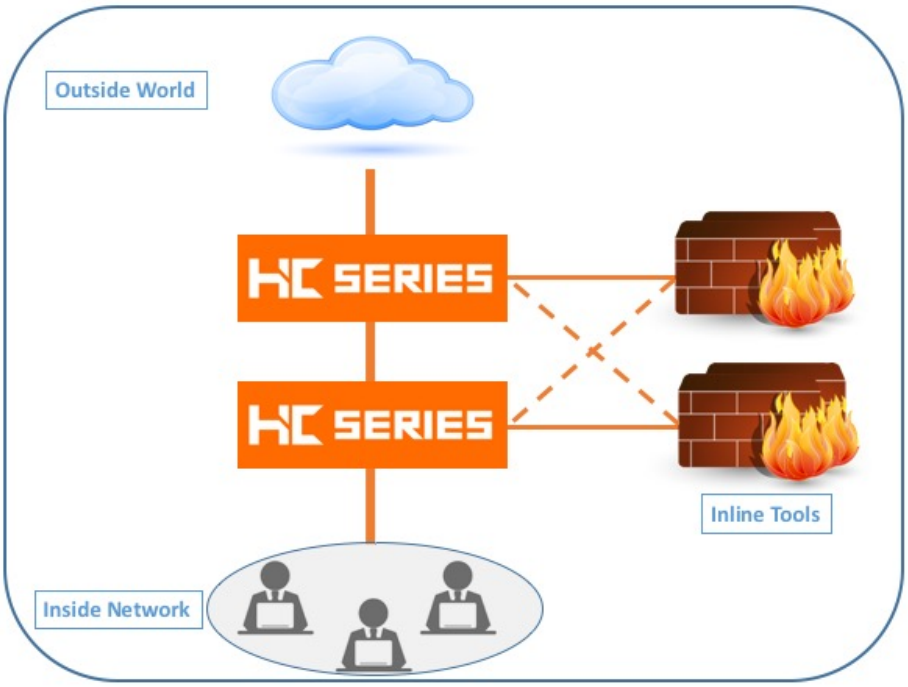

Figure 4-1: GRIP in the network with inline tools

Topology and Configuration

This section discusses in-depth how to configure the two Gigamon GigaVUE HC2s in a GRIP configuration with inline bypass and Check Point 4800s as an inline solution. The configuration on GigaVUE Gigamon HC2 is done via FM but can alternatively be done through the CLI as well. Traffic is sent in a fashion that is load shared among the two inline tool members. Refer to Figure 4-2 for solution topology.

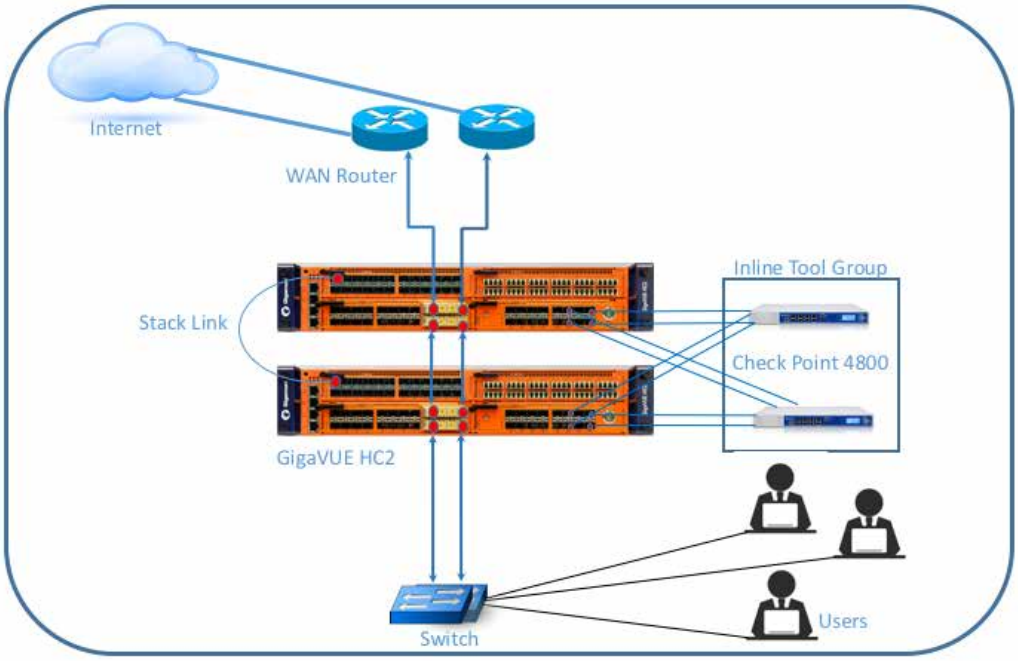

Figure 4-2: Realized Topology with GRIP

Check Point 4800 Configuration

This section discusses the configuration on the Check Point 4800s.

1. Start by logging on to the Check Point Gaia Portal for each 4800 and execute the steps:

   a. Under **Network Management** click on **Network Interfaces.**

   b. Under **Interfaces**, select **Add>>Bridge** as shown in Figure 5-1.

   c. Add the internal and external interfaces and assign a **Bridge Group number**. Add four interfaces (2 pairs) at minimum.

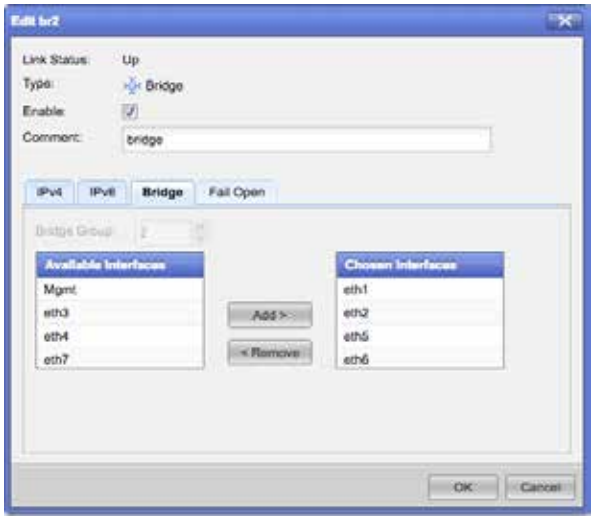

Figure 5-1: Check Point Gaia Web Interface Configuration Page

2. In the Check Point SmartDashboard execute the following:

   a. Select the Check Point appliance under **Network Objects**.

   b. Under **General Properties** in the **Network Security** tab select the required security applications that need to be enabled as shown in Figure 5-2.

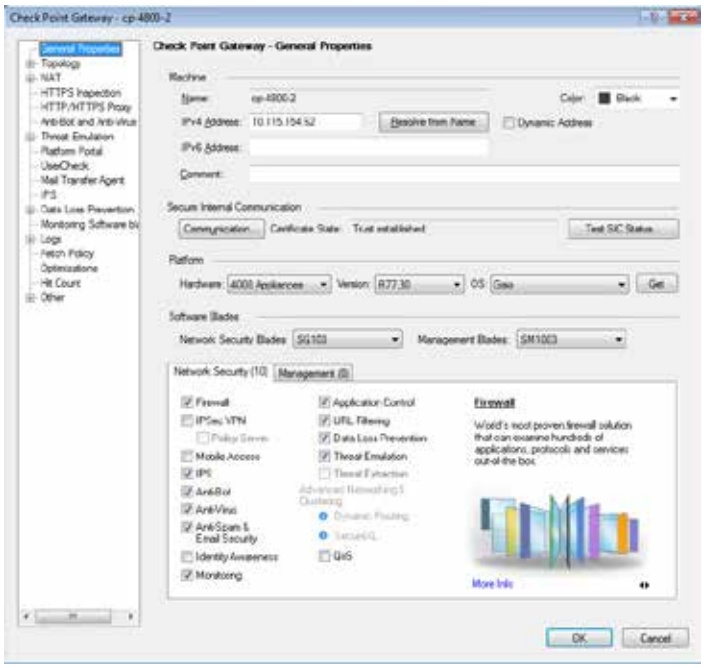

Figure 5-2: Check Point SmartDashboard General Properties

   c. Navigate to **Topology** and select **Get** > **Interfaces with Topology**.

   d. Select and assign the appropriate interfaces as internal or external as shown in Figure 5-3.

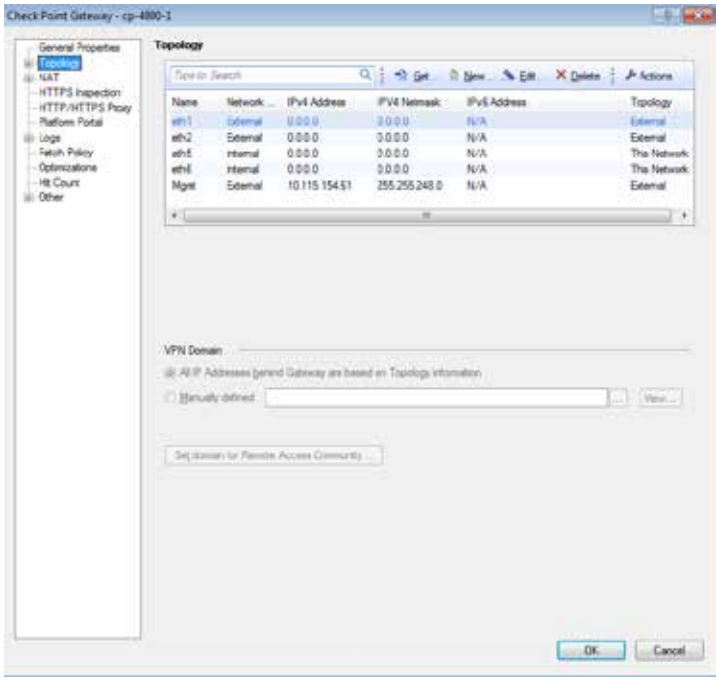

Figure 5-3: Check Point SmartDashboard Topology

e. Navigate to **Policy** check if a valid policy (or policies) exist as shown in Figure 5-4.

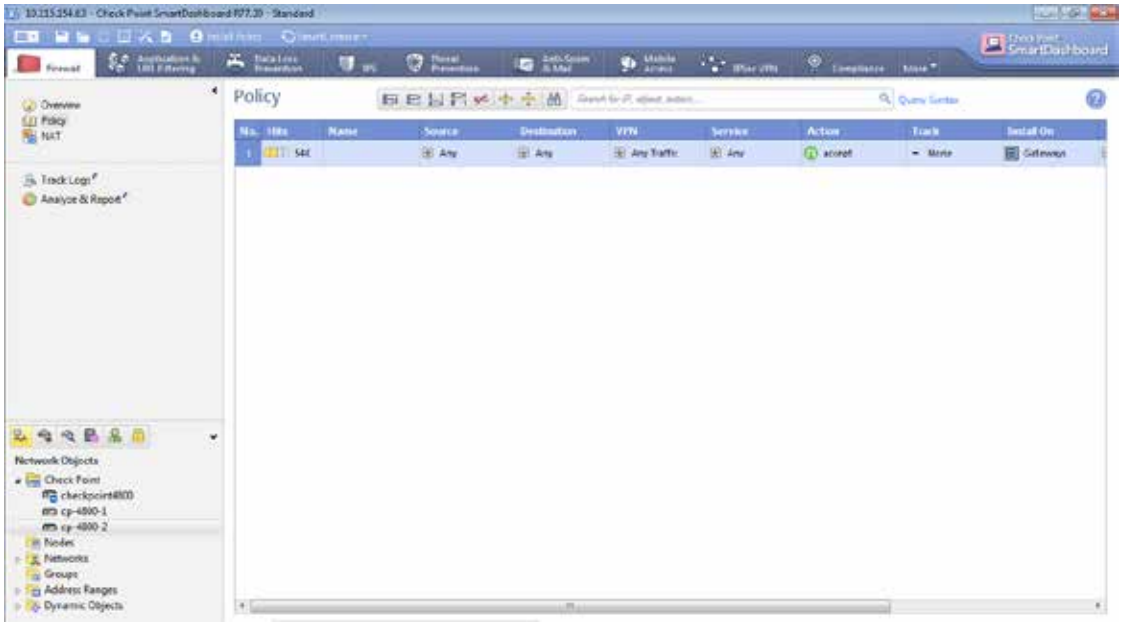

Figure 5-4: Check Point SmartDashboard Policy Page

GigaVUE-HC2 Configuration: Inline Network, Inline Tools and Inline Tool Group

This section provides a step-by-step guide for configuring inline network bypass and inline tools in the Primary GRIP node. The same procedure must be followed for configuring inline network bypass and inline tools in the Secondary GRIP node; steps that differ are explicitly described.

Configuring the GigaVUE-HC2 Inline Network Bypass Pairs

This section covers Gigamon GigaVUE-HC2 inline network bypass pair configuration

1. Log into GigaVUE-FM, select **Physical Nodes**.
2. Select the GigaVUE HC2 from the list of physical nodes that GigaVUE-FM is managing.
3. Select **Inline Bypass > Inline Networks**.

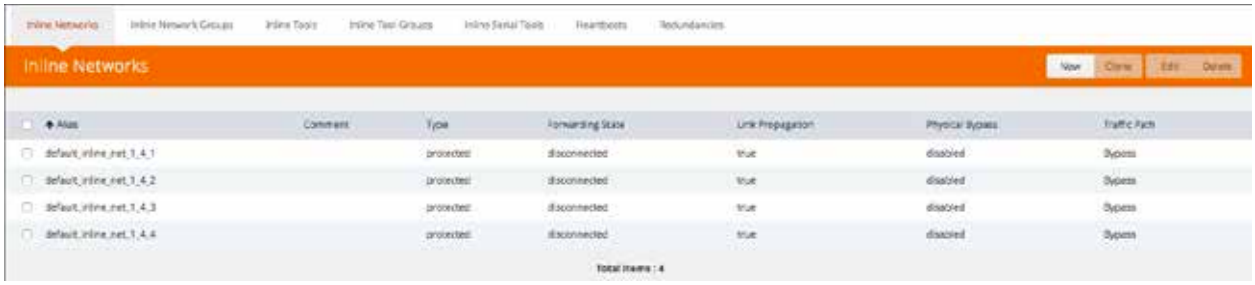

Figure 6-1: Inline Networks Configuration

Select and click **Edit** on the inline port that is represented in Figure 6-1, do the following:

1. In the **Alias** Field, enter an alias and **Comment**.
2. **Port A** and **Port B** are automatically populated, based on earlier port selection.
3. Under **Configuration**, change **Physical Bypass** to **Unchecked**.

   This is needed to create a redundancy profile later on. Disabling physical bypass is not allowed once the redundancy profile has been associated with an inline network
4. **Link Failure Propagation (LFP)** must be **disabled** since the link status must not be propagated on inline-network ports when the primary fails.
5. Change **Traffic Path** > **Inline Tools**.
6. Click **Save**. Refer to Figure 6-2 for configuration output.

Figure 6-2: Inline Network Configuration

7. Repeat steps 1 through 6 for the second inline network.

Configuring the GigaVUE-HC2 Inline Network Groups

This section covers inline network groups configuration on the GigaVUE-HC2

1. Select **Inline Bypass > Inline Network Groups**.
2. Select **New** and enter a suitable **alias** and optionally a **comment**.
3. Under **Inline Network Links** select the Inline Network ports configured in the previous step.
4. Click **Save** as shown in Figure 6-3.

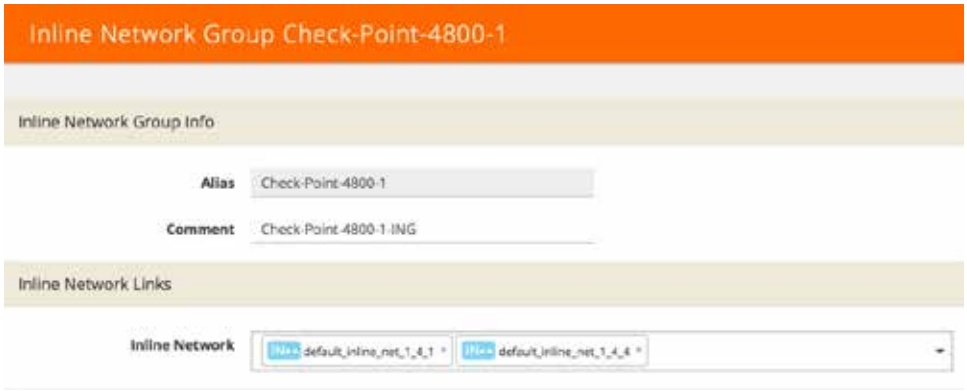

Figure 6-3: Inline Network Groups Configuration

Configuring the Inline Tools

Inline tool port pairs and inline tool group configured in this section will be used in the traffic flow map defined in the later steps.

In GigaVUE-FM navigate to **Inline Bypass > Inline Tools** as shown in Figure 6-4.

Figure 6-4: Inline Tools Configuration

1. Click **New** to open the configuration page for inline tools.
2. In the **Alias** field, type an alias that's convenient and depicts which inline tool this inline tool pair represents.
3. Under **Ports**:
   - Click **Port Editor** and create inline-tool ports
   - For **Port A**, specify the port that corresponds to Side A in the network diagram
   - For **Port B**, specify the port that corresponds to Side B in the network diagram
   - For the network diagram, refer to Figure 4-2
4. Under **Configuration**, configure the following:
   - **Enabled: Checked**
   - **Failover action: ToolBypass**
   - The failover action for this Inline Tool is ToolBypass. It means that the GigaVUE-HC2 will not send traffic to this inline tool if it is considered to be in a failure mode. The inline help field describes other options for inline tool. The other options have very different effects on the overall traffic flow.
   - Recovery Mode: **Automatic**
   - Enabled Heartbeat: **Checked**
   - Profile: **default**
   - HB IP Address A: **Leave Default**
   - HB IP Address B: **Leave Default**

Figure 6-5 Inline Tools Configuration

5. Click **Save** to write the configuration changes to memory as shown in Figure 6-5.

6. Repeat steps 1 through 5 for the second Check Point 4800 appliance and under Inline Tools, the status looks like Figure 6-6.

Figure 6-6: Inline Tools Status

Configuring the Inline Tool Group

The inline tool group configuration on the GigaVUE-HC2 is discussed in this section.

1. In GigaVUE-FM, select **Inline Bypass > Inline Tool Groups**.

2. Click **New** to open the Inline Tool Groups configuration page.

3. In the **Alias** field, enter an alias that represents the inline tool groups.

4. In the **Ports** section, click the Inline Tools field and select all the inline tools for this group from the list of available inline tools. Optionally, the Inline Spare Tool can be selected and an inline tool be selected. In that case, it becomes the primary failure action for this inline tool group.

5. In the **Configuration** section, configure the following and Save once done:

- Enabled: **Checked**
- Keep the defaults for **Release Spare if Possible, Failover Action, Failover Mode, Minimum Healthy Group Size**.
- **Hash: advanced** and **save**. Refer to Figure 6-7 for output.

  The advanced hashing scheme refers to hashing based on source IP, destination IP, L4 source port and L4 destination port. Choosing advanced hash ensures the following:

  - Bi-directional traffic for the same session goes to the same inline tool
  - Traffic is load shared amongst inline tools

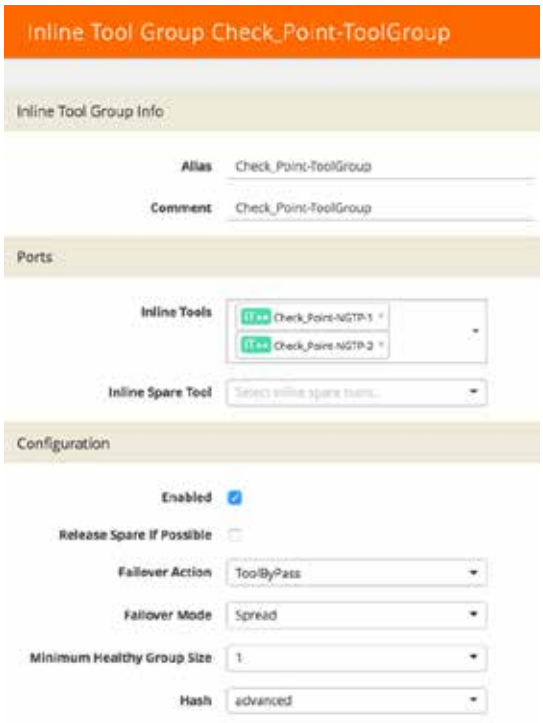

Figure 6-7: Inline Tool Group Configuration

Configuring GRIP

GRIP works by having an active GigaVUE-HC2 forward all inline traffic to inline tools and back into the network. At any given moment, only one of the two HC2s is actively forwarding traffic to the inline tools while the second HC2 is in a standby mode. When a failure is detected over the heartbeat link, the standby HC2 takes over and actively starts forwarding traffic.

GRIP requires the configuration of the following components:

- Stack port on each HC2: The secondary HC2 relies on the signaling link status for opening/closing its bypass protection switch relays; no keep alive or heartbeat messages are exchanged.
- Redundancy Profiles: Each HC2 is configured with a redundancy profile to designate whether it operates as a Primary or a Secondary. Bypass protection switch relays are opened in the Primary and are closed in the Secondary, allowing the traffic to only flow through the Primary.

Step 1: Configuring Stack Port:

The configuration for the stack port is below:

1. On GigaVUE-FM navigate to **Ports**.
2. Select the port connected to the second GigaVUE-HC2 and click **Edit**.
3. Enter a suitable alias and optionally a comment.
4. Under **Parameters**:
   - Admin > **Checked**
   - Type > **Stack**
   - Duplex > **Full**
5. Repeat steps 1 through 4 for the second GigaVUE-HC2. Refer to Figure 6-8 for output.

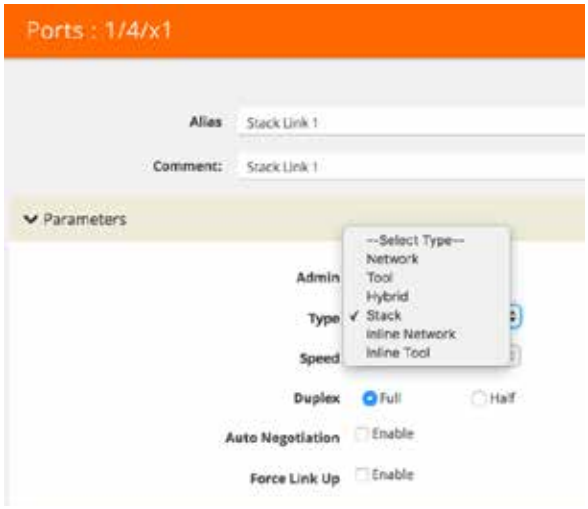

Figure 6-8: Stack Port Configuration

Step 2: Configuring redundancy profiles:

1. Navigate to **Inline Bypass** and click **Redundancies > New**.
2. Enter the following:
   - **Alias**
   - Signaling Port: **Stack Port defined earlier**
   - **Protection Role**: Primary for this node and choose secondary for the second GigaVUE-HC2. Refer to Figure 6-9 for output.

Figure 6-9 Create Redundancy Profile for the primary GigaVUE HC2

3. On the secondary node choose **secondary** as shown in Figure 6-10.

Figure 6-10: Create Redundancy Profile for the secondary GigaVUE HC2

Configuring Inline Traffic Flow Maps

This section describes in detail how to configure traffic flow from the inline network to the inline Check Point tool group and allowing the reader to test the functionality of the Check Point appliances within the group. It is done in a two-step process:

1. Traffic Flow Map with an Inline Bypass Rule.
2. Change the Inline Network Path to Inline Tool.

After going through the previous steps, you can test deployment of Check Point appliances.

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

This section describes the configuration steps to allow the flow of traffic between the Inline Network and the Inline Tool Group. Use the following steps to configure the flow map. The configuration should look like Figure 7-1:

1. In GigaVUE-FM, navigate to **Maps** and click on **New**
2. In the **Map Info** section configure the following:
   - **Map Alias**: Enter a map alias that represents the network source and tool destination
   - **Comments**: Enter comments for the map
   - Type: **Inline**
   - Sub Type: **By Rule**
   - Traffic Path: **Bypass**
3. In the Map Source and Destination section:
   - Set **Source** to the inline network that was created earlier.
   - Set **Destination** to the inline tool groups that were created earlier.
4. Under **Map Rules**:
   - Click **Add a Rule**
     - § In Rule 1 click Condition search… and select IP Version > Version v4 and select Bi Directional.
     - § Leave **Map Order** and **Map Permissions** to default values.

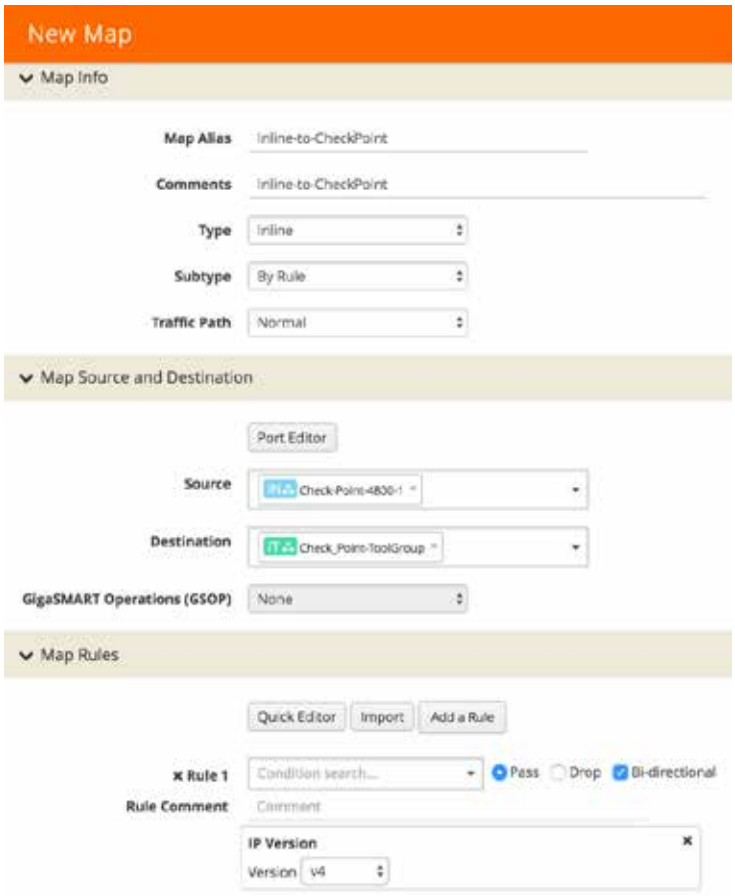

Figure 7-1: New Maps Configuration

Step 2: Apply redundancy profiles

At this point, the inline tools are connected and configured to inspect traffic from the inline network. The next step after configuring maps is to apply the redundancy profiles as follows:

1. In GigaVUE-FM, select inline network defined previously and click **Edit**.
2. Redundancy Profile created in Step 2 Configuring Redundancy Profile.

Figure 7-2: Inline Network with Redundancy Profile

3. Click **Save.** The configuration looks like Figure 7-2.

4. Repeat steps 1 and 3 for the secondary GigaVUE-HC2 in the network.

Testing the Functionality of the Solution in GRIP Mode

This section shows the CLI output for the GigaVUE HC2 in normal operating mode as well as after the failover.

Scenario 1: Normal Operation

After successful configuration, the traffic from the primary GigaVUE HC2 would be load shared to the inline tools for inspection and driven back into the network.

CLI commands to check for normal operation; check for Redundancy Control State.

First GigaVUE HC2 CLI output:

```
HC2-C03-17 # show inline-network alias default_inline_net_1_4_1
=============================================================================
    Inline-Network Alias: default_inline_net_1_4_1
                  Net-A: 1/4/x17
              Net-A Alias:
                  Net-B: 1/4/x18
              Net-B Alias:
                 Comment:
   Link Fail Propagation: true
         Physical Bypass: disable
            Traffic Path: to-inline-tool
        Forwarding State: NORMAL
      Redundancy Profile: Node-1-GRIP-rp
Redundancy Control State: Primary Forwarding
-----------------------------------------------------------------------------

HC2-C03-17 #
HC2-C03-17 # show inline-network alias default_inline_net_1_4_4
=============================================================================
    Inline-Network Alias: default_inline_net_1_4_4
                  Net-A: 1/4/x23
              Net-A Alias:
                  Net-B: 1/4/x24
              Net-B Alias:
                 Comment:
   Link Fail Propagation: true
         Physical Bypass: disable
            Traffic Path: to-inline-tool
        Forwarding State: NORMAL
      Redundancy Profile: Node-1-GRIP-rp
Redundancy Control State: Primary Forwarding
-----------------------------------------------------------------------------
```

Second GigaVUE HC2:

```
HC2-C04-31 # show inline-network alias default_inline_net_3_1_1
=============================================================================
    Inline-Network Alias: default_inline_net_3_1_1
                  Net-A: 3/1/x17
              Net-A Alias:
                  Net-B: 3/1/x18
              Net-B Alias:
                 Comment: Inline-Network-1
   Link Fail Propagation: true
```

```
         Physical Bypass: disable
            Traffic Path: to-inline-tool
       Forwarding State: DISCONNECTED
      Redundancy Profile: Node2-GRIP-rs
Redundancy Control State: Secondary Bypass
------------------------------------------------------------------------

HC2-C04-31 # show inline-network alias default_inline_net_3_1_2
========================================================================
    Inline-Network Alias: default_inline_net_3_1_2
                  Net-A: 3/1/x19
             Net-A Alias:
                  Net-B: 3/1/x20
             Net-B Alias:
                Comment:
   Link Fail Propagation: true
         Physical Bypass: disable
            Traffic Path: to-inline-tool
       Forwarding State: DISCONNECTED
      Redundancy Profile: Node2-GRIP-rs
Redundancy Control State: Secondary Bypass
------------------------------------------------------------------------
```

Scenario 2: Failover Operation

In the failover scenario, the first GigaVUE HC2 is assumed to have a power failure and acts simply as a wire. The traffic from the secondary GigaVUE HC2 would be load shared to the inline tools for inspection and driven back into the network.

CLI commands to check for normal operation; check for Redundancy Control State.

The first GigaVUE HC2 is assumed to have a power failure.

Second GigaVUE HC2 redundancy control state would change to ‘Secondary Forwarding’.

```
HC2-C04-31 # show inline-network alias default_inline_net_3_1_1
========================================================================
    Inline-Network Alias: default_inline_net_3_1_1
                  Net-A: 3/1/x17
             Net-A Alias:
                  Net-B: 3/1/x18
             Net-B Alias:
                Comment: Inline-Network-1
   Link Fail Propagation: true
         Physical Bypass: disable
            Traffic Path: to-inline-tool
       Forwarding State: DISCONNECTED
      Redundancy Profile: Node2-GRIP-rs
Redundancy Control State: Secondary Forwarding
------------------------------------------------------------------------

HC2-C04-31 # show inline-network alias default_inline_net_3_1_2
========================================================================
    Inline-Network Alias: default_inline_net_3_1_2
                  Net-A: 3/1/x19
             Net-A Alias:
                  Net-B: 3/1/x20
             Net-B Alias:
                Comment:
   Link Fail Propagation: true
```

```
         Physical Bypass: disable
            Traffic Path: to-inline-tool
       Forwarding State: NORMAL
      Redundancy Profile: Node2-GRIP-rs
Redundancy Control State: Secondary Forwarding
-------------------------------------------------------------------------
```

3 Summary and Conclusions

For more information on the GigaVUE-HC2 bypass protection, high availability, and scalability provided by Gigamon's Security Delivery Platform, go to *www.gigamon.com.*

How to get Help

For issues with Gigamon products, refer to http://www.gigamon.com/support-and-services/contact-support and your Support Agreement with Gigamon. You can also email Technical Support at support@gigamon.com.

For issues related to Check Point's products, refer to your Support Agreement with Check Point Software Technologies Ltd. and follow the directions on how to open a Support Case.

See Inside Your Network™

4090-01 10/16